Index

A

ABAC (attribute based access control), 179–180
ACFCS (Association of Certified Financial Crime Specialists), 320
adaptive thresholding, 163
Advanced Cloud Security Practitioner training, 318–319
Advanced Encryption Standard (AES), 254
Advanced Persistent Threat 16 (APT16), 90
AEHIS (Association for Executives in Healthcare Information Security), 320
AI. *See* AIOps; artificial intelligence
AIOps (artificial intelligence for IT operations), 11, 38, 145–172, 329–330
  CMDB, 157–158
  complexity of cloud resources, 145–146
  dynamic thresholds, 147–148
  function of, 146
  historical metrics and insights, 153
  IT service management, 170–171
  licensing, 153
  machine learning, 147
  natural language processing, 152
  overview, 145–147
  ServiceNow, 167–169, 339
  Splunk, 161–167
  stages of incident resolution, 148–155
  team changes, 171–172
  transitory problems, 152
  use case, 159–160
  visibility, 155–157
Airbnb, 83
Alibaba, 79
Amazon S3 (Simple Storage Service), 34, 128–129
Amazon service level agreement, 10
Amazon Web Services (AWS), 34, 79
  Centralized Logging dashboard, 138
  Cloud Map, 156
  CloudTrail, 76, 137
  CloudWatch, 76, 137
  data access control, 48
  Direct Connect, 212
  Discovery Service, 9
  encryption, 59
  GuardDuty app, 76
  hardware security modules, 259
  identity access management, 99
  Key Management System (KMS), 260
  Kinesis Data Streams, 138
  Lambda Service, 138
  logging, 137–138, 140
  Microsoft Cloud App Security, 62–63
  network isolation, 271
  open-source projects, 142
  patch management, 133
  tagging, 135–136
  VMware, 9, 216
  VMware Cloud, 216
Anchore Engine, 143
anonymizing data, 56–58
  k-anonymity, 57
  ℓ-diversity, 57
  obscuring data, 58
  overview, 56–57
Anti-Phishing Working Group (APWG), 320
Apache Airflow, 83
application programming interfaces (APIs), 102, 201, 205–206
APT16 (Advanced Persistent Threat 16), 90
APWG (Anti-Phishing Working Group), 320
artifact scanning, 303
artificial intelligence (AI), 11. *See also* AIOps
  data access levels, 96
  identifying user behavior, 119–120
  phishing, 269

COPYRIGHTED MATERIAL

Aruba ClearPass, 184
assets, defined, 14
associate agreements, 108
Association for Executives in Healthcare Information Security (AEHIS), 320
Association of Certified Financial Crime Specialists (ACFCS), 320
AT&T, 120
attorney/client data, 52
attribute based access control (ABAC), 179–180
Aunalytics, 78
Auth0, 47
authentication, 101–103
  API keys, 102
  Facebook, 103
  Firebase, 102–103
  Google, 103
  multifactor authentication, 101–102
  OAuth, 103
automated code testing, 71–78
  data accountability, assurance, and dependability, 77–78
  dynamic code analysis, 72–73
  large amounts of data, 73
  logging and monitoring, 76–77
  repetitive tasks, 73
  simple tasks, 73
  static code analysis, 72–73
automated discovery applications, 8–9, 35–36
AV Test, 190
AWS. *See* Amazon Web Services

B

Background Knowledge attacks, 49
backing up data, 226–227
Balbix, 22
banking information, 52, 221
Bare Metal as a Service (BMaaS), 33
Belafonte, Harry, 281
Bell Integration, 269
Bellaso, Giovan Battista, 254
Bernard of Chartres, 321
Bitcoin, 255–256, 334
Bitglass, 115
blocklists, 150
BMaaS (Bare Metal as a Service), 33
BOMs (software bills of materials), 75
Bootstrap, 74
branching code, 83
branching data, 84
breach prevention and management, 265–287
  cloud native breaches, 280–287
  data loss prevention systems, 279–280
  data theft, 266–276
  employee security, 276–279
  focus, 265–266
building plans, 53

C

Caesar, Julius, 253
canary honeypots, 96
Capital One, 105
CASBs. *See* cloud access security brokers
CCAK (Certificate of Cloud Auditing Knowledge), 318
CCSK (Certificate of Cloud Security Knowledge), 317–319
CDLP (cloud data loss prevention), 229–231
Center for Internet Security (CIS), 320
  Benchmarks, 295–296
  CIS Controls Cloud Companion Guide, 29
  Critical Security Controls, 295
Certificate of Cloud Auditing Knowledge (CCAK), 318
Certificate of Cloud Security Knowledge (CCSK), 317–319
certifications, 121–124, 317–319
Certified Risk and Information Systems Control (CRISC), 318
Certified Security Information Systems Auditor (CISA), 317–318
change control, 77
chaos engineering, 235–240
ChaosD, 93

