Index

A

Access control lists (ACLs), 32, 95, 99, 100, 263, 390
ACLs. *See* Access control lists (ACLs)
Address resolution protocol (ARP), 228
Ad infinitum, 342
Adobe portable document format (PDF) expolits, 197
Advanced metering infrastructure (AMI), 80, 81, 118, 162
  security concerns, 164
  security recommendations, 164
Advanced persistent diligence, 51
  defense-in-depth (DiD) approach, 51
Advanced persistent threats (APTs), 4, 9, 47, 48, 191
  cyber warfare, and, 50
  information targets, 49
AGC. *See* Automatic generation control (AGC)
Air gap, 36, 308
  digital communication, and, 42, 43
  separation, 104
Alerts, 381
  firewall, 340
  HIDS device, 314
  mechanisms used by commercial SIEMs, 381
  NRC RG 5.71 standard, 381
  security, 252
American national standards institute (ANSI), 390, 412
American petroleum institute (API), 398
AMI. *See* Advanced metering infrastructure (AMI)
AMI Headend, 80
Anomaly detection, 5, 330
  behavioural based, 330
  definition of, 330
  examples of, 330
  tools, 332
    log management, 332
    NBAD, 332
    SIEM, 332
ANSI. *See* American national standards institute (ANSI)
ANSI/ISA 84.00.01 standards, 210
Antisocial networks, 200
Antivirus software (AVS), 224
Antivirus systems, 314
Antivirus techniques, 315
API. *See* American petroleum institute (API)
Application behavior whitelists, 337
  examples in enterprise networks, 337
  examples in industrial networks, 337
Application data monitors, 305
Application-layer firewall, 131
Application logs, 358
Application monitoring tools, 338
Applications session details, from an application monitor, 360
Application whitelisting (AWL), 36, 314, 333, 354, 362
APTs. *See* Advanced persistent threats (APTs)
ARP. *See* Address resolution protocol (ARP)
Assessment console, 233
Assets, 11, 356
  critical cyber assets (CCA), 11, 12
  critical digital asset, 16
  cyber assets, 11
  HIDS devices, 313
  ICS components, 11
  ICS servers, 12
  inventory and documentation, 223
  "logical", 11
  logical assets, 11
  physical assets, 11
Attack surface, 5
Attack vectors, 3, 5
Automatic generation control (AGC) system, 174
Automation systems, 2, 7, 42, 80, 187
AWL. *See* Application whitelisting (AWL)

B

Backend protocols, 122
  inter-control center protocol (ICCP), 122
  object linking and embedding for process control (OPC), 122
Badge scanners, 69
Bandwidth, 63, 112
Baselines, measuring of, 327
  behavioural blueprint, 333
Basic process control system (BPCS), 78, 115
Battelle energy alliance (BEA), 304
BEA. *See* Battelle energy alliance (BEA)
Behavioral anomaly detection, 326
Behavioral whitelisting, 333
Behavior monitoring, 365
Beneficial whitelists, examples of, 338, 339
Biometric readers, 69
Black hat, information security conferences, 213
Blacklist security mechanisms, 339
Blacklist solution, 314
BPCS. *See* Basic process control system (BPCS)

Branch topologies, 94
Business information consoles, 68
Business information management systems (BIMS), 75
Business intelligence management, 74
Business networks, 20, 21, 85
Bus topologies, 94

C

CAN. *See* Controller area network (CAN)
Cannibalistic mutant underground malware, 202
Carrier sense multiple access (CSMA), 143
CCA. *See* Critical cyber asset (CCA)
CCTV. *See* Closed-circuit television (CCTV)
CD. *See* Collision domain (CD)
CEF. *See* Common event format (CEF)
Centre for the protection of national infrastructure (CPNI), 396
CEP. *See* Certes networks enforcement point (CEP)
Certes networks enforcement point (CEP), 369
Certified information systems security professional (CISSP) certification, 2
CFATS. *See* Chemical facilities anti-terrorism standards (CFATS)
CFATS risk-based performance standards (RBPS), 412
CFR. *See* Code of federal regulations (CFR)
Chemical facilities anti-terrorism standards (CFATS), 38, 288, 351, 387, 389, 412
CIM. *See* Computer integrated manufacturing (CIM)
CIP. *See* Common industrial protocol (CIP); Control and information protocol (CIP); Critical infrastructure protection (CIP)
CISSP. *See* Certified information systems security professional (CISSP)
Class of service (CoS), 112
Closed-circuit television (CCTV) systems, 69
CM. *See* Configuration management (CM)
Code of federal regulations (CFR), 392, 411
Collision domain (CD), 143
COM. *See* Component object model (COM)
Command line tools, 233
  windows server 2003, 234
  windows XP professional, 234
Commercial off-the-shelf (COTS) technologies, 121
Common criteria's framework, 399
  evaluation assurance level (EAL), 399
  protection profiles (PP), 399
  security assurance requirements (SARs), 399
  security functional requirements (SFRs), 399
  security target (ST), 399
Common event expression framework, 344
Common event format (CEF), 345
Common industrial protocol (CIP), 122, 143, 144, 410
Common vulnerabilities and exposures (CVE), 247
Common vulnerability scoring system (CVSS), 53, 252
  base metric, 252
  environmental metric, 252
  temporal metric, 252
Communication channels, 261
Communication flow
  represented as connections, 89
  represented as sessions, 88
Compliance auditing, 250
Component object model (COM), 150
Computer forensics tool testing (CFTT), 204
Computer integrated manufacturing (CIM), 261
Concurrent time domain multiple access (CTDMA), 143
Conditional formatting feature, 256, 257
Configuration auditing, 250
Configuration management (CM), 358
Configuration monitoring, 358
Content management system (CMS), 363
Contextual information, 365–367
Control and information protocol (CIP), 142, 143
  security concerns, 144
  security recommendations, 144
Control data storage, 270
  data historian system, 270, 271
  network attached storage (NAS) devices, 270
  storage area networks (SAN), 270
Controller area network (CAN), 142
Control loops, 70, 71, 76, 77, 267
  actuator, 267
  controller, 267
  sensor, 267
  supervisory controls, 268
Control networks, 105
Control processes, 4, 72, 76
Control systems
  assets, 4
  vulnerabilities, 44
CPNI. *See* Centre for the protection of national infrastructure (CPNI)
Critical cyber asset (CCA), 12
Critical infrastructure, 3, 9, 26
  critical systems and assets, 26
  homeland security presidential directive seven (HSPD-7), 26
Critical infrastructure protection (CIP), 12, 286, 387

