INDEX

SYMBOLS

$Target variables (IP addresses), 121

A

AAA servers, NAC Framework, 213
Action option (query interface), 96
actions
  alerting actions list, 125
  rules, attaching to, 125
addressable implementation specification (HIPPA Security Rule), 30
admin groups, troubleshooting e-mail notifications, 203
Administrative Safeguards (HIPPA Security Rule), 30-31
Advanced Regex queries, 287
alerting actions list (rules), 125
alerts, 13
All Events and NetFlow-Top Destination Ports graph (Dashboard), 23
All False Positives section (Dashboard), 22
All-Top Destinations chart (Network Status page), 24
All-Top Event Types chart (Network Status page), 24
All-Top Reporting Devices chart (Network Status page), 24
All-Top Rules Fired chart (Network Status page), 24
All-Top Sources chart (Network Status page), 24
antivirus software, Maintain a Vulnerability Management Program category (PCI Data Security Standard), 49
ANY variables (IP addresses), 121
appliances, inherent security, 78-79
approver role (CS-Manager), 184
archives
  archive server
    configuring, 165-166
    planning/selecting, 164-165
  CS-MARS, configuring, 166
direct access of archived events, 173
directory structures, 283
querying
  Advanced Regex queries, 287
  command-line queries, 284-285
  common query text files, 288
  customizing queries, 286-287
  ES directories, 284
  marchive.py utility source code, 289-292
  user rights, 283
  web applications, 285
  zgrep command, 284-285
restoring
  from, 168-169
to reporting appliances, 170-172
retrieving raw events, 173-174
subdirectory structures, 284
Attack Diagram (Dashboard), 22

B - C

batch query reporting method, 93
batch reports, 108-114, 117-119
beeping noises (MARS hardware), troubleshooting, 194
botnets, 38
Build and Maintain a Secure Network category (PCI Data Security Standard), 45-46
built-in reports
default reports list, 92
report groups list, 89-91
case notes, incident investigation, 151
case studies, CS-MARS deployments, 71-72
Check Point logs, troubleshooting, 200
Cisco CSC Module, 226
CISP (Cardholder Information Security Program), PCI Data Security Standard, 42
civil penalties, 23-24, 29
compliance validation requirements (PCI Data Security Standard), 56
configuring
  archive server, 165-166
  CS-Manager, 184-187
CS-MARS
archiving, 166
CS-Manager integration, 185-187
NAC Framework reporting, 214
GC, 263
containment step (incident investigation), 133
covered entities, HIPPA, 28-29
credit cards, PCI Data Security Standard, 42
criminal penalties, HIPPA noncompliance, 29
CSC Module, custom parsers, 249, 255
CS-Manager
approver role, 184
configuring, 184-185
CS-MARS integration, 185-187
Device view, 181-182
firewalls, 188
help desk role, 184
Map view, 181
network administrator role, 184
network operator role, 184
policy lookup, 189
Policy view, 181-182
system administrator role, 185
CS-MARS-GC (Global Controller), 261
CSV view (Report Wizard), 111
CTA (Cisco Trust Agent), NAC Framework, 211-212
custom parsers, 219
adding
devices/applications, 223
log templates, 225-226
Cisco CSC Module, 226
CSC Module, 249, 255
GC, 276
log messages, sending to MARS, 220-221
log templates, 241
fifth log templates, 239
first log templates, 226, 229-232, 235
fourth log templates, 239
second log templates, 235-236
third log templates, 235-236
monitored devices/software, 242
parse, determining what to, 222-223
parsed fields, 229
queries, 243-244
reports, 245
rules, 246-248
customizing archive queries, 286-287

