



INDEX

A

acceptable use policies, 155–156, 247
actions, rules, 277–281
Ad Supported Software, 8
ADI (Application Deployment Investigation), 24–25
Adware, 8
Agent Kit, 133
 creating, 133–137
 files, 139–142
 retrieval, 137–138
Agent Service Control rule, 22
Agent UI Control rule, 22
agent.bundle file, 140
agent.rul file, 140
agent.var file, 140
agents
 CSA upgrades, 265
 diagnostics, CSA 5.0 searches, 283
 identifying number and type, 249
 monitoring deployment, 261–262
 security policy changes, 90, 92–93
 test mode deployment, 255–256
ALE (Annual Loss Expectancy), calculating, 248
Application Behavior Investigation, 25, 197
Application Control rule, 22, 176
Application Deployment Investigation (ADI), 24–25
Application Deployment Unprotected Hosts report, 264
applications
 control options, 32
 control policies, 174–175
 desktop environment, 40–41
 examining uses, 249
 implementation testing, 256–258
 lab testing, 264
 protection goal, 250
 security policies, 166–167
 Microsoft SQL Server 2000-Windows rule module, 170
 Web Server-Apache rule module, 169–170

Web Server-iPlanet-Solaris rule module, 168
 Web Server-Microsoft IIS-Windows rule module, 167–168
 security policy association, 157–159
 tag marking, 33
 tracking, 31
architectures, server configurations, 109
assets, classifying, 249
auditing security policies, 155

B

backups
 project implementation plan, 76
 system maintenance, 263
bots, malicious code, 7

C

CCO ID, 241
change control documentation, 89–9
Change Filter option, Event Log, 203–205
Cisco website, 15
Cisco Security Agent. *See* CSA
Cisco Security Agent Management Console (CSA MC), 17
 communication, 17–18
 configuration management and event reporting, 18
 MSDE (Microsoft SQL Server Desktop Engine), 19
Cisco TAC, 240–241
Cisco website, 246
 licensing, 241
classes, custom policies, 182
Clipboard Access Control rule, 21
CMS ARS document, 11–12
COM Component Access Control rule, 21
command-line parameters, SETUP.EXE, 143–144

Common Services component, 110**communications, CSA MC (Cisco Security Agent Management Console), 17–19****components**

CSA MC (Cisco Security Agent Management Console), 17

communication, 17–18

configuration management and event reporting, 18

MSDE (Microsoft SQL Server Desktop Engine), 19

network communication, 19

Security Agent software, 16

configurations, server hardware, 109**Connection Rate Limiting rule, 22****contact lists, documentation, 100–101****contributors, project implementation plan, 50****critical assets, classifying, 249****CSA (Cisco Security Agent), 5. *See also* CSA 5.0**