Checkpoint
CloudGuard, 335–336
CloudGuard Workload Protection, 305
Chernobyl nuclear disaster, 239
Chief Information Security Officer Executive Network (CISO), 320
Chocolatey, 41
Churchill, Winston, 69
CIEM (Cloud Infrastructure Entitlements Management), 303
CIS. *See* Center for Internet Security
CIs (configuration items), 14
CISA (Certified Security Information Systems Auditor), 317–318
CISA (Cybersecurity and Infrastructure Security Agency), 186
Cisco Annual Internet Report, 313
CISO (Chief Information Security Officer Executive Network), 320
Citrix, 192–193
Clair, 143
cloud access security brokers (CASBs), 40, 115–116, 229–231, 313
agent-based vs. agentless, 115
API vs. forward proxy vs. reverse proxy, 40
basic services, 114–115
defined, 40
limits of, 231
Network Access Control, 183–184
overview, 114
SASE architecture, 118, 300–302
visibility, 230–231
cloud agnostic integration, 78–82
approaches, 81
overview, 79–80
pros-versus-cons assessment, 80–81
cloud auditors, defined, 13
cloud brokers, defined, 12
cloud carriers, defined, 12
cloud consumers, defined, 13
cloud data loss prevention (CDLP), 229–231
Cloud Infrastructure Entitlements Management (CIEM), 303
Cloud Native Application Protection Platform (CNAPP), 303–305
CSPM, 305
CWPP, 304–305
features of, 303–304
cloud native breaches, 280–287
defined, 280
employee data spillage, 284–287
employee error, 281–282
insider data theft, 283–284
Cloud Native Computing Foundation, 114
cloud resource management, 127–144
defense development, 141–144
identifying resources, 128–129
logging, 136–141
patch management, 132–134
tagging, 134–136
virtual resources, 129–132
cloud security, 7, 9, 27
advantages of, 24–26
AIOps, 145–172
breach prevention and management, 265–287
cloud resource management, 127–144
consortiums, 311–321
data access restriction, 95–124
data loss and disaster recovery, 219–240
data storage, 43–64
environment management, 35–38
frameworks for, 289–309
hybrid cloud environments, 195–217
non-network devices, 39–41
people as weakest link, 1
philosophies for managing, 1
public vs. private clouds, 7
security patches, 41–42
security plans, 8–24
services for, 243–263
shared responsibility model, 28–31
software and application development, 65–93
threats to, 1–2
zero trust, 173–193

Cloud Security Alliance (CSA), 311–319
best practices, 312–313
CCM framework, 24
membership in, 313–316
cloud security frameworks, 24
Cloud Security Posture Management (CSPM), 110–114, 304–305, 335
automating compliance, 113
discovering and remediating threats with, 112–113
integrating with DevOps, 113–114
intentional and unintentional breaches, 112–113
visibility, 111
zero trust, 184–185
cloud service providers, defined, 12
Cloud Workload Protection Platforms (CWPPs), 303–305
Cloudcheckr, 110
CloudPassage Halo, 336
Cloudrise, 244
CMDBs. *See* configuration management databases
CMSes (configuration management systems), 15, 328–329
CNAPP. *See* Cloud Native Application Protection Platform
COBIT (Control Objectives for Information and Related Technology), 290–291
Collibra Data Catalog, 46
Colonial Pipeline, 42, 222, 226
Common Criteria (ISO/IEC 15048), 296
Commvault, 228
compliance, 104–114, 332–333
automating, 113
defined, 104
EU data breaches, 287
focus, 266
GDPR, 106–107
global compliance, 104
government compliance, 109–110
HIPAA, 107–109
hybrid cloud environments, 206
maintaining, 110–114
PCI, 104–106
Computing Technology Industry Association (CompTIA), 320
conditional masking, 49
confidentiality agreements, 278
configuration items (CIs), 14
configuration management databases (CMDBs), 14, 98, 157–158, 329
automated discovery applications and, 19
configuration items, 158
defined, 157
potential impacts, 157–158
configuration management systems (CMSes), 15, 328–329
constant values, 49
containers and containerization, 82, 131–133, 140–141
patch management, 133
contractors, restricting access to, 100–101
Control Objectives for Information and Related Technology (COBIT), 290–291
credit card information, 52, 54–55, 104–105, 274
CRISC (Certified Risk and Information Systems Control), 318
crypto service gateways (CSGs), 263
cryptocurrency, 255–256, 334
CryptoLocker, 222
Cryptomathic, 252, 263
CSA. *See* Cloud Security Alliance
CSGs (crypto service gateways), 263
CSIA (Cyber, Space, & Intelligence Association), 320
CSIPs (cybersecurity strategy and implementation plans), 307–309
CSN (Cybercrime Support Network), 320
CSPM. *See* Cloud Security Posture Management
CWP (Symantec Cloud Workload Protection), 336–337
CWPPs (Cloud Workload Protection Platforms), 303–305
Cyber, Space, & Intelligence Association (CSIA), 320
Cyber Kill chain, 149
Cybercrime Support Network (CSN), 320
cybersecurity, origin of term, 105
Cybersecurity Advisors Network (CyAN), 320

