



Numerics

2005 FBI Cybercrime Reports, 50

A–B

access control, monitoring, 43

acknowledgments, 225

Action field (Summary Dashboard), 208

active rules, 77, 265–266

Add Recipient feature, 254

adding

Check Point firewall appliances to
CS-MARS, 166

Cisco IPS appliances to CS-MARS database,
174–175

Cisco PIX firewalls to CS-MARS, 163–164
device information into CS-MARS, 114–121

ExtremeWare switches to CS-MARS
database, 160

IntruVert IntruShield v1.8 to CS-MARS,
178–180

ISS RealSecure Host Sensor to CS-MARS, 186

ISS RealSecure Network Sensor to
CS-MARS, 185

Juniper NetScreen firewall to CS-MARS,
165–166

Juniper NetScreen IDP to CS-MARS
database, 181

Linux OS to CS-MARS database, 194

Microsoft IIS web server to CS-MARS
database, 195–196

NetCache devices to CS-MARS database,
168–170

Oracle database servers to CS-MARS database,
202–203

Snort IPS Sensor to CS-MARS database,
187–188

Solaris OS to CS-MARS database, 194

Symantec ManHunt to CS-MARS database,
182–183

VPN 3000 Series concentrators to CS-MARS
database, 200

add-ons, CMA, 352

Adobe SVG Viewer, 210

graphics, manipulating, 83

agents, communication between CS-MARS and
reporting devices, 95–96

alarms, false positives, 91

creating drop rules for, 92

anomaly detection, 32

Apache web servers, configuring communication
with CS-MARS, 196–198

application inspection, 32

applying filters to queries, 239–240

archiving, 80

NAS storage types, 80

remote storage capacity,
calculating, 81

ASA (Adaptive Security Appliance), 161.

See also Cisco PIX firewall

Attack diagram (Summary
Dashboard), 214

attack diagrams, 83–86

attack mitigation, 16

attack vectors, 83

attacks, 61–63

attributes of system rules,
modifying, 257

audit requirements,
report types, 247

authentication layer
(defense-in-depth), 27

automated log correlation, 34

automated log integration, 35

automated mitigation, 34–35

CS-MARS functionality, 40

automated threat response, 34–35

CS-MARS functionality, 39

AVVID (Architecture for Voice, Video and
Integrated Data), 21

baselining, 89

behavioral profiling, 89–90

blackmail, 60

botnets, 61

bots, 53

C

- calculating, 59, 64–66**
 - remote storage capacity, 81
- canned reports, 247**
- case-management tools, 97**
- Cases field (Summary Dashboard), 209**
- Cases tab (Incidents page), 227–228**
- CATOS Hybrid OS, 152**
- CATOS switches, configuring NetFlow, 324–325**
- Check Point firewall appliances**
 - adding to CS-MARS database, 166
 - device communication with CS-MARS
 - configuring, 354–358*
 - verifying communications parameters, 358*
 - communication with CS-MARS,
 - configuring, 166–167
- Check Point NG FP3/AI modules, side configuration, 353–354**
- Cisco AVVID (Architecture for Voice, Video and Integrated Data), 21**
- Cisco CATOS switches, 324–325**
- Cisco Guard, 30**
- Cisco IOS Software, 152**
 - NetFlow, configuring, 323–324
- Cisco IPS appliance**
 - 4.x appliance, 172
 - 5.x appliance, 173–174
 - adding to CS-MARS database, 174–175
 - communication with CS-MARS, configuring, 171–172
- Cisco IPS switch modules, communication with CS-MARS, configuring, 176**
- Cisco ISR (Integrated Services Router), configuring communication with CS-MARS, 176–177**
- Cisco PIX firewall**
 - adding to CS-MARS, 163–164
 - communication with CS-MARS,
 - configuring
 - SNMP, 163*
 - SSH, 161–162*
 - Telnet, 161*
- Cisco SSM, configuring communication with CS-MARS, 177**
- Cisco-specific security websites, 298–299**
- classifications of CS-MARS-supported devices, 132**
- CMA (Check Point Customer Management Add-On), 352**
- collaborated security events, 14**
- command summary, 327–330**
- commands**
 - hotswap, 331
 - pnlog, 331
 - pnrestore, 81, 331
 - pnupgrade, 333
- communication between CS-MARS and reporting devices, 93**
 - agents, 95–96
 - case-management tools, 97
 - notification methods, 96–98
- communications parameters, verifying on Check Point devices, 358**
- complex rules**
 - creating, 276–278
 - offsets, syntax, 276
- components of CS-MARS, 74**
- configuring**
 - Check Point devices, 353–354
 - communication with CS-MARS, 354–358*
 - Cisco CATOS switches, NetFlow, 324–325
 - Cisco IOS devices, NetFlow, 323–324
 - CS-MARS communication
 - with Apache web servers, 196–198*
 - with Check Point firewall appliances, 166–167*
 - with Cisco IPS appliance, 171–175*
 - with Cisco IPS switch modules, 176*
 - with Cisco ISR, 176–177*
 - with Cisco SSM, 177*
 - with Enterasys Dragon, 188*
 - with ExtremeWare switches, 159–160*
 - with firewalls, 160*
 - with IDSs, 170–171*
 - with IntruVert IntruShield v1.8, 177–178*
 - with ISS RealSecure Sensor, 183–185*
 - with Juniper NetScreen firewalls, 164*
 - with Juniper NetScreen IDP, 180*