Critical national infrastructures, 26
bulk electric, 27
Chemical facilities, 29
homeland security presidential directive seven (HSPD-7), 26
nuclear facilities, 27
Smart Grid, 28
utilities, 26
Cross-source correlation, 345, 346
CSET. *See* Cyber security evaluation tool (CSET)
CSMA. *See* Carrier sense multiple access (CSMA)
CTDMA. *See* Concurrent time domain multiple access (CTDMA)
CVE. *See* Common vulnerabilities and exposures (CVE)
CVSS. *See* Common vulnerability scoring system (CVSS)
Cyber asset whitelists, 335, 336
Cyber-attacks, 45, 171, 309
consequences, 213
espionage
hacking, 45
malware, 45
social engineering, 46
impact of, 173
sobotage
social engineering, 45
targeted, 39
Cyber-attacks, common methods of, 186
blended attacks, 190
denial-of-service attacks, 187
engineering workstation, compromising the, 189
exploitation of functionality, 186
exploitation of vulnerabilities, 186
human–machine interface (HMI), compromising the, 189
man-in-the-middle attacks, 186
replay attacks, 188
Cyber-attacks, industrial targets of, 174, 175
access control system, 175
Active Directory, 174
analyzer management system, 175
application servers, 175
asset management system, 175
condition monitoring system, 175
controller, 175
identity and access management (IAM) server, 174
industrial applications, 174
protocols, 174
Cyber-attack trends, 196
malware, 197
mutating bots, 197
web-based applications, use of, 196
Cyber crime, 53
Cyber sabotage, 171
Cyber safety, 172
Cyber security, 5, 10, 36–37, 172, 210, 261
APTs, 11
attacks, 11
breaches, 11
business networks, 10
critical infrastructure, 10
cyber assets, 10
electronic security perimeter (ESP), 10
enforcement methods, 12
exploits, 11
functional safety, 210
guidelines, 3
industrial control systems, 10
industrial networks, 10
industrial protocols, 10
lifecycle, 262
malware, 11
North American Electric Reliability Corporation (NERC) CIP regulations, 19
operational security, 210
procurement language, 334
risk identification, 210
risk reduction, 210
Cyber security evaluation tool (CSET), 220–222
Cyber terrorism, 53
Cyber-threat, 9
Cyber threat, evolution of, 44
Code Red, 44
Conficker, 44
marconi wireless telegraph system, 44
Morris worm, 44
Slammer, 44
Stuxnet, 44
Cyber war, 4, 11, 39, 49, 53, 253
information targets, 49
Cyber warfare, 50

D

DAMs. *See* Database activity monitors (DAMs)
Dashboards, 68
Dashboards utilizing technologies, 75
Database activity monitors (DAMs), 368
kismet, 368
snort, 368
wireshark, 368
Database injection, 46
Data collection, 227
hardware and software inventory, 227
industrial networks scanning, 227

Data diodes and unidirectional gateways, 308, 309
fiber-optic connection, 308
Data enrichment, 343
contextual information collection, 344
log management system based scrutiny, 344
Data flow analysis, 240
Data historian systems, 67, 73, 74, 353
application monitor, 75
OSIsoft, and, 68
unidirectional gateway, 75
vendors, 67
Data link layer segmentation, 100
Data monitoring methods, 352
monitoring by zones, 352
DCOM. *See* Distributed component object model (DCOM)
DCS. *See* Distributed control system (DCS)
Deep packet inspection, 113
Deep-packet inspection (DPI), 291–293
Deep packet inspection (DPI) system, 13
DEFCON, information security conferences, 213
Demilitarized zone (DMZ), 23, 286
Denial-of-service attacks, 187
Loss of Control (LoC), 187
Loss of View (LoV), 187
Department of energy (DoE), 304
Department of Homeland Security (DHS), 334, 387, 396
penetration test, 397
DHCP. *See* Dynamic host configuration protocol (DHCP)
DHS. *See* Department of Homeland Security (DHS)
Direct monitoring, 368
Distributed component object model (DCOM), 150
Distributed control system (DCS), 1, 14, 15, 219
architectures, 87
Distributed network protocol (DNP), 130
Distributed network protocol 3 (DNP3), 130, 133, 134, 409
industrial network architecture, within, 137
protocol, 265
security concerns, 136
security recommendations, 138
users group, 409
DistTrack. *See* Shamoon
DMZ. *See* Demilitarized zone (DMZ)
DNP. *See* Distributed network protocol (DNP)
DNP3. *See* Distributed network protocol 3 (DNP3)
DNS. *See* Domain name system (DNS)
DoE. *See* Department of energy (DoE)
Domain name system (DNS), 235
Domain servers, 106
DPI. *See* Deep packet inspection (DPI)
DREAD model, consequence estimation, 254, 255
DTP. *See* Dynamic trunking protocol (DTP)
Dual-homing, 94
vendor reference architecture, in, 95
Dynamic host configuration protocol (DHCP), 235, 344
Dynamic trunking protocol (DTP), 102