Cybersecurity and Infrastructure Security Agency (CISA), 186
cybersecurity strategy and implementation plans (CSIPs), 307–309

D

Dagda, 143
dark web, 272
data access control, 47–49
  AWS, 48
  data access control systems, 47
  Immuta, 48
data access levels, 96–98
  artificial intelligence, 96
  honeypots, 96–97
  roles, 97
  user requirements, 97–98
data access restriction, 95–124, 331–332
  authentication, 101–103
  certifications, 121–124
  cloud access, 114–120
  Cloud Security Posture Management, 110–114
  compliance, 104–114
  determining access levels, 95–98
  least privilege policy, 98–101
data access security levels, 60–61
Data Bunker, 228
data bunkers, 227–228
data catalogs, 45–51
  assessing impact to critical functions, 50–51
  building, 46–47
  data access control, 47–49
  data catalog systems, 46
  data labeling, 49–50
  overview, 45
data centers, 29–30
  disaster preparedness, 30
  physical security, 29
  power continuity, 30
  redundancy, 30
  virtual security, 30
data classification systems, 51–54
Data Encryption Standard (DES), 254
data in motion, defined, 59
data integration tools, 45
data labeling, 49–50
  data annotation, 49
  label-based security, 50
  sensitivity levels, 50
  tagging, 49
data lakes, defined, 48
data leakage, 37, 207–208, 279, 284–285
data loss prevention (DLP), 117, 219–240, 279–280
  chaos engineering, 235–240
  cloud data loss prevention, 229–231
  disaster recovery, 220, 228, 232–235
  email, 220–224
  goal of, 219
  key components of, 280
  overview, 219–220
  strategies for, 224–228
data storage
  anonymizing data, 56–58
  data access security levels, 60–61
  data classification systems, 51–54
  encryption, 58–60
  hybrid cloud environments, 201–202
  hyperconverged infrastructure, 212
  segmenting data, 56
  tiered, 202
  tokenizing sensitive data, 54–56
  user access, 61–64
data stores
  defined, 89
  development of, 89
  elements of, 90
data theft, 266–276
  exfiltration, 271–273
  expanding, 269–271
  landing, 267–269
  offboarding employees, 273–276
Datadog Monitoring Software, 337
DataKitchen, 78

DataOps, 82–86, 330
collaboration, 85
innovation pipeline testing, 84
modularized code, 83
monitoring after release, 85
overview, 83
source code control, 83
user trust, 85–86
value pipeline testing, 84
version control, 84
workflow pipeline, 83
DataSecOps, 90–92
challenges of, 90–91
features of, 91
strategy development, 91–92
DDoS (distributed denial of service) attacks, 154, 257
Deep Instinct, 39
Defense Federal Acquisition Regulation Supplement (DFARS), 294–295
denial of service (DoS) attacks, 23
dependency tracking, 75
DES (Data Encryption Standard), 254
Detectify, 20
determining access levels, 95–98
device access, 62–63
DevOps, 65–71
automated code testing, 71–78
best practices, 71
CI/CD, 68
cloud agnostic integration, 78–82
cloud agnosticism, 81
defined, 66
early commitment to security, 69–70
features of, 66
integrating CSPM with, 113–114
reviewing security plan, 70–71
security controls, 70
shift-left concept, 68–69
waterfall method vs. agile method, 66–68
DevSecOps, 86–92
best practices applications, 71
dependency tracking, 75
DFARS (Defense Federal Acquisition Regulation Supplement), 294–295
DHCP (Dynamic Host Configuration Protocol) logging, 36
Diffie, Whitfield, 254
Diffie-Hellman key, 254
disaster recovery, 220, 228, 232–235
business continuity, 232–233
planning for, 232–235
RTO and RPO, 233
testing plans, 234–235
distributed denial of service (DDoS) attacks, 154, 257
DLP. *See* data loss prevention
DNS Security Extensions (DNSSEC), 256–257
Docker, 82, 132, 198–199
Domain Name Service (DNS), 256–257
DoS (denial of service) attacks, 23
Downdetector, 79
Dropbox, 128
Dynamic Host Configuration Protocol (DHCP) logging, 36
DynaTrace, 77