- with Linux OS, 193–194
 - with Microsoft IIS web server, 194–195
 - with NetCache, 167–170
 - with Oracle database servers, 201–202
 - with PIX firewalls, 161–163
 - with routers, 145–150
 - with Snort IPS Sensor, 187
 - with Sun Solaris OS, 193–194
 - with switches, 151–158
 - with Symantec ManHunt, 181
 - with VPN 3000 Series concentrators, 199
 - with Windows OS, 189–191
 - ISS network sensors, 321–322
 - ISS server sensors, 322–323
 - maintenance parameters on CS-MARS, 126–127
 - NetFlow on CS-MARS, 123
 - query type, 233–235
 - reporting devices on CS-MARS, 114–115
 - device information, adding, 114–121
 - system parameters on CS-MARS, 111–113, 127–128
 - vulnerability scanning on CS-MARS, 124
 - console access on CS-MARS, 349–350**
 - correlation of event data, 6**
 - cost of recovering from cyberattack, 64–66**
 - costs of cyberattack, 54–59**
 - count variable, 274**
 - creating**
 - custom reports, 251–253
 - custom system inspection rules, 266–273
 - rules, 255
 - complex rules, 276–278
 - drop rules, 258, 261, 264
 - inspection rules, 256–257
 - with Query tool, 274–276
 - users, 121–122
 - CSA (Cisco Security Agent), 33**
 - CS-MARS (Cisco Security Monitoring, Analysis, and Response System), 13, 35, 283–290**
 - as STM solution, 41
 - automated mitigation, 40
 - automated threat response, 39
 - command summary, 327–330
 - commands
 - hotswap, 331
 - pnreset, 331
 - pnstart, 332
 - pnstatus, 332
 - pnupgrade, 333
 - console access, 349–350
 - evaluation worksheet, 315, 319
 - fact sheet, 304–305
 - global deployment, 45
 - hardware and protocol specifications, 301–304
 - log integration, 36–37
 - on enterprise networks, 19–21
 - on SMB networks, 17–18
 - proactive security framework, 14–17
 - product family, 44
 - sample seed file, 319–320
 - standalone deployment, 45
 - CS-MARS v4.1**
 - product support list, 307
 - report types, 335–347
 - CSV files, importing device information into CS-MARS, 120–121**
 - CSV view report format, 246**
 - custom inspection rules, creating, 266–273**
 - Custom Parsing, 37**
 - custom reports, creating, 251, 253**
 - custom rules, variables, 274**
 - customer success stories, 283–290**
 - cyberattacks, 64–66**
 - costs of
 - intangible costs, 58–59
 - tangible costs, 54–57
 - cyberblackmail, 60**
 - cybercrime, vulnerability of U.S. infrastructure, 50**
- ## D
-
- database (CS-MARS), structure and storage requirements, 79–80**
 - database servers (Oracle), communication with CS-MARS, configuring, 201–202**
 - day-zero worms, Sasser, 41**
 - default actions (rules), 256**
 - defense-in-depth, 26**
 - authentication layer, 27
 - automated log correlation, 35
 - automated mitigation, 35
 - automated threat response, 35