E

EFI. *See* Electromagnetic interference (EFI)
Electromagnetic interference (EFI), 130
Electronic security perimeter (ESP), 10
Cloud, 26
North American Electric Reliability Corporation (NERC) CIP regulations, 24
permieter, definition of, 24
permieter security, 26
EMS. *See* Energy management systems (EMS)
Enclaves, 22
Energy management systems (EMS), 118
Engineering workstation (EWS), 189
ENISA. *See* European Union agency for network and information security (ENISA)
Enterprise networks, 20
Enterprise security, 2
ESP. *See* Electronic security perimeter (ESP)
EtherCAT, 147
security concerns, 147
security recommendations, 148
Ethernet, 2, 88, 94, 96, 121, 127, 141, 144, 148, 161, 230
implementation, real-time methods, 142
Ethernet industrial protocol, 142
control and information protocol (CIP), 142
EtherNet/IP (EIP), 143
EtherNet/IP zone protection, 145
security concerns, 144
security recommendations, 144
Ethernet/IP protocol, exploitation of, 199
control processing unit (CPU) crashing, 199
device boot code, dumping of, 199
device crashing, 199
device resetting, 199
flash updating, 199
system, stopping of, 199
Ethernet network design, 90
Ethernet POWERLINK, 148
security concerns, 148
security recommendations, 149

Ethernet, redundancy in, 90
vendor reference architecture, 90
European Union Agency for Network and Information Security (ENISA), 214, 387
Event correlation, 341, 342
correlation rules comparing, 341
event streams, analysis of, 341
examples of, 343
pattern recognition, 341
Event normalization, 344, 345
EWS. *See* Engineering workstation (EWS)
Exception reporting, 5, 324, 325
Exploitation of functionality, 198
Exploits, 6, 11, 157, 194, 314
External controls, 316

F

False positives, definition of, 354
Federal Energy Regulatory Commission (FERC), 388, 411
nuclear facilities, 27
Federal information processing standards (FIPS), 388, 399, 405
Federal information security management act (FISMA), 38, 388
Feedback loops, 73
FERC. *See* Federal Energy Regulatory Commission (FERC)
Fieldbus network, 91
ControlNet, 91
DeviceNet, 91
FOUNDATION Fieldbus, 91
PROFIBUS-PA, 91
Fieldbus protocols, 122, 123
distributed network protocol (DNP3), 122
Modicon communication bus (Modbus), 122, 123
File integrity monitoring (FIM), 358
File system logs, 358
FIM. *See* File integrity monitoring (FIM)
FIPS. *See* Federal information processing standards (FIPS)
FIPS 140-2 standards, 405
Firewalls, 11, 13, 42, 104
configuration guidelines, 293, 296
zones establishment, 299, 300
creation of, 289
FIRST. *See* Forum of Incident Response and Security Teams (FIRST)
FISMA. *See* Federal Information Security Management Act (FISMA)
Flamer. *See* Skywiper
Forum of Incident Response and Security Teams (FIRST), 252
Functional groups, 22, 31, 266, 268, 277
basic process control, 266
control data storage, 266
malware protection, 266
peer-to-peer control processes, 266
remote access, 266
supervisory controls, 266
trading communications, 266

G

Gaphical user interface (GUI), 76
GCI. *See* General client interface (GCI)
General client interface (GCI), 108
GPS network, 116
Graphical user interfaces (GUIs), 14
GUIs. *See* Graphical user interfaces (GUIs)

H

Hacking methodologies, 6
Hacktivism, 45, 53
Hardware and software inventory, 239
endpoints, 239
HART communication protocol, 108
Hazards and operability analysis (HAZOP), 210
HAZOP. *See* Hazards and operability analysis (HAZOP)
HIDS. *See* Host IDS (HIDS)
Higher layer segmentation, 99
HIPS. *See* Host IPS (HIPS)
HMIs. *See* Human-machine interfaces (HMIs)
Home energy management systems (HEMS), 80
Homeland security presidential directive seven (HSPD-7), 26
bulk electric, 28
utilities, listed, 26
Host cyber security systems, 311
Host firewall, 313
Host IDS (HIDS), 311–313
Host IPS (HIPS), 314
Host security and access controls, implementing of, 309
external controls, 316
security information and event management systems, 316
HSPD-7. *See* Homeland security presidential directive seven (HSPD-7)
Human-machine interface (HMI), 14, 64, 66, 73, 76, 268, 337, 352
console, 189

I

IACS. *See* Industrial automation and control system (IACS)
IAM. *See* Identity and access management (IAM); Identity and authorization management (IAM)
ICCP. *See* Inter-control center communication protocol (ICCP); Inter-control center communications protocol (ICCP)
ICMP. *See* Internet control message protocol (ICMP)
ICS. *See* Industrial control systems (ICS)
ICS application software, 334
ICS assessments, 396, 397
ICS-CERT. *See* Industrial Control System Cyber Emergency Response Team (ICS-CERT)
ICSs. *See* Industrial control systems (ICSs)
Idaho national lab (INL), 304
Identity and access management (IAM), 272, 334, 364
  NetIQ, 364
  oracle identity management, 364
  securonix identity matcher, 364
  tivoli identity, 364
Identity and authorization management (IAM) systems, 218
  microsoft active directory, 218
  RADIUS, 218
IDS. *See* Intrusion detection system (IDS)
IDS/IPS configuration guidelines, 295, 300
  ipvar variables, 299
  portvar variable, 299
  sourcefire example, 298
    snort protocol, 298
  suricata engine, 298
  var command, 299
IDS/IPS rules, recommended, 301
IEC. *See* International Electrotechnical Commission (IEC)
IEC60870-6. *See* Inter-Control Center Communications Protocol (IEC60870-6)
IEC-62264 standard, 263
IEC-62443 standard, 261
IEC 61508/61511 standards, 210
IEDs. *See* Intelligent electronic devices (IEDs)
Incident response, 381
Indsutrial control system (ICS) architectures, 2
Indsutrial control system (ICS) designs, 2
Industrial activity reports, 379, 380
Industrial application layer attacks, 198
Industrial applications, 198
  data historians support multiple methods, 75
  layer attacks, 198, 199
Industrial assets security, 41
Industrial automation and control system (IACS), 14, 392
Industrial Control System Cyber Emergency Response Team (ICS-CERT), 191, 220
Industrial control systems (ICS), 1, 9, 11, 14, 41, 387
  architectures, 4, 121
    publish-subscribe, 92
    token-rings, 92
  compromised, 172
  cyber-attacks on, 171
  deployment errors, 6
  distributed control system (DCS), 14
  errors of complacency, 6
  fundamentals, 4
  graphical user interfaces (GUIs), 14
  human–machine interfaces (HMIs), 14
  misconfigurations, 6
  mistakes, 6
  network connectivity, 16
  network design, 4
  nonroutable areas, 19
  operational aspects of, 52
  operations, 4
  pitfalls, 6
  process control system (PCS), 14
  protocols, modified
    DNP3 over TCP/UDP, 18
    Modbus over TCP/IP, 18
    Modbus/TCP, 18
  routable areas, 19
  safety instrumented system (SIS), 14
  supervisory control and data acquisition (SCADA) system, 14
  vendors, 67
  vulnerabilities, 51
Industrial cyber security, 3, 4
Industrial ethernet, 141
  protocols, 141
Industrial firewall implementation, 7
Industrial network cyber security, 9
Industrial networking, 9, 87
  Ethernet based, 87
  Internet protocol (IP) based, 87
Industrial network protocols, 4, 75, 121
  CIP, 4
  DNP3, 4, 75
  Foundation fieldbus HSE, 4

