

Symbols

- @dynamic list, 153
- @dynamic variable, 143, 153
- @local variable, 143

A

- acceptable use
 - documents, 62–63
 - policies, 17
- access control rules
 - COM components, 155
 - data sets, 147–149
 - file sets, 149–152
 - network address sets, 142–145
 - network services sets, 145–146
 - registry sets, 158
- Access Control Server, 170
- actions
 - See* individual named actions
- ActiveX
 - controls, 104
 - Frame, 236–238, 243
- add to application class actions, 72
- administration
 - backing up databases, 376–378
 - exporting objects, 358–359
 - Help menu, 374–375
 - importing objects, 361
 - licensing, 355–356
 - parameters, 346
 - RBAC, 362
 - administrative control, 364
 - administrative preferences, 365–366
 - VMS rights, 362–364
 - registration control, 357–358
 - restoring databases, 378
 - restricting access, 364
 - roles, 364
 - Search menu, 367
 - all objects, 374
 - application classes, 372
 - groups, 369
 - hosts, 367
 - policies, 369–370
 - rules, 370–371
 - variables, 372
 - sharing components, 358
 - view preferences, 365
- Administrators user state set, 65
- agents
 - Agent Control Panel, 187–192
 - Status, 188–190
 - System Security, 191–192
 - Untrusted Applications, 192
 - agent kits, 49, 168
 - creating, 168–170
 - downloading, 177
 - installing, 171–179
 - components, 163–164
 - executable files, 78, 168
 - interaction rules, 306
 - interfaces
 - Linux, 200
 - Solaris, 200–201
 - Windows, 185–198
 - network shim, 170–171
 - policy manager, 164
 - registering, 355–357
 - self-protection, 77
 - software, updating 49, 179, 182
 - system 4.5, 358
 - uninstalling, 182–183
- agent service control rule, 77–78
- agent UI rule, 79–81, 306
- alerts, 227–229
 - alert events, 209
 - configuring, 227
 - creating, 349
 - customizing, 228
 - event sets, 225
 - geographic groups, 346
- All Linux mandatory group, 122
- All Solaris mandatory group, 122
- All Windows mandatory group, 122
- allow actions, 72
- analysis feature, Event Management Wizard, 327, 333
- anomaly detection, 16