D

Dashboard, 21, 271
All False Positives section, 22
Attack Diagram, 22
Events and NetFlow chart, 23
Events and Sessions chart, 23
Events section, 22
False Positive Events chart, 23
HotSpot Graph, 22
Incidents section, 22
Recent Incidents Table, 22
data access restrictions, Implement Strong Access
Control Measures category (PCI Data Security Standard), 50
default reports list, 92
degraded RAID arrays, troubleshooting, 194-196
deployment scenarios
GC, 59-61
LC, 59-60
sizing deployments, 63
determining EPS, 65-66
determining storage requirements, 67-68
find command, 67
flood conditions, 69
future growth considerations, 69
grep tool, 66
healthcare case study, 72
IPS considerations, 64-65
maximum EPS table, 64
reporting performance, 69
retail chain case study, 71
state government case study, 71
topology awareness planning, 70
standard controllers, 59-60
Destination IP option (query interface), 95
destination port numbers list, 98
device events, receiving, 205
Device option (query interface), 95
Device view (CS-Manager), 181-182
disaster recovery, archiving, 167
configuring
archive server, 165-166
CS-MARS, 166
direct access of archived events, 173
planning/selecting archive server, 164-165
restoring from, 168-169
restoring to reporting appliances, 170-172
retrieving raw events, 173-174
disk usage command, determining disk storage space, 203
DISTINCT variables (IP addresses), 121
documenting installations, 193
drop rules, 127
  creating, 128-131
  creating/editing, false-positive tuning, 152, 156

e g e r s  f i r e w a l l  r u l e s ,  8 3 - 8 4
e-mail, troubleshooting admin group notifications, 203
encryption, Protect Cardholder Data category (PCI Data Security Standard), 48
eradication step (incident investigation), 134
ES directories, querying archives, 284
event collection/correlation (SIM), 7
event logs, troubleshooting, 197-200

e n t s  m e s s a g e s
  NetFlow, 9
  SDEE, 11
  SNMP, 10-11
  Syslog, 10

events
  defining, 13
  determining details of (incident investigation), 149
  device events, troubleshooting, 205
types (queries), filtering, 102
Events and NetFlow chart (Dashboard), 23
Events and Sessions chart (Dashboard), 23
Events option (query interface), 95
Events section (Dashboard), 22

F

False Positive Events chart (Dashboard), 23
False Positive Wizard, 152-153, 156
false positives
  All False Positives section (Dashboard), 22
  defining, 17-18
  system-determined false positives, defining, 19-20
unconfirmed false positives, defining, 18
user-confirmed false positives, defining, 19
FDIC (Federal Deposit Insurance Corporation), Gramm-Leach Bliley Act, 36
filtering query event types, 102
financial institutions, Gramm-Leach-Bliley Act, 35
Financial Privacy Rule (Gramm-Leach-Bliley Act), 35
find command, sizing CS-MARS deployments, 67
firewalls, 188
egress firewall rules, 83-84
  ingress firewall rules, 82
installing, Build and Maintain a Secure Network category (PCI Data Security Standard), 45-46
flood conditions, CS-MARS deployments, 69
forensics, 135
cases, creating, 136-138
containment step, 133
eradication step, 134
false-positive tuning
  creating/editing drop rules, 152, 156
  determining where to tune, 151
  editing system rules, 152, 157-161
False Positive Wizard, 152-153, 156
identification step, 133
initial investigations, 136-138
  port numbers, 140
  tracking affected IP addresses, 139
lessons learned step, 134
preparation step, 133
recovery step, 134
viewing incident details
  case notes, 151
  changing views, 145
  determining what events mean, 149
  disabling switch ports, 145
  graphical view, 142-144
  host color codes, 142
  logical view, 141
  mitigation options, 144
  physical view, 142
  session graph options, 144
  tracking attacker activities, 147
  viewing raw log messages, 146
G

GC (Global Controller), 59-61
configuring, 263
CS-MARS-GC, 261
custom parsers, 276
Dashboard, 271
drilling down into incidents, 272
global rules, versus local rules, 274
installing, 263
  enabling communications between controllers, 264, 268
troubleshooting, 269
logging in/out, 270
overview of, 262
queries/reports, 273
reasons for deploying, 261
recovery, 278
security and monitor devices, 275
software upgrades, 276-277
zones, 262-263, 269
global rules versus local rules, 274
Gramm-Leach-Bliley Act
affected individuals/companies, 35
financial institutions, 35
Financial Privacy Rule, 35
penalties for noncompliance, 36
Pretexting Provisions, 35
Safeguards Rule, 35-36
  employment management/training, 37
  information systems, 37-38
  security monitoring, 40
  system failure management, 38-39
graphical view (incident investigation), 142-144
grep tool, sizing CS-MARS deployments, 66