ICCP, 4
Modbus, 4, 75
OPC, 4, 75
PROFIBUS, 75
Profibus, 4
Profinet, 4
Wireless HART, 4
Zigbee, 4
Industrial networks, 2, 4, 15, 21, 85, 171, 213, 219
business networks, comparison between, 88
common topologies, 92
components availability, 220
data communication integrity, 220
functional demarcation, 82
human health, 220
industrial control systems (ICS), components of, 59
logical assets, 225, 226
network topologies, 93
Industrial network security, 41
2010 Black Hat USA conference, 44
need for improvement, 41
Red Tiger Security, research by, 43
regulatory compliance standards, 6
vulnerability, 44
Industrial network security, documents of, 412
ANSI/ISA-99.00.01-2007, 412
ANSI/ISA-99.02.01-2009, 412
ANSI/ISA-TR99.00.01-2007, 412
ISA-99, 412
Industrial network security mapping, 395
compensating controls, use of, 396
Industrial network security, misperceptions of, 36
cyber security, 36–37
Industrial networks scanning, 228
device scanners, 228
network mapper (nmap), 228
traffic scanners, 229
tcpdump for Linux, 229
windump for Windows, 229
wireshark dissectors, 230
microsoft message analyzer, 231
vulnerability scanners, 229
Industrial network tuning, 355
Industrial protocol (IP), 338
filtering, 7
Industrial protocols, 3, 16
open systems interconnection (OSI) model, 17
TCP/IP model, 17, 18
Industrial protocols, history-oriented, 75
OPC historical data access (OPC-HDA), 75
Industrial protocol simulators, 164
distributed network protocol 3 (DNP3), 165
inter-control center communications protocol (ICCP), 165
Modbus, 165
object linking and embedding (OLE) for process control (OPC), 165
physical hardware, 166
Industrial security recommendations, 29
access control, 34
advanced, 34
user authentication, 35
critical systems, identification of, 29
critical assets, NRC's logical map for, 30
NERC CIP, 29
defense-in-depth, 32
functional zones, topological layers of, 37
open systems interconnection (OSI) model, 37
policy layers, 37
protective measures, 34
subnetworks, topological layers of, 37
network segmentation, 31
systems, isolation of, 31
critical services, 31
demilitarized zones (DMZs), functional, 31
functional groups, separation of, 32
service segmentation methods, 32
Industrial security recommendations, advanced, 35
application whitelisting, 36
policy whitelisting, 36
security monitoring, 36
Industrial systems
initial vectors, 46
legacy devices, 42
legacy protocols, 42
Industrial systems risks, 210
hacktivists group, 210
on-site control systems engineer, 210
package equipment supplier, 210
people's liberation army unit 61398, 210
vendor site support specialist, 210
Inferred monitoring, 369, 371
Information collection and management tools, 370
data historians, 374
log management systems, 372, 373
security information and event management systems, 372, 374
splunk security operation center, 373, 375
syslog aggregation, 371
Information security, 2
INL. *See* Idaho national lab (INL)
Institute for Security and Open Methodologies, 398
Integrated control systems, 319
Intelligent electronic devices (IEDs), 64, 98, 268, 352

Inter-control center communications protocol (ICCP), 157
industrial control system (ICS)-aware intrusion protection system, 162
industrial network architecture, within, 160
monitoring of, 161
protocol operation, 159
security concerns, 159
security recommendations, 160
uses of, 159
International Electrotechnical Commission (IEC), 158, 390, 413
International Organization for Standardization (ISO), 211, 214, 387
International Society of Automation, 388
International Standards Association (ISA), 412
International Standards Organization (ISO), 413
Interner relays, 62
Internet control message protocol (ICMP), 228
Internet protocol (IP), 2
networks, 121
Intrusion detection, 303
anomaly based, 303
Intrusion detection system (IDS), 13, 353, 405
Intrusion prevention system (IPS), 131, 139, 162, 324, 405
Intrusion prevention systems (IPS), 13
IP. *See* Industrial protocol (IP); Internet protocol (IP)
IPS. *See* Intrusion prevention system (IPS)
ISA. *See* International Standards Association (ISA)
ISA 95 model, 291
ISA-62443 security standards, 275
ISA 62443 standard, 288, 392–394
group 1, 393
group 2, 394
group 3, 394
group 4, 395
ISA-62443 zone and conduit model, 22
block diagram, 22
network diagram, 23
ISO. *See* International Organization for Standardization (ISO)
ISO/IEC 27002 standard, 390
ISO 27000 standard, 288
series, 390, 391
IT/OT metrics, analysis of, 332
IT/OT systems correlation, 347, 348