- host intrusion-prevention layer, 32–33
- network intrusion-prevention layer, 31–32
- perimeter layer, 28–30
- security best practices, 33–34

delivering reports, 253–255**deploying CS-MARS**

- initial configuration, 108–111
 - system parameters, entering, 111–113*
- maintenance parameters, configuring, 126–127
- NetFlow, configuring, 123
- network placement, 102–104
- reporting devices, configuring, 114–121
- security hardening, 104–107
- system parameters, configuring, 127–128
- users, creating, 121–122
- vulnerability scanning, configuring, 124

displaying

- attack vectors, 83
- inspection rules, 256

DoS attacks, 29, 53**drop rules, 77, 257**

- creating, 92, 258, 261, 264

DTM (distributed threat mitigation), 176**duplicating system rules, 257****dynamic vulnerability scanning, configuring on CS-MARS, 124**

E**EAPoUDP messages, 148****emailing reports, 253–255****enforcing security policies, 42****Enterasys Dragon, configuring communication with CS-MARS, 188****enterprise financial company, 288–289****enterprise networks, deploying CS-MARS, 19–21****EoU (EAP over UDP), 148****evaluation worksheet, CS-MARS, 315, 319****event correlation, 90****event data correlation, 6****event database storage requirements, 79–80****Event Type field (Summary****Dashboard), 208****events, 75****examples of FUD, 50–51****extortion, ransomware, 60****ExtremeWare, configuring for switch/CS-MARS communication, 159–160**

F**false positive tunes, 258. See also drop rules****False Positive Tuning Wizard, 258****false positives, 15, 91–92**

- acknowledgment, 225
- graphing, 216

False Positives tab (Incidents page), 225–227**filters, applying to queries, 239–240****firewalls, 30, 164**

- Check Point firewall appliances, configuring CS-MARS communication, 166–167

- Cisco PIX

 - adding to CS-MARS, 163–164*

 - configuring CS-MARS communication, 161–163*

- CS-MARS communication, configuring, 160

- Juniper NetScreen, configuring CS-MARS communication, 164

flows, 88–89**forensics analysis, 83–86****format types of reports, 246–247****formatting criteria for reports, 246****FUD (fear, uncertainty, and doubt), 49**

- examples of, 50–51

FWSM (Firewall Service Module), 161. See also Cisco PIX firewall

G**GCs (Global Controllers), 44, 73**

- hardware specifications, 74

generic routers, enabling for CS-MARS communication, 149–150**global deployment (CS-MARS), 45****government security controls and information web sites, 296–297****Gramm-Leach-Bliley Act, 10****graph types in Network Status tab, 220–222****graphics display, manipulating with Adobe SVG Viewer, 83**

H

- hardware specifications for CS-MARS, 73, 301, 303–304
- HIPAA (Health Insurance Portability and Accountability Act), 10
- host intrusion-prevention layer (defense-in-depth), 32–33
- HotSpot graph (Summary Dashboard), 213–214
- hotswap command, 331

I

- ICS (Cisco Incident Control Server), 31
- IDSs (intrusion detection systems)
 - CS-MARS communication, configuring, 170–171
 - Juniper NetScreen IDP, configuring CS-MARS communication, 180
- importing device information into CS-MARS, 120–121
- inactive rules, 77, 265–266
- in-band incident notification, 16
- Incident ID field (Summary Dashboard), 208
- incident ID, viewing, 229–232
- incident notification, 16
- incidents, 76
 - path vectors, displaying, 83
 - vector information, viewing in Summary Dashboard, 212–213
 - viewing in Summary Dashboard, 208–211
- Incidents page, 223
 - Cases tab, 227–228
 - False Positives tab, 225–227
 - Incidents tab, 224–225
- Information Summary column (Summary Dashboard), 216, 219
- initial CS-MARS configuration, 108–111
 - system parameters, entering, 111–113
- inspection rules, 76, 256–257
 - customizing, 266–270, 273
 - viewing, 256
- installing CS-MARS, 108
- instant queries, 235
- intangible costs of cyberattacks, 58–59
- interaction between reporting devices and CS-MARS, 93
 - agents, 95–96
 - case-management tools, 97
 - notification methods, 96–98
- interpreting X, Y axis graphs, 219
- IntruVert IntruShield v1.8
 - adding to CS-MARS database, 178–180
 - communication with CS-MARS, configuring, 177–178
- IPSs (intrusion prevention systems)
 - Cisco IPS appliance
 - adding to CS-MARS database, 174–175
 - configuring CS-MARS communication, 171–174
 - Cisco IPS Catalyst switch modules, configuring CS-MARS communication, 176
 - Cisco ISR, configuring CS-MARS communication, 176–177
 - Cisco SSM configuring CS-MARS communication, 177
 - Enterasys Dragon, configuring CS-MARS communication, 188
 - IntruVert IntruShield v1.8, configuring CS-MARS communication, 177–178
 - ISS RealSecure Sensor, configuring CS-MARS communication, 183–185
 - Snort IPS Sensor, configuring CS-MARS communication, 187
 - Symantec ManHunt, configuring CS-MARS communication, 181
- ISS (Internet Security Systems)
 - network sensors, configuration scripts, 321–322
 - RealSecure Sensor
 - adding to CS-MARS database, 185–186
 - configuring communication with CS-MARS, 183–185
 - server sensors, configuration scripts, 322–323
 - SiteProtector, 320