Anonymous Login (Null Session) user state set, 65

Antivirus Installations report, 262–263

API rules, 306

applications

behavior investigation, 27, 275–276

analysis, 283, 300–306

classes, 305

configuring, 276–280

importing policy, 302

remote agents, 281–283

reports, 285–286, 297

terminating early, 280

timing, 279

UNIX, 299

builder rules, 136

classes, 125

behavior investigation, 305

built-in, 126, 131–133

configuring, 127, 130

dynamic, 133–136, 140

managing, 140

Search menu, 372

sharing components, 358

shell scripts, 140

static, 133–134

subprocesses, 130

system processes, 141

control, 25

control rule, 81–82

deployment investigation, 27, 55, 250–251

application mapping, 256

collecting data, 253

configuring, 251

data management, 260–261

groups, 251–255, 345

product associations, 255–257

reports, 262–273

unknown applications, 259–260

fingerprinting, 15

mapping, 256

unknown, 259–260

attacks

backdoor attacks, 14–15

blended threats, 8–11

day-zero attacks, 21

detecting, 15–16

DoS attacks, 7

insiders, 12–13

life cycles, 23–24

malicious code, 23

sneakernet, 15

spyware, 12

viruses/worms, 5–6

See also individual attack names

auditing, 232–233

audit log policies, 121

audit trails, 116, 232–234

reports, 233

automatic updates, 179

auto-pruning, 224

auto-start mechanisms, 10

availability, 312

B

backdoor attacks, 14–15

backups

Backup menu, 376

databases, 376–378

licenses, 378

Backup Operators user state set, 65

balloon messages, 186

Base Operating System Protection - Windows

policy, 323

behavior

analysis, 333

attack detection, based on 16

See also applications

Best Practices document, 338

bin directories, 198

blended threats, 8–9

delivery mechanisms, 9

destructive behavior, 11

propagation mechanisms, 9–10

scanning mechanisms, 9

buffer overflows, 104–106, 178

bulk transfers, groups, 48

bundled exploits, 9

C

- candy shell security, 14
- capabilities, 24–27
- challenge responses, 198
- changes (auditing), 233
- checksums, 16
- Cisco ACS (Access Control Server), 170
- Cisco Partners, 339
- Cisco Secure VPN Client, network shim, 171
- Cisco Security Agent, overview, 21–28
- Cisco Self-Defending Network Initiative, 169, 208
- Cisco Trust Agent, 26, 54, 169, 208
- Cisco Trust Agent Infected Posture system state set, 67
- CiscoWorks Common Services, 343
- CiscoWorks VPN/Security Management System.
 - See VMS server
- Citrix MetaFrame/XP 165
- clipboard access control rule, 82–83
- cloning, 315
 - components, 316
 - editing, versus, 329
 - rule modules, 111, 315
- CLSIDs, 155, 158
- cmd.exe, 81
- COM
 - component access control rules, 83–85, 179
 - component sets, 85, 155–158, 358
 - events, 290–291
 - objects, 83
- COM Object Extraction utility, 156
- command shells, 81–82
- communication, 29–31
- communication security, 167
- components, 27–29, 358
- confidentiality, 312
- Configuration Restoring Console, 378
- configure role, 364
- connection rate limit rule, 85–86
- consistency checks, 116
- correlation
 - engine, rules/events, 164
 - events, 25
- critical events, 209
- Crystal Report viewer, 236
- CSA (Cisco Security Agent), overview, 21–28
- csactl utility, 181, 201

- CSAgent folders, 174
- csalog.txt file, 77
- CSV reports, 297
- CTA (Cisco Trust Agent), 26, 54, 169, 208
- custom groups, 38
- custom programs, 228

D

- damaging payloads, 11
- data
 - access control rules, 86–87, 179
 - availability, 312
 - confidentiality, 312
 - history, 361
 - integrity, 312
 - sets, 147–149, 358
 - theft, 82
- databases
 - backing up, 376–378
 - CiscoWorks, 363
 - event logs, 212
 - MS SQL, 167
 - MSDE, 167, 343
 - restoring, 378
 - searching, 367
 - VMS user, 362
- day-zero attacks, 21
- DCOM (Distributed Component Object Model), 9
- default actions, 72–74
- denial-of-service attacks
 - See DoS attacks
- deny actions, 42, 71–72
- deploy role, 364
- Description field, 77
- Desktop - All Types group, 44, 47
- Desktop - Remote group, 47
- Detailed Description field, 77
- detect rules, 55
- detection
 - attacks, 15
 - application fingerprinting, 15
 - automation, 16
 - behavior-based attacks, 16
 - log file scraping, 15
 - signature-based attacks, 15
 - rules, 111

- Dialup user state set, 65
- directories, 88
 - backups, 376
 - bin, 198
 - log, 198
 - paths, 116
 - protecting, 26, 194
 - read/write operations, 287
 - Solaris, 177
 - Windows, 174
- Distributed Component Object Model (DCOM), 9
- distributed firewalls, 25
- DMP (dump) files, 335
- DNS (Domain Name Server), 343
- DoS (denial-of-service) attacks, 85
 - network shims, 171
 - worms, 7
- downloads
 - agent kits, 177
 - untrusted, 192
- drivers, 91, 108
- dump files, 335
- dynamic application classes, 133–136, 140
- @dynamic
 - list, 153
 - variable, 143, 153

E

- EAP (Extensible Authentication Protocol), 170
- echo response packets, 95
- edge security mechanisms, 14
- e-mail, 8
 - data theft, 82
 - hackers, 10
 - sniffers, 101
- emergency events, 209
- Enabled check box, 77
- encryption, 14
- enforcement
 - active enforcement, 62
 - Enforcement Mode, 41
 - agents, 349
 - rule modules, 113
 - rules, 55, 63, 111
- enhancements, 353
- error events, 209
- event logs, 77, 205, 210–212
 - alerts, 227
 - application behavior investigation, 282
 - axis labels, 209
 - correlating messages, 96
 - databases, 212
 - Event field, 216–218
 - Event Monitor, versus, 334–335
 - filtering, 212–213
 - filtering view, 328
 - fine-tuning policies, 328–329
 - interpreting, 214–215
 - managing, 223–224
 - remote agents, 283
 - syslog events, 109
 - troubleshooting, 57, 355
 - using, 214–215
 - verbose logging, 326
- Event Log Viewer, 214
- Event Management Wizard, 217, 330–334
- Event Monitor, 219
 - event logs, versus, 334–335
 - filtering, 219–222
- events
 - alerts, 209, 227–229
 - auto-pruning tasks, 224
 - axis labels, 209
 - COM, 290–291
 - correlation, 25
 - critical, 209
 - emergency, 209
 - errors, 209
 - event counts per day, 208–210
 - event sets, 225–226, 327
 - Event Monitor, 222
 - hosts, 226
 - policy rules, 226
 - predefined, 225
 - sharing components, 358
 - Events menu, 205
 - alerts, 227
 - Status Summary screen, 206–208
 - file events, 286
 - all events, 288–289
 - directory summary, 286–287
 - individual file summary, 287
 - UNIX, 299
 - filtering, 220, 288, 328