J

Java database connectivity (JDBC), 75
Jitter, 111

K

Keyboard video mouse (KVM) switching system, 68
Key performance indicator (KPI), 210
KPI. *See* Key performance indicator (KPI)

L

Latency, 87, 111, 315, 374
Layer 2 network segmentation, 105
Layer 4-7 segmentation, 100
LDAP. *See* Lightweight directory access protocol (LDAP)
Lightweight directory access protocol (LDAP), 334, 363
Liquefied natural gas (LNG), 388
Live host identification, 231
scanning techniques, 231, 234
noisy/dangerous, 232
port mirroring, 232
quiet/friendly, 231
span ports, 232
LNG. *See* Liquefied natural gas (LNG)
Log collection, 368
Logical assets, 11
Logical network boundaries, 266
layer 3 device, 266
rule sets, 266
Logical segmentation, 104, 105
Logon format, 345
Log storage and retention, 382, 383
data availability, 384
data retention, 382
nonrepudiation, 382
write once read many (WORM) drives, use of, 382

M

Malware, 45, 46
social networking, and, 200
Malware infection, dealing with, 203
disk images, cloning of, 203
engineer-detected malware, reversing of, 203
infection detection, 203
logs analysis, 203
memory analysis, 203
monitoring, 203
safe and reliable manufacturing process, 203
sandbox, 203
Malware infections, advanced, 204
Malware mutations, 202
Malware, weaponized, 47, 48

Mandiant's Memoryze, 204, 205
Man-in-the-middle (MitM) cyber attacks, 174, 186
Master boot record (MBR), 225
Master terminal unit (MTU), 63
MBR. *See* Master boot record (MBR)
MBSA. *See* Microsoft baseline security analyzer (MBSA)
MDMS. *See* Meter data management system (MDMS)
Mesh networks, 92
Mesh topologies, 94
Metasploit Framework, 50
Meter data management system (MDMS), 118
Microsoft active directory, 363
Microsoft baseline security analyzer (MBSA), 249
MitM cyber attacks. *See* Man-in-the-middle (MitM) cyber attacks
Modbus. *See* Modicon communication bus
Modbus+. *See* Modbus Plus
Modbus ADU, 127
Modbus ASCII, 126
Modbus organization, 409
Modbus Plus (Modbus+), 126, 127
Modbus protocols, 409
Modbus RTU, 126
Modbus TCP, 127, 128
Modbus/TCP traffic, 355
  cisco discovery protocol, 356
  internet control Message protocol, 356
  internet group management protocol, 356
  internet protocol version 6, 356
  link layer discovery protocol, 356
  link-layer multicast name resolution, 356
  multicast DNS, 356
  web services discovery protocol, 356
  windows NetBIOS traffic, 356
Modicon communication bus (Modbus), 122–125
  application layer messaging protocol, 123
  Data Requests, 126
  Function Codes, 124
  industrial network architecture, within, 128
  layer 7 protocol, 123
  Modbus ADU, 127
  Modbus ASCII, 126
  modbus frame, 124
  Modbus over TCP/IP, 127
  Modbus Plus, 126, 127
  modbus protocol transaction, 125
  Modbus RTU, 126
  Modbus TCP, 127, 128
  protocol data units (PDUs), 123
  security concerns, 129
    authentication, lack of, 129
    broadcast suppression, lack of, 129
    encryption, lack of, 129
    message checksum, lack of, 129
  security recommendations, 129
  variants, 126
Monitoring user identities, 362
MTU. *See* Master terminal unit (MTU)
Multihoming, 94

N

NAS. *See* Network attached storage (NAS)
National Institute of Standards and Technology (NIST), 214, 387, 392
National Petrochemical and Refiners Association (NPRA), 398
National Security Agency, 397
National Vulnerability Database (NVD), 247
NBAD. *See* Network Behavior Anomaly Detection (NBAD)
NERC. *See* North American Electric Reliability Corporation (NERC)
NERC CIP. *See* North American Reliability Corporation Critical Infrastructure Protection (NERC CIP)
Network architecture, 82
Network attached storage (NAS), 270
Network behavior anomaly detection (NBAD), 326, 365
Network diagrams, 2
Network flows, 361
Network hops, 113
Network layer segmentation, 100
Network management systems (NMSs), 75
Network performance, 111
  bandwidth, 111
  jitter, 111
  latency, 111
  throughput, 111
Network perimeters, 24
Networks
  connectivity, 266
    functional groups, definition of, 268
    network segmentation, 266
  division of, 99
    absolute, 99
    bidirectional, 99
    conditional, 99
    unidirectional, 99
  nonroutable networks, 18
    DNP3, 18
    fieldbus, 18
    Modbus/RTU, 18