J

Juniper NetScreen firewall

- adding to CS-MARS database, 165–166
- communication with CS-MARS, configuring, 164

Juniper NetScreen IDP

- adding to CS-MARS database, 181
- configuring communication with CS-MARS, 180

L

L2 discovery, configuring for switch/CS-MARS communication, 151

- on switches running CATOS, 153–154
- on switches running Cisco IOS 12.2, 152

LCs (Local Controllers), 44, 73

legislation

- Gramm-Leach-Bliley Act, 10
- HIPAA, 10
- Sarbanes-Oxley Act, 9
- security and financial audit requirements, reporting, 247

Linux OS

- adding to CS-MARS database, 194
- configuring CS-MARS communication, 193–194

loading reports as On-Demand Query, 249–250

M

maintenance parameters, configuring on CS-MARS, 126–127

manipulating graphics display on Adobe SVG Viewer, 83

manual queries, 238–242

manufacturers of SIMs, multivendor solution, 21–22

Matched Rule field (Summary Dashboard), 208

memory allocation information for NetFlow, 307

MIBs, network discovery, 87

Microsoft IIS web server, configuring CS-MARS communication, 194–195

migrating from SIM to STM, 12

mitigation devices, 138

modifying system rule attributes, 257

monitoring access control, 43

multiple-offset rules, syntax, 276

multivendor solution to SIMs, 21–22

My Reports tab, 222

N

NAC (network admission control), 28

NAC-specific messages, configuring for switch/CS-MARS communication, 156–157

- on switches running CATOS, 158
- on switches running IOS, 157

NAC-specific reporting, enabling for router/CS-MARS communication, 148–149

NAS (networked attached storage) types, 80

native CS-MARS applications, 36–37

Nessus VA scanning, 92

NetCache

- adding to CS-MARS database, 168, 170
- configuring CS-MARS communication, 167–168

NetFlow, 88–90

- CS-MARS communication, 158
- on CATOS switches, 158
- on IOS devices, 158

configuring

- on Cisco CATOS switches, 324–325
- on Cisco IOS devices, 323–324
- on CS-MARS, 123

enabling for router/CS-MARS communication,

- 146–147

event activity, viewing, 215

memory allocation information, 307

performance guide, 306–307

NetFlow platform guide, 305

network discovery, methods of, 86–87

network intrusion-prevention layer

(defense-in-depth), 31–32

network sensors (ISS), configuring, 321–322

Network Status tab, 220

- graph types, 220–222

NFS, archiving, 80

O

- offsets, 266**
 - syntax, 276
- on-demand queries, 237**
 - creating for reports, 249–250
- OPSEC (Open Platform for Security), 21, 359**
- Oracle database servers**
 - adding to CS-MARS database, 202–203
 - configuring communication with CS-MARS, 201–202
- out-of-band incident notification, 16**

P

- parsers, 76**
- part numbers, 74**
- patented technologies of CS-MARS, 77–78**
- Path column (Summary Dashboard), 209, 211**
 - incident vector information, viewing, 212–213
- Peak view report format, 246**
- perimeter layer (defense-in-depth), 28–30**
- Perl configuration scripts**
 - for ISS network sensors, 321–322
 - for ISS server sensors, 322–323
- placement of CS-MARS, 102–104**
- pnlog command, 331**
- pnrestore command, 81, 331**
- pnupgrade command, 333**
- predefined reports, 247**
 - viewing with Report tab, 248
- proactive security framework, 14–17**
- probability of reoccurring attacks, 62–63**
- product support list (CS-MARS v4.1), 307**
- protocol security hardening, 107**
- protocol specifications (CS-MARS), 301–304**
- pulling data, 6**
- pushing data, 6**