- informational, 209
- insertion tasks, 223–224
- local event manager, 164
- messages, 167
- network events, 293
 - all events, 294
 - destination port summary, 293
 - filtering, 294
 - UNIX, 299
- notice, 209
- registry, 289–290
- reporting, 235
 - by group reports, 238
 - by severity, 235–238
- suppressing, 220
- syslog, 109
- Test Mode, 216
- warning, 209
- Everyone user state set, 65
- exceptions
 - rules, 217, 330–334
 - handling routines, 104
- expiration date (demo), 355
- exploits, 9–10
- exporting objects, 358–359
- Extensible Authentication Protocol, 170

F

- false positives, 326
- file
- File interceptor, 164
- file servers, 7
- file version control rule, 90–91
- files
 - access control rules, 88–89, 149, 179
 - agent executables, 168
 - events, 286
 - all events, 288–289
 - directory summary, 286–287
 - individual file summary, 287
 - UNIX, 299
 - file sets, 149, 152
 - sharing components, 358
 - UNIX, 152
 - hosts, 167

- protecting, 26, 194
- sharing, 287
- RTR, 197
- XML, 359
- Filter Events window, 220
- filtering
 - audits, 232–234
 - data filters, 87
 - events, 288
 - event log, 212–213
 - Event Monitor, 219–220
 - event sets, 222, 225
 - Filter Events window, 220
 - host-associated events, 57
 - network events, 294
 - fine-tuning policy, 328
 - registry data, 290
 - user information, 42
- fingerprinting, applications, 15
- firewalls, 13
 - distributed, 25
 - end users, 25, 80
 - Linux, 200
 - personal rules, 163
- flags, 95
- floppy disks, 5–6
- foreign languages, 64–65
- functional groups, 345

G

- geographic groups, 345
- global reports, 27
- groups, 35–49
 - application deployment investigation, 251, 345
 - assigning membership, 56
 - bulk transfers, 48
 - changing membership, 47–48
 - comparing, 39
 - creating custom groups, 40–44
 - functional, 345
 - geographic, 345
 - Group Detail reports, 239
 - Host Detail reports, 239–241
 - hosts, 314
 - implementation plan, 344

- inheritance, 50
- mandatory, 36, 122, 315, 344
- modifying, 42
- policies, 122, 314
- Policy Detail reports, 241–243
- predefined, 36–37, 44–47
- reporting events, 238
- rule precedence, 122
- scaling, 37
- Search menu, 369
- servers, 346
- sharing components, 358
- Short Polling groups, 345
- Software Update groups, 345
- SIDs (Windows), 64
- Test Mode, 41, 345
- types, 35–38
- user state sets, 347
- Verbose Logging Mode, 41
- viewing, 38–40
 - associated events, 49
 - event log, 212–213
 - membership, 47–48
 - related events, 42
- Guest user state set, 65
- GUIs (graphical user interfaces). *See* interfaces

H

- hackers, 10
- hard drives, 165–166
- Help menu, 374–375
- HIDS (Host Intrusion Detection System), 22
- hierarchy, CSA components, 313
- high priority
 - deny actions, 72
 - terminate process deny actions, 71
- hint messages, 30, 41, 327
- HIPS (Host Intrusion Protection System), 22
- history, 361
- hives
 - registry sets, 158
 - writing to, 98
- Host Detail reports, 239–241
- Host Intrusion Detection System (HIDS), 22
- Host Intrusion Prevention System (HIPS), 22
- hosts, 35, 49–57, 314

- application deployment investigation, 253, 345
- changing group membership, 56
- conflicting rules, 73
- event sets, 226
- Host Detail reports, 239–241
- inheritance, 50
- limiting connections, 85
- network shims, 170
- policies, 122
- polling intervals, 51–52
- Search menu, 367
- Test Mode, 52, 345
- troubleshooting, 57
- updates, 207
- viewing
 - configuration, 50
 - group membership, 48
 - host-associated events, 57
- working with, 52–55
- hosts file, 167
- hotfixes
 - CTA, 169
 - displaying, 264
- HTML Frame, 236–237, 243
- HTTP (Hypertext Transfer Protocol)
 - blended threats, 9
 - MC communication, 30
- HTTPS (Hypertext Transfer Protocol Secure)
 - blended threats, 9

I

- ICMP (Internet Control Message Protocol), 95
- IDS (Intrusion Detection System), 13, 348
- implementation plan, 337–338, 352
 - CiscoWorks Common Services, 343
 - future enhancements, 353
 - groups, 344
 - network shim, 341
 - project phases, 338–339
 - continuing evolution, 353
 - implementation phase, 352
 - pilot phase, 350–352
 - planning, 339
 - testing, 339–350
 - training, 339
- users, 350