Networks *(cont.)*
routable networks, 18
AppleTalk, 18
DECnet, 18
Novell IPX, 18
security controls, 263
access control lists (ACLs), 263
firewalls, 263
IPS devices, 263
network IDS, 263
segmentation in industrial systems, 98. *See also* Network segmentation
traffic, analysis of, 113
whitelisting, 99, 194
Network security controls, 78, 113, 290
application monitors, 290
industrial protocol filters, 290
network whitelisting devices, 290
Network segmentation, 85, 86, 96–98, 287
business networks, 98
local control networks, 98
methods, 102
application layer, 103
benefits of, 103
DataLink layer, 103
network layer, 103
physical layer, 103
session layer, 103
operations networks, 98
plant control networks, 98
process networks, 98
public networks, 98
safety networks, 98
supervisory control networks, 98
Network segregation, 24
conduits, 24
zones, 24
Network services, 106
directory services, 106
domain services, 106
identity and access management (IAM), 106
principle of least route, 106
Network statistics commands, 236
process identification (PID), 236
Next-generation firewalls (NGFW), 52
NGFW. *See* Next-generation firewalls (NGFW)
Night Dragon, 49
command and control (C2) servers, 49
remote administration toolkits (RATs), 49
NIST. *See* National Institute of Standards and Technology (NIST)
NIST SP 800-82 standard, 392
Nmap scripting engine (NSE), 228
Nonroutable networks, 18, 19
Normalization process, 343
North American Electric Reliability Corporation (NERC), 12, 276, 286, 387
bulk electric, 27
CIP regulations, 19
nuclear facilities, 27
North American Electric Reliability Corporation Critical Infrastructure Protection, 351
North American Reliability Corporation, 411
North American Reliability Corporation Critical Infrastructure Protection (NERC CIP), 411
reliability standards, 389
critical infrastructure security, 389
NPRA. *See* National petrochemical and refiners association (NPRA)
NRC. *See* Nuclear Regulatory Commission (NRC); United States Nuclear Regulatory Commission (NRC)
NRC regulation 5.71 standard, 392
NSE. *See* Nmap scripting engine (NSE)
Nuclear Regulatory Commission (NRC), 262, 288, 387
nuclear facilities, 27
NVD. *See* National Vulnerability Database (NVD)

O

Object linking and embedding (OLE), 150
Object linking and embedding database (OLEDB), 75
Object linking and embedding (OLE) for process control (OPC), 150–152, 157
client–server communications, 153
foundation, 409
industrial control system (ICS)-aware intrusion protection system, 157
industrial network architecture, within, 154
protocol, 409
operation, 152
security concerns, 155
legacy authentication services, 156
OPC server integrity, 156
RPC vulnerabilities, 156
security recommendations, 156
uses of, 154
OISF. *See* Open information security foundation (OISF)
OLE. *See* Object linking and embedding (OLE)
OneWireless, 108
On-site control system engineer, 212
OPC. *See* Object linking and embedding (OLE) for process control (OPC)
Open database connectivity (ODBC), 75
Open information security foundation (OISF), 298
Open source intelligence (OSINT), 46

Open source security information management (OSSIM), 370, 377
Open-source security testing methodology manual (OSSTMM), 398
Open source vulnerability database (OSVDB), 53
Open-source vulnerability database (OSVDB), 247
Open systems interconnection (OSI) model, 17, 18, 45, 86, 230, 287
  layers of, 99
Operational technology (OT), 352
OSI. *See* Open systems interconnection (OSI)
OSINT. *See* Open source intelligence (OSINT)
OSIsoft, 67., 68, 76, 251, 379
OSSIM. *See* Open source security information management (OSSIM)
OSSTMM. *See* Open-source security testing methodology manual (OSSTMM)
OSVDB. *See* Open source vulnerability database (OSVDB)
OT. *See* Operational technology (OT)

P

Passive logging, 368
Passive monitoring, 299
Patch management, 316
  security conduit establishment, 317
  vulnerability management, 316, 318
Patch management strategy, 303
PCS. *See* Process control system (PCS)
PDF. *See* Portable document format (PDF)
PDU. *See* Protocol data units (PDU)
Penetration testing tools
  CANVAS, 53
  Metasploit, 53
Penetration testing utilities, 44
  Backtrack, 44
  Metasploit, 44
PHA. *See* Process hazard analysis (PHA)
Physical assets, 11
Physical-layer controls, 104
Physical layer segmentation, 100
Physical-layer separation, 104
Physical security, 11, 41, 42
  air gap separation, 42
Physical segmentation, 104
Physical separation of systems, 104
Plant level control processes, 268, 270
  integration levels, 268
Plant safety design, protection layers, 79
PLCs. *See* Programmable logic controllers (PLCs)
PLR. *See* Programmable logic relays (PLR)
Policy whitelisting, 36
Port's VLAN ID (PVID), 96
Predeployment testing, 319
Principle of least privilege, 107, 261
Principle of least route, 107, 261
Printers, 69
Print servers, 69
Process automation, 319
  integrated control systems, 319
Process control system (PCS), 14, 26, 78
Process fieldbus (PROFIBUS), 139
  fieldbus message specification (FMS), 139
  PROFIBUS DP, 139, 140
  PROFIBUS PA, 139
  PROFIdrive, 139
  PROFINET, 139
  security concerns, 140
  security recommendations, 141
Process hazard analysis (PHA), 210
Process networks, 105
Production information management, 73
PROFIBUS. *See* Process fieldbus (PROFIBUS)
PROFIBUS isochronous real time (IRT), 146
PROFINET, 146
  implementation, 146
  security concerns, 147
  security recommendations, 147
Programmable logic controllers (PLCs), 59, 98, 352
  components of, 60
  ladder diagrams (LD), 60
  ladder logic, 61, 62
  operational flow diagram, 63
  sequential function charts (SFC), 62
Programmable logic relays (PLRs), 59
Protocol anomaly detection, 305
Protocol data units (PDU), 337
Protocol filtering, 99
Protocol monitoring, in industrial networks, 305
  application data monitors, 305
  industrial security devices, 305, 306
  secure crossing zenwall access control module, 305
  session inspection, 305
  tofino security appliance, 305
Protocols, device uses in industrial networks, 274, 275
Purdue reference model, 45
Purpose-built network, 107

Q

QFD. *See* Quality function deployment (QFD)
Quality function deployment (QFD), 256
Quality of service (QoS), 112
Query, 377
  event correlation editor, 378, 379
  incident query, 378, 379
  user activity filtration, 378