E

EaaS (Encryption as a Service), 262
ECC (elliptic curve cryptography), 255
ECDSA (Elliptic Curve Digital Signature Algorithm), 260
edge computing (edge delivery), 31, 197–198, 299
EEOC (Equal Employment Opportunity Commission), 277
Elasticsearch, 137–138
elliptic curve cryptography (ECC), 255
Elliptic Curve Digital Signature Algorithm (ECDSA), 260
email, 220–224
deleting, 60
encryption, 178–179
malware, 221–222
offboarding employees, 274
ransomware, 222–223

employee security management, 276–280
  background checks, 277
  confidentiality agreements, 278
  employee data spillage, 284–287
  employee error, 281–282
  employee records, 52
  employee training, 278–279, 312
  offboarding employees, 273–276
encryption, 2, 58–60, 312
  of data in motion, 59
  of data in use by applications, 60
  end-to-end, 177–179
  quantum computing, 334
  security keys, 29, 52
  of stored data, 59–60
  symmetric, 253–254
  zero trust, 192
Encryption as a Service (EaaS), 262
endpoint device management, 176–177
end-to-end encryption, 177–179
  email, 178–179
  public key/private key encryption, 177–178
enumeration, 58
environment management, 35–38
  application auditing, 38
  automated discovery applications, 35–36
  growth and chaos, 39
  log management tools, 35–36
  restricting access, 36
  supply chain security risk management, 36–38
  virtual device management, 38
Equal Employment Opportunity Commission (EEOC), 277
Equifax, 105
escalation automation, 165
European Union (EU), 20, 287
Everbridge, 234
Exate, 92
ExaVault, 250

F

FaaS (Function as a Service), 34
Face ID, 102
Facebook, 103, 245, 267–268
Falco, 114, 143
Family Educational Rights and Privacy Act (FERPA) of 1974, 53, 104
Fast IDentity Online Universal 2nd Factor (FIDO U2F) tokens, 244, 248–249
FBI, 222, 287
FDA (US Food and Drug Administration), 296–297
federal contractor data, 52
Federal Financial Institutions Examination Council (FFIEC) Cyber Assessment Tool (CAT), 292
Federal Information Security Modernization Act (FISMA) of 2002, 52, 305–307
Federal Information Systems Security Educators Association (FISSEA), 320
Federal Risk and Authorization Management Program (FEDRAMP), 292
Federal Trade Commission (FTC), 286, 294
FERPA (Family Educational Rights and Privacy Act) of 1974, 53, 104
FFIEC (Federal Financial Institutions Examination Council) Cyber Assessment Tool (CAT), 292
FIDO U2F (Fast IDentity Online Universal 2nd Factor) tokens, 244, 248–249
Firebase, 102–103
Firewall as a Service (FWaaS), 118, 300
FIRST (Forum of Incident Response and Security Teams), 320
FirstEigen, 78
FISMA (Federal Information Security Modernization Act) of 2002, 52, 305–307
FISSEA (Federal Information Systems Security Educators Association), 320
FontAwesome, 74
forensic investigations, 120
FortiCASB, 207
Fortinet
  Cloud Security, 338–339
  FortiCASB, 206–207
  SWG, 116

Forum of Incident Response and Security Teams (FIRST), 320
Franklin, Benjamin, 69
FTC (Federal Trade Commission), 286, 294
FTP servers, 272
Fukushima Daiichi nuclear disaster, 239
Function as a Service (FaaS), 34
Futurex HSM, 252
FWaaS (Firewall as a Service), 118, 300

G

GAPP (Generally Accepted Privacy Principles), 123
Gartner, 41, 119, 289
Gauntlt, 71
General Data Protection Regulation (GDPR), 104
  compliance, 106–107
  Lead Auditor and Consultant certification, 319
Generally Accepted Privacy Principles (GAPP), 123
Genie, 83
geofencing, 63
GFILanGuard, 41
Git, 83
GIT source code control system, 100
GitHub, 76, 143
Gitrob, 144
Git-secrets, 144
GLBA (Gramm-Leach-Bliley Act), 293–294
God roles, 99
Google
  authentication, 103
  quantum computing, 333
Google Cloud
  Data Catalog, 46
  Discovery Service, 9
  encryption, 59
  hardware security modules, 259
  logging, 136–137, 140
  market share, 79
  network isolation, 271
  patch management, 133
  service level agreement, 10
Google Drive, 128
governance by design, 84
GPS, 63
Gramm-Leach-Bliley Act (GLBA), 293–294
Ground Control, 235

H

Hancock, Jeff, 281
hard tokens, 244, 246–247
Hardware Asset Management (HAM), 210–211
hardware risk assessments, 108
hardware security modules (HSMs), 251–259
  cloud HSMs, 259
  cryptocurrency, 255
  cryptography, 252–253
  data security requirements, 256
  defined, 251
  DNSSEC, 256–257
  evaluating, 258–259
  functions of, 252
  key management, 253–256
  OpenDNSSEC, 257–258
  tamper resistance, 255
hashing, 58
Health Insurance Portability and Accountability Act (HIPAA), 47, 52, 89, 104
  breaches, 109
  compliance, 107–109
  forms, 108
  training, 109
heat and color maps, 21–22
Hellman, Martin, 254
Help Net Security, 277
Hewlett Packard
  HPE Cloud Volumes, 207
  HPE Hybrid Cloud Solution, 216
high interaction honeypots, 96
HIPAA. *See* Health Insurance Portability and Accountability Act
hole-in-the-bucket problem, 281
Homogeneity attack, 49

honeypots, 30, 96–97
HSMs. *See* hardware security modules
hybrid cloud environments, 195–217
  advantages of, 203–207
  data storage, 201–202
  defined, 195–196
  end points, 200–201
  migrating to, 213–216
  private clouds, 199–200
  public clouds, 196–199
  ready-made packages, 216–217
hyperconvergence, 199, 212
hypervisors, 38, 130