- importing objects, 361
- informational events, 209
- inheritance, 50, 55
- insider attacks, 12–13
- installation, 164
 - agent kits, 168
 - creating, 168–170
 - installing, 171, 177–179
 - network shim, 170–171
 - rebooting, 178–179
 - uninstalling, 182–183
 - updating software, 179, 182
 - CSA MC, 166–167
 - MSDE database, 166–167
 - quiet/nonquiet installs, 169
 - requirements, 165–167
- Installation Application policy, 121
- Installation Process Detected system state set, 68
- Installed Products report, 263–264
- Instant Messenger policy, 324–325
- integrity, 312
- interaction, user 344
- interceptors, 164
- interfaces
 - Linux, 200
 - Solaris, 200–201
 - Windows, 185
 - Agent Control Panel, 187, 190–192
 - audible notifications, 195
 - directories, 198
 - firewalls, 193–195
 - GUI, 187, 190–192
 - Programs menu, 196–198
 - stopping, 199
 - system tray options, 186–187
 - tools, 198
 - tray icon, 186
 - user interaction, 198
- Internet Control Message Protocol (ICMP), 95
- IDS (Intrusion Detection Sensor/System), 13, 348
- IP (Internet Protocol)
 - blended threats, 9
 - Morris worm, 7
 - stack-hardening mechanisms, 94
- IP addresses, 93
 - agent resolution, 166
 - Linux, 166

- network address sets, 142
- quarantined, 152
- Solaris, 166
- system state sets, 68
- Unprotected Hosts report, 270
- Windows, 165
- Intrusion Prevention System, 22
- IPSec VPN tunnels, 14

K–L

- kernel protection rule, 91–93
- known vulnerabilities, 90
- Learning Mode, 194
- LIBC routines, 105
- licenses, 355–356
 - backups, 378
 - VMS server, 356
- life cycles, attacks, 23–24
- Linux
 - agents
 - agent kits, 177–178, 183
 - components, 164
 - interface, 200
 - buffer overflows, 178
 - CSA installation requirements, 166
 - file access control rules, 179
 - mandatory groups, 36
 - network access control rules, 179
 - Red Hat, 200
 - Red Hat Packet Manager (RPM), 177
 - view preferences, 365
- lists, 141
- local event manager, 164
- @local variable, 143
- locks, 192
- Log Deny Actions option, 335
- logging, 77
 - analyzing log data, 283
 - deny actions, 42, 335
 - Event field, 216–217
 - event logs. *See* event logs
 - history, 361
 - log directories, 198
 - log file scraping, 15

- local event manager, 164
- purging logs, 225
- rule precedence, 76
- security logs, 189
- Test Mode, 327
- verbose logging, 220, 277, 326
- login modules, VMS, 362

M

- maintenance
 - See* administration
- malicious code, 21–23
- Management Center Reachable system state set, 67–68
- Management Console. *See* MC
- mandatory
 - groups, 36, 122, 315, 344
 - policies, 122
 - rules, 36
- manipulation rules, 75–76
- manual updates, 181
- mapping applications, 256
- MC (Management Console), 27–28
 - event messages, 167
 - MSDE database, 167
 - saving changes, 41
 - state sets, 64
 - updating rules, 164
 - viewing events, 205
- media streams, 103
- memory, 104, 165–166
- meta characters, 147
- microphones, 103
- Microsoft Data Engine (MSDE) database, 167
- Microsoft Office policy, 323–324
- Microsoft Windows. *See* Windows
- modules, 61
- monitor
 - actions, 72
 - roles, 364
 - rules, 76
- Morris worm, 7
- MSDE (Microsoft Data Engine) database, 167, 343

N-O

- NAC (Network Admission Control), 26, 54, 66–68
- name resolution, 167
- net start command, 99
- Network Admission Control (NAC), 26, 54, 66–68
- Network Applications interceptor, 164
- Network Data Flows report, 265–267
- network events, 293
 - all events, 294
 - destination port summary, 293
 - UNIX, 299
- network interface cards (NICs), 106
- network interface control rule, 106–107
- Network Intrusion Detection System (NIDS), 22
- Network Server Applications report, 267–268
- network services sets, 145–146, 358
- network shield rules, 94–96, 178
- network shims, 94, 170–171
 - conflicts, 347
 - implementation plan, 341
- Network Traffic interceptor, 164
- networks
 - access control rules, 93, 171, 179
 - address sets, 142–145, 358
 - attacks. *See* attacks
 - Linux, 166
 - locks, 192
 - Solaris, 166
 - Windows, 165
- NICs (network interface cards), 106
- NIDS (Network Intrusion Detection System), 22
- nonquiet installs, 169, 172
- nonroot user state set, 65
- notice events, 209
- NT event log rule, 96–97
- objects
 - exporting, 358–359
 - Help menu, 374
 - importing, 361
 - referencing, 358
 - restricting administrator access, 364
 - Search menu, 374
- ODBC DSN, 212
- online help, 374

operating systems (supported), 28, 165–166.
See also individual operating systems