H

hard disk storage space, determining, 202-203
hardware (MARS), troubleshooting, 193
  beeping noises, 194
  degraded RAID arrays, 194-196
healthcare case study (CS-MARS deployments), 72
Healthy Secure Posture reports (NAC Framework), 214
held desk role (CS-Manager), 184

HIPPA (Health Insurance Portability and Accountability Act)
covered entities, 28-29
noncompliance, 29
Security Rule
  addressable implementation specification, 30
  Administrative Safeguards, 30-31
effort/cost of, 34
  Physical Safeguards, 30-32
  required implementation specification, 30
  security monitoring, 33-34
  Technical Safeguards, 30-33
HotSpot Graph (Dashboard), 22
hotswap command, degraded RAID arrays, 195-196

identification step (incident investigation), 133
IDS, network security, 85-86
ifconfig command, troubleshooting device events, 205
Implement Strong Access Control Measures category (PCI Data Security Standard)
data access restrictions, 50
restricting physical access to cardholder data, 52
unique ID assignments, 51
implementation specifications (HIPPA Security Rule), 30
incident investigation, 135
cases
  creating, 136-138
  notes, 151
containment step, 133
eradication step, 134
false-positive tuning
  creating/editing drop rules, 152, 156
determining where to tune, 151
ingesting system rules, 152, 157-161
False Positive Wizard, 152-153, 156
identification step, 133
incidents, defining, 15
initial investigations, 136-138
port numbers, 140
  tracking affected IP addresses, 139
lessons learned step, 134
preparation step, 133
recovery step, 134
viewing incident details
  changing views, 145
determining what events mean, 149
disabling switch ports, 145
  graphical view, 142-144
  host color codes, 142
  logical view, 141
mitigation options, 144
  physical view, 142
session graph options, 144
  tracking attacker activities, 147
viewing raw log messages, 146
Incidents chart (Network Status page), 24
Incidents section (Dashboard), 22
ingress firewall rules, 82
inherent security, 78-79
inline query reporting method, 93
installing
documenting installations, 193
firewalls, Build and Maintain a Secure Network category (PCI Data Security Standard), 45-46
GC, 263
enabling communications between controllers, 264, 268
troubleshooting, 269
internal controls, Sarbanes-Oxley Act, 41-42
IP addresses
  $Target variables, 121
  ANY variables, 121
  DISTINCT variables, 121
  SAME variables, 121
tracking, incident investigation, 139
IPS (Intrusion Prevention Systems)
  CS-MARS deployments, 64-65
  network security, 85-86
J - K - L
JBoss, 268
Key Pattern field, custom parsers, 229
Keyword option (query interface), 96
keywords
  matches within queries, 96
  queries, 107
LC (local controllers), 59-60
lessons learned step (incident investigation), 134
local rules versus global rules, 274
log messages
  NetFlow event messages, 9
  SDEE event messages, 11
  SNMP event messages, 10-11
  Syslog event messages, 10
  viewing raw log messages (incident investigation), 146
log templates
  CSC Module, 249, 255
custom parsers, 241
    adding to, 225-226
    fifth log templates, 239
    first log templates, 226, 229-232, 235
    fourth log templates, 239
    second log templates, 235-236
    third log templates, 235-236
logging in/out of GC, 270
logical view (incident investigation), 141
M
Maintain a Vulnerability Management Program category (PCI Data Security Standard), 49-50
Maintain an Information Security Policy category (PCI Data Security Standard), 55
Map view (CS-Manager), 181
marchive.py utility source code, querying archives, 289-292
MARS
  alerts, 13
  hardware, troubleshooting, 193
    beeping noises, 194
    degraded RAID arrays, 194-196
  mitigation, 13
  purpose of, 12
  query engine, 13
  reporting, 13
  rules engine, 13
topologies, 12
visualization, 12
merchant levels (PCI Data Security Standard), 43
messages (event)
  NetFlow, 9
  SDEE, 11
O - P

on-demand reports, creating, 97-108
Operation option (query interface), 96

Parsed field, custom parsers, 229
passwords (system), Build and Maintain a Secure Network category (PCI Data Security Standard), 46