I

IaaS. *See* Infrastructure as a Service
IaC (Infrastructure as Code), 112, 185, 244
IAM (identity access management), 97–99
IAPP (International Association of Privacy Professionals), 320
IASAP (International Association of Security Awareness Professionals), 320
IBM
  disaster recovery, 228
  Network Job Protocol, 272
  quantum computing, 333
  Watson Knowledge Catalog, 46
ICMCP (International Consortium of Minority Cybersecurity Professionals), 320
identity access management (IAM), 97–99
Identity Management Institute (IMI), 320
identity theft, 268
IDFactors, 256
IIA (Institute of Internal Auditors), 320
immigration documents, 53
Immuta, 48
Imprivata, 32
inbound IP whitelisting, 61
Information Systems Security Association (ISSA), 320
Information Technology Infrastructure Library (ITIL), 297
Infragard, 320
Infrastructure as a Service (IaaS)
  CSPM, 111, 114
  defined, 33
  licensing, 153
  security, 34
  shared responsibility model, 28, 35
Infrastructure as Code (IaC), 112, 185, 244
Institute of Internal Auditors (IIA), 320
Integration Platform as a Service (iPaaS), 45
intellectual property documents, 53, 117, 123, 227, 273–274, 278, 280, 295
International Association of Privacy Professionals (IAPP), 320
International Association of Security Awareness Professionals (IASAP), 320
International Consortium of Minority Cybersecurity Professionals (ICMCP), 320
International Information Systems Security Certification Consortium (ISC2), 320
International Standards Organization (ISO)/ International Electrotechnical Commission (IEC)
  2700 Series, 295
  27001 certification, 121
  27017/18 framework, 24
  27701 framework, 24
  Common Criteria (ISO/IEC 15048), 296
  compliance definition, 104
Internet Security Alliance (ISA), 321
IP access, 61–62
  inbound IP whitelisting, 61
  outbound IP whitelisting, 61
  spoofing, 62
iPaaS (Integration Platform as a Service), 45
ISA (Internet Security Alliance), 321
Isaca, 290, 317
ISC2 (International Information Systems Security Certification Consortium), 320
ISO/IEC. *See* International Standards Organization/ International Electrotechnical Commission
ISSA (Information Systems Security Association), 320
Istio, 82

IT Asset Management (ITAM), 17–18, 209–211, 297
IT Information Sharing and Analysis Center (IT-ISAC), 321
IT Operations Management (ITOM), 168–171
IT security credentials, 52
IT Service Management (ITSM), 155, 159
  goal of, 155
  performance analytics, 170–171
  ServiceNow, 168–169
  traditional approaches vs., 170
ITAM (IT Asset Management), 17–18, 209–211, 297
ITIL (Information Technology Infrastructure Library), 297
IT-ISAC (IT Information Sharing and Analysis Center), 321
ITOM (IT Operations Management), 168–171
ITSM. *See* IT Service Management
Ivanti, 19

J

JavaScript, 74
jQuery, 74
jQueryUI, 74
JSON, 136
JumpCloud, 47
Jupyter Notebook, 93
just-in-time privileges, 99

K

k-anonymity, 49, 57
key management services (KMSs), 59, 259–262
  defined, 259–260
  encryption-key lifecycle, 262
  SSH compliance, 260–261
keyloggers, 269
Kindervag, John, 174
Kipling, Rudyard, 189
KMSs. *See* key management services
knowledge base articles, 153
Kubernetes
  containers, 140–141
  Falco and, 114
  Istio and, 82
  Kubernetes Security Posture Management (KSPM), 304
  RBAC, 271

L

Lacework, 340
LANs (local area networks), 201, 270
LBAC (location based access control), 63
least privilege policy, 98–101
  contractors, 100–101
  just-in-time privileges, 99
  need-to-know strategy, 99
  trusted employees, 99–100
  zero trust, 182
LinkedIn, 269
ℓ-diversity, 57
local area networks (LANs), 201, 270
location based access control (LBAC), 63
logging, 136–141
  accountability, 181
  automated code testing, 76–77
  AWS, 137–138
  Azure, 139
  containers, 140–141
  deleting log files, 64
  Google Cloud, 136–137
  overview, 136
  third-party log management software, 139–140
  zero trust, 192
logical networks, defined, 34
Lookout, 119
low interaction honeypots, 96