P

-
- packets, malformed, 170
 - Partners, Cisco, 339
 - patches, 93
 - payloads, 6
 - damaging, 11
 - worms, 7
 - permission reports, VMS, 363
 - permissions, 194, 364
 - persistence, 10
 - pilot phase, 350, 352
 - ping sweeps, 9
 - planning, 337–339
 - point security, 13–14
 - policies, 61, 119, 311, 314
 - agent
 - interaction rules, 306
 - policy manager, 164
 - systems, 122
 - UI rules, 306
 - API rules, 306
 - audit logs, 121
 - availability, 312
 - component hierarchy, 313–314
 - confidentiality, 312
 - creating, 312–322
 - CSA-related, 312
 - deploying, 315–316
 - documents, 311
 - enforcement. disabling, 279
 - filtering, 120
 - fine-tuning, 325–326
 - DMP/RTR files, 335
 - event log entries, 328–329
 - event log versus Event Monitor, 334–335
 - Event Management Wizard, 330–334
 - features impacting, 326–327
 - filtering event log view, 328
 - troubleshooting, 335
 - groups, 122, 314
 - importing behavior policies, 302
 - integrity, 312
 - mandatory, 122
 - new versus predefined, 313
 - Policy Detail reports, 241, 243
 - predefined, 119, 121–122, 322, 347
 - Base Operating System Protection - Windows, 323
 - Instant Messenger, 324–325
 - Microsoft Office, 323–324
 - rules, 226
 - Search menu, 369–370
 - security, 312
 - settings, 120–121
 - sharing components, 358
 - testing, 342, 348
 - tuning, 311
 - updating, 51, 164–167
 - Policy Detail reports, 241–243
 - polling, 80, 327
 - polling intervals, 30, 51
 - groups, 41
 - hosts, 51–52
 - pop-up messages, 186
 - ports
 - ephemeral, 146
 - network services variable, 146
 - scans, 9, 95, 164, 170, 348
 - precedence
 - mandatory groups, 122
 - rules, 36, 73–76
 - predefined
 - event sets, 225
 - groups, 36–37
 - policies, 119
 - rule modules, 118
 - system state sets, 67
 - user state sets, 64
 - preferences, administrative, 365–366
 - printf() calls, 106
 - privileges, 105
 - processors, 165–166
 - Product Authorization Key (PAK) code, 355
 - Product Usage report, 268–270
 - Profiler utility, 300
 - PROGIDs, 155, 158
 - project implementation. *See* implementation plan
 - Promiscuous Mode, 106
 - proprietary traffic, 101, 106

Protect Mode, 41
pull/push model, 30

Q

quarantined files/IP addresses, 152–153
query
 actions, 72
 rules, 73–76
 settings, 153–155, 358
 tokens, 154
 user default allow/deny/terminate actions, 72
quick link options, rule modules, 114–116
quiet installs, 169, 172

R

rate limits, connections, 85
RBAC (role-based access control), 232, 362
 administrative control, 364
 administrative preferences, 365–366
 inheriting VMS rights, 362–364
reactive detection, 15
Red Hat, 200. *See also* Linux
Red Hat Packet Manager (RPM), 177
refresh rates, 210
registration, 172, 355–358
registry
 access control rules, 98–99, 158
 editing, 289
 events, 289–290
 filtering, 290
 pop-up messages, 186
 sets, 158, 358
 writing to, 98
remote agents
 application behavior investigation, 281–283
 event logs, 283
remote policy updates, 31
Remote Procedure Call (RPC), 9
remove from application class actions, 72
reports, 327
 ActiveX Frame reports, 236–238, 243
 antivirus installations, 262–263
 audit trails, 232–234
 behavior reports, 285–286, 297
 configuring, 236
 creating, 243–245
 CSV reports, 297
 events, 235
 by group reports, 238
 sets, 225
 by severity, 235–238
 global, 27
 Group Detail reports, 239
 Host Detail reports, 239–241
 hotfixes, 264
 HTML Frame reports, 236–237, 243
 installed products, 263–264
 network data flows, 265–267
 network server applications, 267–268
 Policy Detail reports, 241–243
 product usage, 268–270
 Reports menu, 231
 Event by Severity option, 235
 Group Details reports, 239
 Host Detail reports, 239
 Policy Detail reports, 241
 sharing components, 358
 sorting options, 238
 summary reports, 295
 behavior, 295
 behavior by process, 295
 UNIX, 299
 UNIX Behavior Analysis reports, 299
 unprotected hosts, 270–271
 unprotected products, 271–273
 viewing, 243
request trace (RTR) files, 197, 335
resource access control rule, 107–108
role-based access control. *See* RBAC
Root user state set, 65
Rootkit Detected system state set, 69
rootkit/kernel protection rule, 108–109
RPC (Remote Procedure Call), 9
RPM (Red Hat Packet Manager), 177
RTR (request trace) files, 197, 335
rule modules, 61, 111, 314
 application behavior analysis, 300
 application behavior investigation, 303–306
 audit trails, 116
 cloning, 111, 315