R

RAS. *See* Remote access servers (RAS)
RATs. *See* Remote administration toolkits (RATs)
RBAC. *See* Role-based access control (RBAC)
RBPSs. *See* Risk-based performance standards (RBPSs)
Real-life vulnerabilities, 7
Redhat Linux system, 356
Red Tiger Security, 43
Regulatory compliance standards, 6
  CFATS, 6
  CIP, 6
  ISA 62443, 6
  ISO /IEC 27002:2005, 6
  NERC, 6
  NIST 800-53, 6
  NIST 800-82, 6
  NRC RG 5.71, 6
Regulatory guide (RG), 412
Relational database management system (RDBMS), 68
Reliability standards, 388
Remote access, 108, 272, 273
  application layer firewalls, 272
  attack vectors, and, 109
  end-point policy enforcement, 272
  external conduit zones, 272
  industrial control systems (ICS), and, 108
  point-to-point authorization, 272
  risks of, 109
  security controls, 109
  trusted conduit zones, 272
Remote access servers (RAS), 272
Remote access toolkit (RAT), 190
Remote administration toolkits (RATs), 49
Remote procedure calls (RPC), 85
  protocol, 150
Remote terminal units (RTUs), 63, 98, 268, 352
Replay attacks, 188
Repository for industrial security incidents (RISI), 45
Repository of industrial security incidents (RISI), 53
RG. *See* Regulatory guide (RG)
Ring topologies, 94
RISI. *See* Repository for industrial security incidents (RISI)
Risk assessment, 5
Risk assessment methodologies, 215, 216
Risk-based performance standards (RBPS), 389
  metric 8 standard, 389
  metric 8.2.1 standard, 389
  metric 8.3 standard, 390
  metric 8.5 standard, 390
  metric 8.8 standard, 390
Risk-based performance standards (RBPSs), 412
Risk classification and ranking, 253
  consequences, 253, 254
    estimation strategies, 254
Risk management, 5, 210, 214
  event containing, 211
  operational security, 213
  security flaws identification, 211
  standards, 213, 215
  vulnerabilities identification, 211
Risk mitigation, 37, 210
Risk ranking, 256
Risk reduction, 257
Risks, 211
  definition of, 211
Risk tolerance, 210
ROC800L liquid hydrocarbon remote controller, 65
Role-based access control (RBAC), 273
Routable networks, 18, 19
RPC. *See* Remote procedure calls (RPC)
RTUs. *See* Remote terminal units (RTUs)
Rule-less detection systems, 304
  threshold rule, 304

S

Safety instrumented systems (SIS), 14, 78, 85, 114, 173
  principle of least privilege, 115
  probability of failure on demand (PFD), 114
  safety integrity level (SIL), 114
Safety integrity level (SIL), 275
Safety level, 264
Safety systems, 115
  logic solvers, 115
SAN. *See* Storage area networks (SAN)
SCADA. *See* Supervisory control and data acquisition (SCADA)
SDEE. *See* Security device event exchange protocol (SDEE)
SDLC. *See* Secure development lifecycle (SDLC)
Secure development lifecycle (SDLC), 395
Secure distributed network protocol 3 (DNP3), 133–135
Security
  assessment, 3
    threats, 244
  audits, 218
  awareness, 201
  breach, 220
  conduits, 261
    classification of, 264

definition of, 262
identification of, 264
countermeasures, 12
device configurations, 288
events, 353
false positives, 353
rationalization, 353
information management, 376
level, 264
lifecycle, 257, 276
achieved security level, 276
capability security level, 276
foundation requirements (FR), 276
requirement enhancements (RE), 276
system requirements (SR), 276
target security level, 276
monitoring, 36
tools, 201
plan, 201
practices, 37
tests. *See* Security tests
vulnerability assessments, 218
zones, 261, 264
goals establishment, 264
communication, 264
physical access to assets, 264
logical, 261
monitoring, 367, 376
physical, 261
separation, 265
business zones, 265
control zones, 265
zones establishment, 277
assets allocation, 278
communication assets assigning, 278
security conduits documentation, 279
technology, allowing of, 278
threats evaluation, 278
vulnerabilities evaluation, 279
Security controls, 12, 105, 109
anomaly detection systems, 111
application control, 110
attack vectors, minimizing of, 110
defense-in-depth, 110
demilitarized zone (DMZ) security, 110
network-based security control, deployment of, 110
principle of least privilege, 110
secured application server, 110
security information and event management systems (SIEMs), 110
Security device event exchange protocol (SDEE), 369
Security information and event management systems (SIEMs), 5, 75, 288, 326
Security policy development, 288
Security tests, 216, 217
ethical hacking, 217
penetration test, 217
definition of, 220
vulnerabilities, discovering of, 216
Security vulnerability assessment (SVA), 398
Segregation methodologies, 97
Sequential function charts (SFC), 62
SERCOS. *See* Serial real-time communications system (SERCOS)
Serial real-time communications system III (SERCOS III), 149
security concerns, 150
security recommendations, 150
Service level agreements (SLA), 216
SET. *See* Social engineering toolkit (SET)
SFC. *See* Sequential function charts (SFC)
Shallow packet inspection, 291
Shamoon, components of, 195
dropper, 195
reporter, 195
wiper, 195
SIEM. *See* Security information and event management (SIEM)
SIEM dashboard, 364, 365
SIL. *See* Safety integrity level (SIL)
SIS. *See* Safety instrumented system (SIS)
Situational awareness, 5
Skywiper, modules in, 195, 196
flame, 196
frog, 196
gadget, 196
munch, 196
suicide, 196
telemetry, 196
viper, 196
weasel, 196
SLA. *See* Service level agreements (SLA)
Smart grids, 3, 9, 24, 25, 28, 80, 162
deployment, components of, 80
network, 116
expanding attack surfaces, 117
scalability, 117
security concerns, 164
security recommendations, 164
threat targets, 81
threat vectors, 81
Smart lists, 338
definition of, 338
examples of, 339
process, 339, 340
Sneaker net, 335