Pattern Name field, custom parsers, 229
PCI Data Security Standard, 42
affected individuals/companies, 43
Build and Maintain a Secure Network category (PCI Data Security Standard), 45-46
categories/requirements table, 44
compliance validation requirements, 56
Implement Strong Access Control Measures category, 50-52
Maintain a Vulnerability Management Program category, 49-50
Maintain an Information Security Policy category, 55
merchant levels, 43
penalties for noncompliance, 43
Protect Cardholder Data category, 47-48
Regularly Monitor and Test Networks category, 53-54

Peak view (Report Wizard), 111
performance, CS-MARS deployments, 69
Physical Safeguards (HIPPA Security Rule), 30-32
physical view (incident investigation), 142
pndbusage command, 203
pnrestore command, restoring from archives, 168-169, 172
policy lookup (CS-Manager), 189
Policy view (CS-Manager), 181-182
port numbers
destination port numbers list, 98
incident investigation, 140

Position 1 field, custom parsers, 229
posture checks (NAC Framework), 213-214
posture validation servers, NAC Framework, 213
preparation step (incident investigation), 133
prepopulating queries, 98
Pretexting Provisions (Gramm-Leach-Bliley Act), 35
Protect Cardholder Data category (PCI Data Security Standard), 47-48
Python, querying archives via marchive.py utility source code, 289-292

queries
archives, 283
  Advanced Regex queries, 287
  command-line queries, 284-285
  common query text files, 288
  customizing queries, 286-287
  ES directories, 284
  marchive.py utility source code, 289-292
  user rights, 283
  web applications, 285
  zgrep command, 284-285
custom parsers, 243-244
default time periods of, 99
filtering event types, 102
GC, 273
keyword matches, 96
keywords, 107
multiple-line queries, creating via Operation field, 96
prepopulating, 98
query interface, 93
  Action option, 96
  Destination IP option, 95
  Device option, 95
  Events option, 95
  Keyword option, 96
  Operation option, 96
  Reported User option, 95
  Rule option, 96
  Service option, 95
  Source IP option, 95
report groups list, 89-91
Report Wizard, 108-114, 117-119
Reported User option (query interface), 95
reporting, 7, 13
reporting methods, 93
rerunning, 105
submitting, 103-104
query engine, 13

RAID arrays, troubleshooting, 194, 196
raidstatus command, degraded RAID arrays, 194, 196
raw events, retrieving from archives, 173-174
raw log messages, viewing (incident investigation), 146
real-time query reporting method, 93
Recent Incidents Table (Dashboard), 22
Recent view (Report Wizard), 111
recovery
  disaster, archiving, 164, 167
  configuring archive server, 165-166
  configuring CS-MARS, 166
  direct access of archived events, 173
  planning/selecting archive server, 164-165
  restoring from, 168-169
  restoring to reporting appliances, 170-172
  retrieving raw events, 173-174
GC, 278
recovery step (incident investigation), 134
Regularly Monitor and Test Networks category (PCI Data Security Standard), 53-54
reports
batch reports, 108-109, 111-114, 117-119
built-in reports
  default reports list, 92
  report groups list, 89-91
custom parsers list, 245
GC, 273
on-demand reports, creating, 97-108
query interface, 93-96
reporting methods, 93
required implementation specification (HIPPA Security Rule), 30
restoring from archives, 168-172
retail chain case study (CS-MARS deployments), 71
routing protocols, 98
Rule option (query interface), 96
rules, 120
actions, attaching to, 125
alerting actions list, 125
creating, 121, 125-126
custom parsers, 246-248
defining, 14, 121
drop rules, 127-131
queries, submitting as, 104
rules engine, 13