- comparing, 112
- creating, 113–116
- policies, 119
 - groups/agents, 122
 - predefined, 121–122
 - settings, 120–121
- predefined, 116–119
- Profiler utility, 300
- quick link options, 114–116
- Rule Generation module, 283
- Search menu, 370–371
- sharing components, 358
- system state sets, 66
- test beds, 342
- Test Mode, 113
- working with, 111–112
 - comparing, 112
 - creating, 113–116
 - using predefined modules, 116–119
- rule/event correlation engine, 164
- rules, 61–63, 313
 - actions, 71–72
 - access control
 - COM components, 155
 - data sets, 147–149
 - file sets, 149–152
 - network address sets, 142–145
 - network services sets, 145–146
 - registry sets, 158
 - agent service control, 77–78
 - agent UI control, 79–81
 - application builder rules, 136
 - application classes, 125
 - application control, 81–82
 - buffer overflow, 104–106
 - clipboard access control, 82–83
 - cloning, 111
 - COM component access control, 83–85, 179
 - configuration options, 76–77
 - conflicts, 75, 348
 - connection rate limit, 85–86
 - creating, 305
 - data access control, 86–87, 179
 - detection rules, 55, 111
 - directories, 88
 - editing, 329
 - enforcement rules, 55, 111
 - Event Monitor, 334
 - Event Wizard, 217
 - exception rules, 217, 330–334
 - file access control, 88–89, 179
 - file version control, 90–91
 - fine-tuning, 325
 - hosts, 314
 - local event manager, 164
 - locks, 192
 - kernel protection, 91–93
 - mandatory groups, 315
 - mandatory rules, 36
 - manipulation, 75–76
 - modules, 61, 111, 314
 - application behavior analysis, 300
 - application behavior investigation, 303–306
 - audit trails, 116
 - cloning, 111, 315
 - comparing, 112
 - creating, 113–116
 - policies, 119–122
 - predefined, 116–119
 - Profiler utility, 300
 - quick link options, 114–116
 - Rule Generation module, 283
 - Search menu, 370–371
 - sharing components, 358
 - system state sets, 66
 - test beds, 342
 - Test Mode, 113
 - working with, 111–116
 - monitor rules, 76
 - network access control rules, 93, 179
 - network interface control, 106–107
 - network shield, 94–96, 178
 - NT event log, 96–97
 - override options, 41
 - policies, 312
 - precedence, 36, 73–76
 - query rules, 73–74
 - registry access control, 98–99
 - resource access control, 107–108
 - rootkit/kernel protection, 108–109
 - rule actions, 71–72
 - rule sets, 36
 - Enabled check box, 77
 - rule/event correlation engine, 164
 - rule-override options, 41

- Search menu, 371
- service restart, 99–100
- sniffer and protocol detection, 101–102
- Solaris, 72
- state sets, 63
 - managing, 70
 - MC, 64
 - system state, 66–69
 - user state, 63–66
- syslog control, 109–111
- system API, 102, 104
- Test Mode, 52
- tuning, 305, 311
- updating, 164
- user interfaces, 185
- Run key, 10
- RunOnce key, 10

S

- SAFE, 31
- scope creep, 337
- scripts
 - agent kits
 - installing, 179
 - uninstalling, 182
 - shell, 140
- SDNI (Self-Defending Network Initiative), 26
- Search menu, 367
 - all objects, 374
 - application classes, 372
 - groups, 369
 - hosts, 367
 - policies, 369–370
 - rule modules, 370–371
 - rules, 371
 - variables, 372
- Secure Shell (SSH), 14
- Secure Sockets Layer (SSL), 30, 167, 343
- security
 - candy shell security, 14
 - communication security, 167
 - edge devices, 14
 - endpoint security, 31
 - file/directory protection, 26
 - firewalls, 13
 - IDSs, 13
 - levels, 192
 - NAC, 26
 - point security, 13–14
 - policies, 17–18, 62–63, 342
 - acceptable use, 62
 - agent systems, 122
 - application control, 25
 - compliance versus enforcement, 18
 - rule modules, 111
 - system state sets, 68
 - SAFE, 31
 - security identifiers (SIDs), 64
 - Security Level Low system state set, 68
 - Self-Defending Network Initiative (SDNI), 26
 - self-protection, agent, 77
 - servers
 - licences, 355
 - network shims, 171
 - using groups, 346
 - workstations, versus, 346
 - Servers - All Types group, 47
 - Servers - IIS Web Servers group, 47
 - service patches, 169
 - service restart rule, 99–100
 - Service user state set, 65
 - sets, 141
 - shell scripts, controlling, 140–141
 - shims. *See* network shims
 - Short Polling groups, 345
 - SIDs (security identifiers), 64
 - signature-based attack detection, 15
 - signatures
 - attacked detection, based on, 15
 - signed UPD hint messages, 31
 - Slammer worm, 11
 - sneakernet, 5, 15
 - sniffer and protocol detection rule, 101–102
 - sniffers, 101, 106
 - software, updates, 167, 179–182
 - automatic, 179
 - manual, 181
 - groups, 345
 - Solaris
 - agent kits
 - installing, 177
 - uninstalling, 183