Q

- queries, 232, 256**
 - filters, applying, 239–240
 - instant, 235
 - manual, 238–240, 242

- on-demand, 237
 - creating for reports, 249–250

- Query tool, creating rules, 274–276**
- query type, configuring, 233–235**

R

- ransomware, 60**
- RDEP (Remote Data Exchange Protocol), 171**
- Recent view report format, 246**
- recipients, assigning to reports, 254**
- recovering from cyberattacks**
 - with CS-MARS, 65–66
 - without CS-MARS, 64–65
- regulatory compliance, 9**
 - Gramm-Leach-Bliley Act, 10
 - HIPAA, 10
 - Sarbanes-Oxley Act, 9
- remote storage capacity, calculating, 81**
- reoccurrence of attacks, probability of, 62–63**
- Report Creation tool, 251**
- Report tab, viewing predefined reports, 248**
- reporting devices, 137**
 - communication with CS-MARS, 93
 - agents, 95–96
 - notification methods, 96–98
 - configuring, 114–121
- reports**
 - CS-MARS v4.1, 335–347
 - customizing, 251–253
 - emailing, 253–255
 - format types, 246–247
 - formatting criteria, 246
 - loading as On-Demand Query, 249–250
 - predefined, 247–248
- restoring archived data, 81**
- ROI (return on investment), 49**
- rootkits, 52**
- routers, configuring CS-MARS communication, 145**
 - generic routers, 149–150
 - NAC-specific reporting, 148–149
 - NetFlow, 146–147
 - SNMP, 146
 - syslog, 147

Rule Creation tool, 256**rules, 76**

- active, 265–266
- complex, creating, 276–278
- creating, 255
 - with *Query tool*, 274–276
- default actions, 256
- drop rules, 257
 - creating, 258, 261, 264
- inactive, 265–266
- inspection rules, 256–257
 - customizing, 266–273
- offsets, 266
 - syntax, 276
- variables for customization, 274

S

- sample seed file, CS-MARS, 319–320
- Sarbanes-Oxley Act, 9
- Sasser worm, 41
- security and financial audit requirements, reporting, 247
- security policies, enforcing, 42
- security tools and testing sites, 298
- seed file input, network discovery, 86
- selecting location for CS-MARS deployment, 102–104
- sequential path information attack diagram, 84
- serial console access on CS-MARS, 349–350
- server sensors (ISS), configuring, 322–323
- sessions, 76
- setting up CS-MARS, 108
- severity level variable, 274
- SIC communication, enabling, 354
- signature matching, 31
- SIM (security information management), 5
 - core functions, 6–8
 - migrating to STM, 12
 - multivendor solution, 21–22
 - third-party vendors, certification, 21
- SiteProtector, 320
- small business success stories, 289–290
- SmartCenter servers, 166
- SMB networks, deploying CS-MARS, 17–18

SNMP (Simple Network Management Protocol)

- configuring
 - for *Cisco PIX firewall/CS-MARS communication*, 163
 - for *router/CS-MARS communication*, 146
 - on *ExtremeWare switches*, 159
- MIBs for network discovery, 87

Snort IPS Sensor

- adding to CS-MARS database, 187–188
- communication with CS-MARS, configuring, 187

spam, 53**spyware, 52****SSH (Secure Shell), configuring for Cisco PIX firewall/CS-MARS communication, 161–162****standalone deployment (CS-MARS), 45****standard attack vector diagram, 84****standard path analysis attack diagram, 84****state government success stories, 283–284****static data, 92****STM (security threat mitigation), 5, 11–12, 41****storage requirements for CS-MARS****database, 79–80****storing event data, 6****success stories, 283–290****Summary Dashboard**

- Attack diagram, 214
- HotSpot graph, 213–214
- incidents, viewing, 208–209
- Information Summary column, 216, 219
- Path column, 211–213
- Time vs. Rate graph, 214
- X, Y axis graphs, interpreting, 219

Sun Solaris OS

- adding to CS-MARS database, 194
- configuring CS-MARS communication, 193–194

superV process, 333**supported CS-MARS devices**

- AAA logs, data type definition and usage, 137
- AAA servers, 144
- antivirus, 142
- antivirus server logs, data type definition and usage, 136
- classifications of, 132
- data type definitions and usage (table), 133–137