M

machine learning, 147. *See also* AIOps; artificial intelligence
malware, 190, 192, 208, 221–222, 272
  email, 267
  FIDO U2F tokens, 249
  least privilege policy, 98

supply chain security risk management, 38
virtual security, 30
man traps, 29
Manage Engine Desktop Central, 132
managed data protection services, 244
managed service providers, 120
ManageEngine
Cloud Security Plus, 140
Patch Manager Plus, 41
man-in-the-middle attacks, 245, 249
Matilda Cloud, 156
Mayorkas, Alejandro, 334
McAfee
MVISION Cloud, 184
MVISION Cloud-Native Application Platform (CNAPP), 305
MCAS (Microsoft Cloud App Security), 62–63
Mean Time To Acknowledgment (MTTA), 159
Mean Time To Repair (MTTR), 159
Mean Time To Resolution (MTTR), 151
MediaFire, 128, 250–251
MFA (multifactor authentication), 101–102, 175–176, 245
microsegmentation, 270–271
microservice modules approach, 81, 83
Microsoft 365, 50, 62
Microsoft Azure
Active Directory, 47, 338
Advisor, 71
ExpressRoute, 212
hybrid cloud solutions, 217
location based access control, 63
logging, 139
market share, 79
network isolation, 271
service map application, 157
Microsoft Cloud App Security (MCAS), 62–63
Microsoft Cosmos DB, 92–93
Microsoft Jet Database, 47
Microsoft Teams, 62
middleware protection systems, 117–120
artificial intelligence, 119–120
data loss prevention systems, 117
Firewall as a Service, 118
forensic investigations, 120
managed service providers, 120
Secure Access Service Edge, 118–119
secure web gateways, 117
Mt. Gox cryptocurrency exchange, 256
MTTA (Mean Time To Acknowledgment), 159
MTTR (Mean Time To Repair), 159
MTTR (Mean Time To Resolution), 151
multiclouds, 206
multifactor authentication (MFA), 101–102, 175–176, 245
MyAssetTag, 39

N

NAC (Network Access Control; Network Admission Control), 182–184
National Cybersecurity Alliance (NCSA), 321
National Cybersecurity Society (NCSS), 321
National Institute of Standards and Technology (NIST), 186, 248, 279
Cybersecurity Framework Policy Template Guide, 29
NIST 800-171, 109–110, 294–295
Risk Management framework, 24, 306–309
National Technology Security Coalition (NTSC), 321
natural language processing (NLP), 152
NCSA (National Cybersecurity Alliance), 321
NCSS (National Cybersecurity Society), 321
NDAs (nondisclosure agreements), 278
need-to-know strategy, 99
Netflix, 83
Netskope, 41, 119
Network Access Control (NAC; Network Admission Control), 182–184
network isolation, 270–271
Network Job Protocol (NJP), 272
network segmentation, 270–271
network sniffers, 269
Newton, Isaac, 321
Nigerian prince scam, 221
Nirvanix, 79

NIST. *See* National Institute of Standards and Technology
NJP (Network Job Protocol), 272
NLP (natural language processing), 152
noncompete agreements, 278
nondisclosure agreements (NDAs), 278
non-network devices, 39–41
  clouds asset security brokers, 40
  inventorying, 39–40
notable event aggregation policy, 164
NSA, 142
nShield, 258–259
NTSC (National Technology Security Coalition), 321
null values, 49

O

OAuth (Open Authorization), 103
obscuring data, 58
Odetta, 281
offboarding employees, 273–276
OMIGOD vulnerability, 139
on-demand tokens, 244, 247–248
one-time passwords (OTPs; tokens), 245–249
  on-demand tokens, 244, 247–248
  FIDO U2F tokens, 244, 248–249
  hard tokens, 244, 246–247
  soft tokens, 246
Open Authorization (OAuth), 103
OpenDNSSEC, 256–258
OpenID, 102–103
OpenSCAP, 143
open-source code
  AWS, 142
  codebase security, 143–144
  container security, 143
  software composition analysis, 74–75
Oracle
  data labeling, 50
  DBMS, 128
  service level agreement, 10
OTPs. *See* one-time passwords
outbound IP whitelisting, 61

P

PaaS. *See* Platform as a Service
Palo Alto Prisma, 338
patch management, 41–42, 132–134, 269
  containers, 133
  implementing, 133–134
  patch management applications, 41
  virtual machines, 133
Patch Management as a Service (PMaaS), 269
payment card industry (PCI), 47, 52
  certification, 124
  certifications, 142
  compliance, 104–106
  Payment Card Industry Data Security Standard (PCI DSS), 104, 293
PBAC. *See* policy based access control
PC Cyborg, 221
penetration-testing (pen-testing), 20
perimeter security, 174
permutating, 58
Personal Information Protection and Electronic Documents Act (PIPEDA), 293
phishing, 208, 221, 248, 267–269
PKI Solutions, 258
plainID, 180
Platform as a Service (PaaS)
  advantages of, 33
  CSPM, 111
  defined, 32
  licensing, 153
  security, 33
  security responsibilities, 28, 35
PMaaS (Patch Management as a Service), 269
policy based access control (PBAC), 179–180, 192
  characteristics of, 179
  overview, 180
  previous strategies, 179–180
Poll, Joseph, 222
POPI (Protection of Personal Information Act), 104
post-admission NAC systems, 183
Prancer, 244
pre-admission NAC systems, 183