- arguments, 201
- buffer overflows, 178
- components, 164
- default actions, 74
- directories, default installation, 177
- file access control rules, 179
- interfaces, 200–201
- mandatory groups, 36
- network access control rules, 179
- query rules, 72
- software updates, 181
- view preferences, 365
- See also* UNIX
- spoofing, 67–95
- spyware, 12
- SQL server, 343
- SSH (Secure Shell), 14
- SSL (Secure Sockets Layer), 30, 167, 343
- state sets, 63–65
 - managing, 70
 - system state, 66–69
 - user state, 63–66, 347
 - wildcards, 66
- static
 - application classes, 133–134
 - files, 16
- status summary, 206
 - event counts per day, 208–210
 - network, 207–208
 - refresh, 210
- success criteria, planning, 337–339, 350
- summaries
 - COM object, 291
 - destination port, 293
 - directory, 286
 - event counts per day, 208–210
 - individual file, 287
 - key registry, 289
 - refresh, 210
 - reports, 295
 - status, 206–210
 - UNIX, 299
- symbolic link attacks, 107
- SYN floods, 95, 164, 170
- syslog
 - control rule, 109–111
 - events, 109
- system API rule, 102–104

- System Booting system state set, 68
- system calls, 104–105
- system files, 92
- system state sets, 66–69
 - configuring, 69
 - predefined, 67
 - sharing components, 358
- system tray options, 186–187
- Systems - Test Mode group, 47

T

- tasks
 - auto-pruning, 224
 - event insertion, 223–224
- TCP (Transmission Control Protocol)
 - blended threats, 9
 - ephemeral ports, 146
 - MC communication, 30
 - port scans, 95
- technical support, 374–375
- Terminal Services, 165
- terminate process deny actions, 71
- test beds, 342
- Test Mode, 52
 - events, 216
 - groups, 41, 345
 - logging, 326–327
 - rule modules, 113
- testing phase, 339–340
 - alerts, creating, 349
 - administrative settings, creating/configuring, 346
 - Enforcement Mode, placing policy in, 349
 - exporting/reporting/documenting, 349
 - gathering information, 341–342
 - management architecture, installing 343
 - test bed size and components, determining, 342
 - test hierarchy, creating/configuring, 343–346
 - test policies
 - adding advanced policies, 348–349
 - creating base test policies, 346–347
 - deploying, 347–348
 - tuning, 348–349
 - training staff/users, 339, 349–350
 - success, verifying 350

- theft, data, 82
- time parameters, 279
- timeframes
 - polling intervals, 327
 - rules, 325
 - software updates, 181
- tokens, query, 154
- traceroute packets, 95
- training, staff/users, 339, 349–350
- Transmission Control Protocol. *See* TCP
- tray icon, 186
- Trojan horses
 - agent self-protection, 77
 - detecting, 93
 - preventing execution, 102
 - trapping keystrokes, 103
- troubleshooting
 - event logs, 335
 - isolated breaches, 346
 - using Short Polling groups, 345
- tuning
 - false positives, 326
 - imported rule modules, 303–306
 - policies, 311

U

- UDP (User Datagram Protocol)
 - blended threats, 9
 - ephemeral ports, 146
 - hint messages, 31, 41, 327
 - Log check box, 93
 - port scans, 95
- Uniform Resource Identifiers (URIs), 86
- UNIX
 - application behavior investigation, 276, 299
 - auto-start mechanisms, 10
 - buffer-overflow attacks, 105
 - COM objects, 156
 - components, 164
 - data filters, 87
 - directory paths, 116
 - file sets, 152
 - LIBC routines, 105