S

Safeguards Rule (Gramm-Leach-Bliley Act), 35-36
employment management/training, 37
information systems, 37-38
security monitoring, 40
system failure management, 38-39
SAME variables (IP addresses), 121
Sarbanes-Oxley Act, 40-42
SDEE (Simple Device Event Exchange), event messages, 11
security
Check Point logs, troubleshooting, 200
CS-Manager
approver role, 184
configuring, 184-185
CS-MARS integration, 185-187
Device view, 181-182
firewalls, 188
help desk role, 184
Map view, 181
network administrator role, 184
network operator role, 184
policy lookup, 189
Policy view, 181-182
system administrator role, 185
GC, 275
inherent security, 78-79
monitoring, Safeguards Rule (GLB Act), 40
networks, 81
egress firewall rules, 83-84
IDS, 85-86
ingress firewall rules, 82
IPS, 85-86
security management networks, 79-80
Security Rule (HIPPA)
addressable implementation specification, 30
Administrative Safeguards, 30-31
Physical Safeguards, 30-32
required implementation specification, 30
security monitoring, 33-34
Technical Safeguards, 30-33
Service option (query interface), 95
session graph options (incident investigation), 144
sessionization, 5, 8
sessions, defining, 14
SIM (Security Information Management)
alerting, 8
event collection/correlation, 7
mitigation, 8
networks, role in, 6-7
reporting, 7
sessionization, 8
topology awareness, 8
sizing CS-MARS deployments, 63
EPS
determining, 65-66
maximum EPS table, 64
find command, 67
flood conditions, 69
future growth considerations, 69
grep tool, 66
healthcare case study, 72
IPS considerations, 64-65
maximum EPS table, 64
reporting performance, 69
retail chain case study, 71
state government case study, 71
storage requirements, determining, 67-68
topology awareness planning, 70
SNMP (Simple Network Management Protocol), 10-11, 220
snmpwalk command, troubleshooting unknown reporting device IP, 198
software upgrades, GC, 276-277
Source IP option (query interface), 95
SOX Act. See Sarbanes-Oxley Act
SSH (Secure Shell), 78-79
standalone controllers, 59-60
state government case study (CS-MARS deployments), 71
storage
  CS-MARS deployments, requirements for, 67-68
  hard disk space, determining, 202-203
switch ports, disabling (incident investigation), 145
Syslog, 10, 220
system administrator role (CS-Manager), 185
system failures, managing, 38-39
system passwords, Build and Maintain a Secure Network category (PCI Data Security Standard), 46
system rules, editing, 152, 157-161
system-determined false positives, defining, 19-20

e-mail, admin group notifications, 203
event logs, 200
GC installations, 269
MARS hardware, 193-196
monitored device logs, 201
unknown reporting device IP, 197-199

U - V

UDP ports
destination port numbers list, 98
MARS communication requirements, 80-81
unconfirmed false positives, defining, 18
unique ID, Implement Strong Access Control Measures category (PCI Data Security Standard), 51
unknown reporting device IP, troubleshooting, 197-199
upgrades (software), GC, 276-277
user-confirmed false positives, defining, 19
validation, compliance validation requirements (PCI Data Security Standard), 56
Value Type field, custom parsers, 229
viewing
  incident details (incident investigation)
  changing views, 145
determining what events mean, 149
disabling switch ports, 145
  graphical view, 142-144
  host color codes, 142
  logical view, 141
  mitigation options, 144
  physical view, 142
  session graph options, 144
  tracking attacker activities, 147
  viewing raw log messages, 146
raw log messages (incident investigation), 146
visualization, 12
vulnerabilities
  managing
    Maintain a Vulnerability Management Program category (PCI Data Security Standard), 49-50

T

TCP ports
destination port numbers list, 98
MARS communication requirements, 80-81
tcpdump command, troubleshooting
device events, 205
monitored device logs, 201
Technical Safeguards (HIPPA Security Rule), 30, 32-33
topologies, 12
  awareness, SIM, 8
  CS-MARS deployments, 70
Total view (Report Wizard), 111
tracking
  attacker activities (incident investigation), 147
  IP addresses, incident investigation, 139
troubleshooting
  Check Point logs, 200
device events, 205

e-mail, admin group notifications, 203
event logs, 200
GC installations, 269
MARS hardware, 193-196
monitored device logs, 201
unknown reporting device IP, 197-199
W

wizards

False Positive Wizard, 152-153, 156
Report Wizard, 108-114, 117-119

X - Y - Z

zero-day attacks, 39
zgrep command, querying archives, 284-285