Prisma Cloud, 71
privacy by design, 84
private clouds
  data storage, 201–202
  overview, 199–200
Progress, 250
Protection of Personal Information Act (POPI), 104
pseudoanonymization, 48
public clouds, 196–199
  data storage, 201–202
  environment management, 197
  security management, 198–199
  speed, 197–198
public key cryptography, 178
Pure Storage, 228

Q

Qualsys, 19
quantum computing, 333–334

R

ransomware, 2, 16, 23, 42, 226, 287
  cloud, 223
  email, 222–223
  history of, 222–223
  least privilege policy, 99
rapid response, 308
RBAC (role-based access control), 179, 271
Recovery Point Objective (RPO), 233
Recovery Time Objective (RTO), 233
Regroup, 234
regular expression masking, 48
remote access trojans (RATs), 272
REST APIs, 129
retail passerby login problem, 160
RFID, 63
risk assessment databases, 22–24
  confidential data loss, 23
  data access loss, 23
  fields to track, 24
  integrity loss, 23
  mitigation plans, 24
  security levels, 24
Risk Management Association (RMA), 321
risk management plans, 13–16
  assessing consequences of disaster, 15
  asset inventory, 14–15
  asset management applications, 14–15
  assigning risk to team members, 15–16
  diagrams, 14
  disaster planning, 16
  identifying risks, 14–15
RMA (Risk Management Association), 321
role-based access control (RBAC), 179, 271
rounding, 48
RPO (Recovery Point Objective), 233
RSA algorithm, 260
RTO (Recovery Time Objective), 233

S

SaaS. *See* Software as a Service
SABSA (Sherwood Applied Business Security Architecture), 291–292
SAM (Software Asset Management), 210–211
SASE. *See* Secure Access Service Edge architecture
Satori, 92
SCA (software composition analysis). *See* software composition analysis
SCF (Security Controls Framework), 294
scratch files, 60
Scribe Data Labeler, 49
SD-IX (software-defined interconnections), 212
SDNs (software defined networks), 131
SDWANs (software-defined wide-area networks), 119, 303
Secure Access Service Edge (SASE) architecture, 118–119, 298–303
  components of, 300–303
  objective of, 299

secure File Transfer Protocol (sFTP), 250
Secure Shell (SSH)
  automating key management, 282
  key management services, 260–261
  offboarding employees, 274
secure sockets layer (SSL) protocol, 33, 250
secure web gateways (SWGs), 117, 300
security consortiums and alliances, 311–321, 333
  certifications, 317–319
  Cloud Security Alliance, 311–317
  general, 319–321
Security Controls Framework (SCF), 294
security frameworks, 289–309
  CNAPP, 303–305
  common, 290–297
  NIST Risk Management framework, 305–309
  SASE architecture, 298–303
Security Industry Association (SIA), 321
security information and event management (SIEM), 181–182, 192
security plans, 8–24
  applications list, 8, 326
  asset inventory, 8, 326
  automated discovery applications, 8–9
  determining which assets to protect, 17–20, 326
  heat and color maps, 21–22
  risk assessment databases, 22–24
  risk levels, 20–21
  risk management plans, 13–16, 326
  security team, 11–13, 327–328
  service level agreements, 10
  steps for, 325–324
Security Service Edge (SSE), 299
security team, 11–13
  finding people for, 12
  stakeholders, 12–13
security zones, 270–271
Sematext, 141
service level agreements (SLAs), 10–11, 208–209
  items covered in, 10
  links to, 10
  security, 10–11
  your responsibilities, 11
service maps, 168
service meshes, 81–82
ServiceNow, 339
  Common Service Data Model (CSDM), 158
  Discovery, 157
  Mapping Patterns, 157
  Performance Analytics, 171
  using with Splunk, 165–166
session hijacking, 248
sFTP (secure File Transfer Protocol), 250
shared responsibility model, 28–31
  data centers, 29–30
  defined, 28
  industry standards, 29
  responsibilities per service, 28
  security keys, 29
  your responsibilities, 31
SharePoint, 62
Sherwood Applied Business Security Architecture (SABSA), 291–292
shifting values, 58
SIA (Security Industry Association), 321
SIEM (security information and event management), 181–182, 192
single sign on (SSO), 32
6 Rs framework, 214
Skycasters, 235
Slack, 284
SLAs. *See* service level agreements
sneakernet, 272
Snowflake, 76
SOC 2. *See* System and Organization Controls 2
social security numbers, 52–53
soft tokens, 246
software and application development, 65–93
  automated code testing, 71–78
  cloud agnostic integration, 78–82
  DataOps, 82–86
  DataSecOps, 90–92
  DevOps, 65–71
  DevSecOps, 86–90