Social engineering toolkit (SET), 198, 201
Social networking, 200, 201
  as malicious vector, 202
  sites, industrial networks, 200
Software development lifecycle (SDL), 254
SP99. *See* Standards and practices committee 99 (SP99)
SPC. *See* Statistical process control (SPC)
Spear-phishing, 46
  campaigns, targeted, 201
Split zones, 283, 284
SQC. *See* Statistical quality control (SQC)
SQL. *See* Structured query language (SQL)
Standards and practices committee 99 (SP99), 392
Star topologies, 94
Statistical process control (SPC), 73, 327
Statistical quality control (SQC), 73, 327
Storage area networks (SAN), 270
Structured query language (SQL), 377
Stuxnet, 12, 48, 50, 141, 191–194, 341
  infection processes, 192
  lessons learned from, 193, 194
Supervisory control and data acquisition (SCADA), 1, 9
  architectures, 87
  system, 14, 15
Supervisory controls, 268, 269
  human–machine interface (HMI), 268
Supervisory data, 74
Supervisory workstation, 67
SVA. *See* Security vulnerability assessment (SVA)
System assets, 59
  control system components
    human–machine interfaces (HMIs), 59
    intelligent electronic device (IED), 59
    programmable logic controllers (PLCs), 59
    remote terminal units (RTUs), 59, 63
  field components
    actuators, 59
    gauges, 59
    indicators, 59
    motor drives, 59
    sensors, 59
System availability management, 317
System characterization, 223
  entry points, 224, 225
  online, 223
  physical, 223
  trust boundary, 224
System logs, 356
System operations, 70
  business information management, 74
  control loops, 70
  control processes, 72
  feedback loops, 73
  production information management, 73

T

TASE. *See* Telecontrol application service element (TASE)
TASE.2. *See* Inter-control center communications protocol (TASE.2)
TCP/IP model, 17, 18
Telecontrol application service element (TASE), 158
Testing and assessment methodology establishment, 219
Theoretical assessment tests, 220
  physical, 221
    online *versus* offline, 221, 223
    white box *versus* black box, 222, 223
Threat actor, 212
Threat detection, 5, 340
  event correlation, 340
  local privileges elevation, 340
  persistent access, creating of, 340
  track covering leaving indicators, 340
Threat event, 212
Threat identification, 241, 242
  system characterization, 241
Threat sources, 212, 241, 242
  insider based, 212
    capability, 212
    opportunity, 212
Threat vectors, 243–245
Throughput, 112
Tiered correlation, 346, 347
Tiered segmentation, 105
Tofino industrial security appliance, 355
Tofino security appliance, 305
Topologies, 92
  bus, 92
  mesh, 92
  ring, 92
  star, 92
  tree, 92
Trading communications, 271
  Inter-control center communication protocol (ICCP), 271
Tree topologies, 94
Triangle microworks communication protocol test harness, 165
Trojanized ICS software, 313
Trojan virus, 314
Type of service (ToS), 112, 314

U

UCF. *See* Unified compliance framework (UCF)
Unified compliance framework (UCF), 396
Unified threat management (UTM), 290
  appliances, 13, 52
United States Department of Homeland Security (DHS), 412
United States Nuclear Regulatory Commission (NRC), 411
  RG 5.71, 412
  title 10 CFR 73.54, 411
Unmitigated risk, 210
US Department of Homeland Security (DHS), 43, 220, 222
Users, role of, 272, 274
User whitelists, 334
UTM. *See* Unified threat management (UTM)

V

Variable frequency drives (VFD), 191
Variable-length subnet masking (VLSM), 287
VFD. *See* Variable frequency drives (VFD)
Virtual LANs (VLANs), 96, 97, 267, 286
  ethernet packet header, 267
  segmentation, 102, 105
  vulnerabilities, 102
    dynamic trunking protocol (DTP), 102
    layer 2 attacks, 102
    switch spoofing, 102
    VLAN Hopping, 102
    VLAN trunking, 102
Virtual private networks (VPNs), 53, 87, 272, 283
VLANs. *See* Virtual LANs (VLANs)
VPNs. *See* Virtual private networks (VPNs)
Vulnerability assessments, 5, 218
Vulnerability identification, 246, 247
  man-in-themiddle (MitM) attacks, 246
Vulnerability management, 316, 318
Vulnerability prioritization, 251
Vulnerability scanners, 246
  host based, 249
  nessus, 248, 249
    example of, 251
  passive, 249
Vulnerability scanning, 246
  aggressiveness control, 249

W

WAP. *See* Wireless access point (WAP)
Waterfall security, protocol support, 308, 310
Watering hole, 46
W32.DistTrack. *See* Shamoon
Weaponized industrial cyber threats, 190
  shamoon, 195
  skywiper, 195
  stuxnet, 191
WFP. *See* Windows File Protection (WFP)
Wide area connectivity, 115
Wide area network (WAN), 115
  communication, 157
Wi-Fi, 69
  Bluetooth, 69
  wireless LAN (WLAN), 69
Window Management Instrumentation Command-line (WMIC), 236
Windows event collector, 356
Windows File Protection (WFP), 358
Windows management instrumentation (WMI), 236, 356
  example, 357
Wireless access, 107
Wireless access point (WAP), 283
WirelessHART, 108, 109
Wireless industrial networking, 108
  OneWireless, 108
  WirelessHART, 108, 109
Wireless mesh topologies, 94
Wireless networks, 4, 107, 266
  industrial control systems (ICS) architectures, and, 108
  technologies, 4
WMI. *See* Windows management instrumentation (WMI)
WMIC. *See* Window Management Instrumentation Command-line (WMIC)

X

xml files, 165, 232

Z

Zone and Conduit model, 5, 22, 261, 265
Zone criticality, 290, 291
Zone perimeter, 285
  demilitarized zone (DMZ), 286
Zones
  based on protocol use, 275
  defined by process, 267
  demilitarized zone (DMZ), 23
  ISA- 62443 standard, 22
Zone segmentation, 86, 97
  industrial control systems (ICS), and, 86