- Promiscuous Mode, 106
- root users, 65
- rule modules, 111
- rule types
 - agent service control, 77–78
 - agent UI control, 79–81
 - application control, 81–82
 - buffer overflow, 104–106
 - connection rate limit, 85–86
 - data access control, 86–87
 - file access control, 88–89
 - network access control, 93
 - network interface control, 106–107
 - network shield, 94–96
 - resource access control, 107–108
 - rootkit/kernel protection, 108–109
 - syslog control, 109–111
- shell scripts, controlling, 140–141
- spoofing, 95
- symbolic link attacks, 107
- SYN flooding, 95
- See also* Solaris
- UNIX Behavior Analysis reports, 299
- Unprotected Hosts report, 270–271
- Unprotected Products report, 271–273
- updates, 30, 51, 327
 - hosts, 207
 - policies, 167
 - scheduled, 179
 - software, 167, 179–182
 - automatic, 179
 - manual, 181
 - groups, 345
- URIs (Uniform Resource Identifiers), 86
- User Datagram Protocol. *See* UDP
- user implementation plan, 350
- user information, filtering, 42
- user interaction, 344
- user interfaces, 29, 81
- user profiles (VMS), 363
- user state sets, 63–65, 347
 - configuring, 65
 - predefined, 64
 - sharing components, 358
 - wildcards, 66

V

- variables, 141
 - COM component sets, 155–158
 - data sets, 147–149
 - @dynamic, 143
 - file sets, 149–152
 - @local, 143
 - network address sets, 142–145
 - network services sets, 145–146
 - quarantined files/IP addresses, 152–153
 - query settings, 153–155
 - registry sets, 158
 - Search menu, 372
 - special variables, 89
- verbose logging, 220, 277, 326
- Verbose Logging Mode, 41
- version information, 375
- view preferences, 365
- Virus Detected system state set, 68–69
- viruses
 - command shells, 81
 - day-zero attacks, 21
 - @dynamic list, 153
 - e-mail, 8
 - encryption, 14
 - floppy disks, 5–6
 - global implications, 11
 - history, 5–7
 - Internet, 7
 - LANs, 6
 - life cycles, 23–24
 - payload, 6
 - persistence, 10
 - single environment, 8
 - sneakernet, 5
 - system state sets, 68–69
 - testing system protection, 348
 - WANs, 7
 - zip files, 14
- VMS server, 343–344
 - administrator rights, 362–364
 - license, 356
 - RBAC, 362
- vulnerabilities, 9

W

- WANs (wide-area networks)
 - polling intervals, 51
 - viruses, 7
- warning events, 209
- web servers, 86
- webcams, 103
- websites
 - Cisco.com, 165, 338–339, 375
 - Cisco.com/go/safe, 31
 - SANS.org, 18
- wide-area networks. *See* WANs
- wildcards
 - COM components sets, 155
 - directories, 194
 - files, 194
 - registry sets, 158
 - state sets, 66
- Windows
 - agent kits
 - downloading, 177
 - installing, 171–177
 - applications
 - behavior investigation, 276
 - classes, 126
 - deployment investigation, 249
 - auto-start mechanisms, 10
 - COM objects, 83, 156
 - CSA installation requirements, 165
 - data filters, 87
 - DCOM, 9
 - directories
 - default installation, 174
 - paths, 116
 - hidden shares, 23
 - hotfixes, 264
 - interfaces
 - Agent Control Panel, 187, 190–192
 - audible notifications, 195
 - directories, 198
 - firewalls, 193–195
 - GUI, 187, 190–192
 - Programs menu, 196–198
 - stopping, 199
 - system tray options, 186–187
 - tools, 198

- tray icon, 186
- user interaction, 198
- mandatory groups, 36
- quiet/nonquiet installation, 172
- registry, 289
 - filtering, 290
 - sets, 158
- restarting services, 99
- RPC, 9
- rule modules, 111
- rule sets, 96–97
- rule types
 - agent service control, 77–78
 - agent UI control, 79–81
 - application control, 81–82
 - clipboard access control, 82–83
 - COM component access control, 83–85
 - connection rate limit, 85–86
 - data access control, 86–87
 - file access control, 88–89
 - file version control, 90–91
 - kernel protection, 91–93
 - network access control, 93
 - network shield, 94–96
 - registry access control, 98–99
 - service restart, 99–100
 - sniffer and protocol detection, 101–102
 - system API, 102–104
- SIDs, 64
- updates, 93
- user prevalence, 8
- view preferences, 365
- workstations
 - defense in depth, 348
 - licenses, 355
 - servers, versus, 346
- worms
 - command shells, 81
 - day-zero attacks, 21
 - @dynamic list, 153
 - e-mail, 8
 - encryption, 14
 - global implications, 11
 - history, 5–7
 - life cycles, 23–24
 - mandatory groups, 315
 - Morris, 7

- payloads, 7
- persistence, 10
- single environment, 8
- Slammer, 11
- SSH, 14
- SSL, 14
- Windows, 8

X–Z

- XML files, 359

- zip files, 14