risks, 92–93
Software as a Service (SaaS)
advantages of, 31
CSPM, 111
defined, 31
hybrid cloud environments, 207
licensing, 153
offboarding employees, 274
security, 32
security responsibilities, 28, 35
siloes, 44
Software Asset Management (SAM), 210–211
software bills of materials (BOMs), 75
software composition analysis (SCA), 74–76
dependency tracking, 75
open-source code, 74–75
overview, 74
plugging security holes, 75–76
software defined networks (SDNs), 131
software-defined interconnections (SD-IX), 212
software-defined wide-area networks (SDWANs), 119, 303
source code control systems, 83
Splunk, 77, 161–167, 330
adaptive thresholding, 163
Alert system, 162–163
On-Call, 165–166
Deep Dive, 164
Event Analytics, 164
Executive Dashboard, 164
IT Service Intelligence (ITSI), 163, 165–166
Observability Cloud, 161–162
Phantom, 164–167
predictive analytics module, 163
Security Analytics for AWS, 163
Service Analyzer, 164
using with ServiceNow, 165–166
spoofing, 62, 177–178, 221
SQL database scripting exploits, 272
SSE (Security Service Edge), 299
SSH. *See* Secure Shell
SSL (secure sockets layer) protocol, 33, 250
SSO (single sign on), 32
stakeholders, 12–13
app and data users, 13
cloud auditors, 13
cloud brokers, 12
cloud carriers, 12
cloud consumers, 13
cloud service providers, 12
storage gateways, 272
StrongSalt, 262
student records, 53, 104
supervised machine learning, 147
supply chain security risk management, 36–38
data leakage, 37
defined, 36
malware attacks, 38
supply chain breaches, 37
SWGs (secure web gateways), 117, 300
swim lanes, 164
swivel chair data entry, 205
Symantec Cloud Workload Protection (CWP), 336–337
symmetric encryption, 253–254
Synopsis, 75
Sysdig, 114
System and Organization Controls 2 (SOC 2)
availability, 122–123
certification, 122–123
compliance, 18
confidentiality, 123
ITAMs, 18
privacy, 123
processing integrity, 123
security, 122
system logs (syslogs), 35

T

tagging, 134–136
  case-sensitivity, 135
  device access, 62
  name/value pairs, 135
  sample tags, 135
  storage format, 136
  usefulness of, 134
Tanium Asset, 19
TapID Mobile Account Security, 249
temporary files, 60, 64
Tenable.io, 19
Tessian, 281
Thales Group, 258–259
Threat Stack Cloud Security Platform, 336
thresholds
  adaptive thresholding, 163
  defined, 163
  dynamic thresholds, 147–148
Thycotic Secret Server, 282
Tibco Cloud Integration, 45
tiered backups, 226–227
TLS (Transport Layer Security), 59
tokens and tokenization, 54–56
  accessing system, 55
  authentication, 55–56, 175
  credit card information, 54–55
  isolating system, 55
  one-time passwords, 245–249
  tokens, defined, 54
Tor, 63, 272
trade secrets, 51, 53, 199, 227, 278
Transport Layer Security (TLS), 59
truncating, 58
trust anchors, 257
trusted employees, 99–100
two-factor authentication, 55–56, 63, 175–176

U

UEBA (user and entity behavior analytics systems), 181–182
unmanaged devices, 62
unsupervised machine learning, 147
US Department of Homeland Security, 334
US Food and Drug Administration (FDA), 296–297
user access, 61–64
  device access, 62–63
  IP access, 61–62
  location based access control, 63
  stale data, 64
user and entity behavior analytics systems (UEBA), 181–182

V

Venafi, 282
Veracode, 71
Verizon Data Breach Investigations, 283
version control systems, 83–84
VIPGames, 282
virtual private networks (VPNs), 42
  hybrid cloud environments, 201
  offboarding employees, 274
virtualization and virtual machines (VMs), 129–132
  containers, 131–132
  defined, 130
  device management, 38
  hyperconverged infrastructure, 212
  overview, 130
  patch management, 133
  security concerns, 130–131
  tagging, 135
voicemail systems, 275
VPNs. *See* virtual private networks

W

WannaCry, 222
waterfall method
  agile method vs., 66–68
  shift-left concept, 68–69
weirdness protection, 301–302
whitelisting, 61
wide area networks (WANs), 119, 201, 303
WinSock FTP (WS_FTP), 250
Wiz, 93
WWE, 27

X

XML, 136

Y

Yubiko, 249

Z

zero trust, 173–193, 312, 330–331
  challenges of, 190–194
  defined, 173
  features of, 175–185
  implementing, 185–194
  perimeter security vs., 174
  SASE architecture, 302–303
Zero Trust Network Access (ZTNA), 302–303
Zoho Patch Management Plus, 132