- database logs, data type definition and usage, 136
 - database servers, 144
 - firewalls, data type definition and usage, 134, 140
 - host IDS, 142
 - data type definition and usage, 135*
 - host OS, 143
 - mitigation devices, 138
 - network IDS/IPS devices, 141
 - data type definition and usage, 135*
 - reporting devices, 137
 - router/switch devices, 139
 - data type definition and usage, 133*
 - security events, data type definition and usage, 136
 - SNMP, 145
 - data type definition and usage, 137*
 - switches, data type definition and usage, 133
 - syslog data, data type definition and usage, 137
 - syslog servers, 145
 - table, 138
 - VPN devices, 141
 - data type definition and usage, 134*
 - vulnerability assessment data, 143
 - data type definition and usage, 136*
 - web proxy devices, 144
 - data type definition and usage, 136*
 - web server logs, data type definition and usage, 136
 - web servers, 144
 - switches**
 - CS-MARS communication, configuring, 151
 - L2 discovery, 151–154*
 - NAC-specific messages, 156–158*
 - NetFlow, 158*
 - syslog, 155–156*
 - ExtremeWare, configuring CS-MARS communication, 159–160*
 - Symantec ManHunt**
 - adding to CS-MARS database, 182–183
 - communication with CS-MARS, configuring, 181
 - syntax for multiple-offset rules, 276**
 - syslog**
 - configuring for Juniper NetScreen firewall/CS-MARS communication, 164
 - configuring for switch/CS-MARS communication, 155
 - on switches running CATOS, 155–156*
 - on switches running IOS, 155*
 - configuring for router/CS-MARS communication, 147
 - system-determined false positives, 91**
 - system inspection rules, customizing, 266–273**
 - system parameters**
 - configuring on CS-MARS, 127–128
 - entering, 111–113
 - system rules, 257**
-
- ## T–U
- tangible costs of cyberattacks, 54–57**
 - TCO (total cost of ownership), 49, 63–64**
 - technical evaluation worksheet, CS-MARS, 315, 319**
 - Telnet, configuring for Cisco PIX firewall/CS-MARS communication, 161**
 - third-party CS-MARS-supported devices, 138**
 - AAA servers, 144
 - antivirus devices, 142
 - database servers, 144
 - firewall devices, 140
 - host IDS devices, 142
 - host OS devices, 143
 - network IDS devices, 141
 - router/switch devices, 139
 - SNMP, 145
 - syslog servers, 145
 - VPN devices, 141
 - vulnerability assessment devices, 143
 - web proxy devices, 144
 - web servers, 144
 - third-party VA tools, 93**
 - Time field (Summary Dashboard), 208**
 - time range variable, 274**
 - Time vs. Rate graph (Summary Dashboard), 214**
 - Top N variable, 246**
 - topologies, methods of network discovery, 86–87**
 - Total view report format, 246**

traffic filtering, 28
traffic monitoring, 88
 NetFlow, 89
 with NetFlow, behavioral profiling, 89–90
Trojan horses, 53
undetermined false positives, 91
unified security platform, 10–11
user-defined rules, 257
users, creating, 121–122

V

VA (vulnerability analysis), 92
 methods of information retrieval
 Nessus, 92
 third-party tools, 93
variables
 for custom rule creation, 274
 for report formatting, 246
verifying communications parameters on Check Point devices, 358
viewing
 drop rules, 257
 incident ID, 229–232
 incident vector information in Summary Dashboard, 212–213
 incidents (Summary Dashboard), 208–211
 vector information, 212–213
 inspection rules, 256
 maintenance parameters on CS-MARS, 126–127
 predefined reports with Report tab, 248
viruses, 52

VPN 3000 Series Concentrators
 adding to CS-MARS database, 200
 communication with CS-MARS, configuring, 199
vulnerability of U.S infrastructure to cybercrime, 50
vulnerability scanning, configuring on CS-MARS, 124

W

web interface, entering system parameters, 111–113
web servers, configuring communication with CS-MARS
 Apache, 196–198
 Microsoft IIS web server, 194–195
websites
 government security controls and information, 296–297
 security tools and testing, 298
 security-related, 295–296
Windows OS, configuring CS-MARS communication, 189–191
worms, 52
 Sasser, 41

X–Z

X, Y axis graphs, interpreting, 219
zero-day, 61
zero-day attacks, 61
zombies, 53