ADI (Application Deployment Investigation), 24–25

Application Behavior Investigation, 25

capabilities, 15

components

CSA MC (Cisco Security Agent Management Console), 17–19

network communication, 19

Security Agent software, 16

deployment, 131

Agent Kit, 133–142

installation requirements, 131–133

host groups, 19–20

creative usage, 20–21

mandatory, 20

policies, 21–24

troubleshooting, 217

event logs, 222–223

licensing, 217–219

name resolution, 219

network shim, 220–221

NOC, 221–222

remote control, 223–225

tools, 225, 228

CSA 5.0, 267

agent diagnostics, 283

database maintenance, 284

event log, 271

group level changes, 272–273

hosts, 273–276

operating system, 267

rules, 277

actions, 277–281

modules, 276

searches, 281–282

security agent, 285

Status Summary screen, 268

Most Active section, 269–270

Network Status section, 268–269

system warnings, 267

CSA MC (Cisco Security Agent Management Console), 17

communication, 17–18

configuration management and event reporting, 18

MSDE (Microsoft SQL Server Desktop Engine), 19

CSACTL, troubleshooting CSA, 229–230**CSAgent-Install.log, 232**

troubleshooting event logs, 223

csalog.txt, 217–219, 232**CSAMC45-install.log file, 223****custom policies**

Application Behavior Investigation, 197

Monitor Rules, 196–197

reasons for default change, 173

application control, 174–175

exception rules, 173–174

monitoring system interactions, 175

samples, 182

dynamic application classes, 191–196

state-based policies, 183–190

tuning process, 175

best practices, 180–182

dynamic application classes, 179–180

rule capabilities, 175–176

state sets, 176–179

D

- data protection, 33**
- Data Access Control rule, 22**
- data1.hdr file, 141**
- data1.zip file, 141**
- data2.zip file, 141**
- databases**
 - CSA 5.0, 284
 - Event, 201–202
 - automated filtering from direct links, 212–214*
 - event correlation, 214–215*
 - Event Log, 202–208*
 - Event Monitor, 210–212*
 - maintenance, 263
 - project implementation plan, 76
- DBCC SHRINKFILE, 239**
- DDoS (Distributed Denial of Service), 7**
- deleting events, 237–239**
- deployment**
 - CSA, 131
 - Agent Kit, 133–142*
 - installation requirements, 131–133*
 - executive sponsor, 43
 - guidelines, 245–246
 - information gathering, 246–252*
 - maintenance, 263–265*
 - pilot phase, 252–260*
 - protect mode, 262–263*
 - test mode, 260–262*
 - information gathering
 - environment, 35–42*
 - purpose definition, 30–35*
 - project manager, 43
 - project team, 43
 - support teams, 44–45
- desktops**
 - implementation environment, 38–39
 - applications, 40–41*
 - operating system support, 39*
 - security policies
 - Linux, 165*
 - Solaris, 165–166*
 - Windows, 162–165*

- detected access option, 279**
- detected boot option, 278**
- detected rootkit option, 278**
- detection rules, 22**
- diagnostics**
 - agent, 283
 - troubleshooting CSA, 230–231
- Distributed Denial of Service (DDoS), 7**
- documentation**
 - change control, 89–93
 - contact and support lists, 100–101
 - pilot phase, 259–260
 - project implementation plan, 75
 - quality assurance, 93–94
 - debugging, 94–99*
 - hardware platform testing, 100*
 - security policy, 81–88
- dump files, 232**
- dynamic application classes, custom policies, 179–180, 191–196**

E

- electronic personal health information (ePHI), 11**
- enforcement rules, 22**
- engine32.zip file, 141**
- environment, CSA implementation, 35**
 - desktops, 38–41
 - laptops, 38–41
 - network, 35–37
 - operations analysis, 41–42
 - servers, 37–38
- ePHI (electronic personal health information), 11**
- espionage, hackers, 9–10**
- Ethereal, troubleshooting CSA, 226**
- Event databases, 201–202**
 - automated filtering from direct links, 212, 214
 - event correlation, 214–215
 - Event Log, 202–203
 - Change Filter option, 203–205*
 - Eventset filtering option, 207*
 - Find Similar filtering option, 208*
 - Event Monitor, 210–212

event logs, 202–203

- Change Filter option, 203–205
- CSA 5.0, 271
- Eventset filtering option, 207
- Find Similar filtering option, 208
- project implementation plan, 77
- troubleshooting CSA, 222–223

Event Monitor, 210–212

events

- correlation, 214–215
- deleting, 237–239

Eventset filtering option, 207

exception rules, 173–174

executive sponsors, implementation, 43, 50

Explain Rules link, 161

F

File Access Control rule, 22, 176

File option, 279

File Version Control rule, 21

files, Agent Kit, 139–140, 142

Filter Events option (Event Log), 271

filters, Event Log

- automated from direct links, 212, 214
- Change Filter option, 203–205
- Eventset filtering option, 207
- Find Similar filtering option, 208

Find Similar filtering option, 32, 208

G

goals, identifying for implementation, 250–252

government, legislation, 10–11

- HIPAA (Health Insurance Portability and Accountability Act), 11–12
- Sarbanes-Oxley, 12
- Senate Bill 1386, 12–13
- Visa PCI, 13

groups

- hosts, 19–20
 - creative usage, 20–21*
 - mandatory, 20*
- levels, CSA 5.0, 272–273

guidelines, implementation, 245–246

- information gathering, 246–252
- maintenance, 263–265
- pilot phase, 252–260
- protect mode, 262–263
- test mode, 260–262

H

hackers, 9

- insiders, 10
- script kiddies, 9
- targeted espionage, 9–10

hardware

- platform testing documentation, 100
- server installation requirements, 109–110

Health Insurance Portability and Accountability Act (HIPAA), 11–12

hierarchy, policies, 23–24

HIPAA (Health Insurance Portability and Accountability Act), 11–12

Host Address option, 279

Host Recycle Bin (CSA 5.0), 273–276

hosts

- converting to protect mode, 262
- CSA 5.0, 273–276, 281
- groups, 19–21

I

ICCPING, troubleshooting CSA, 228–229
implementation

- executive sponsor, 43
- guidelines, 245–246
- information gathering, 246–252
- maintenance, 263–265
- pilot phase, 252–260
- protect mode, 262–263
- test mode, 260–262
- information gathering
 - environment, 35–42*
 - purpose definition, 30–35*
- project manager, 43
- project plan, 73–74

project team, 43
support teams, 44–45

importing custom policies, 181–182
information, gathering for CSA implementation, 246

Acceptable Use Policy, 247
environment, 35–42
goal determination, 250–252
inventory, 249
purpose definition, 30–35
Security Policy, 247
security problems, 248–249

Insecure option, 278

insiders, hackers, 10

installing

CSA, requirements, 131–133
servers, 107, 110
 hardware requirements, 109–110
 multiple server, 122–129
 single server, 110–122
 single servers, 107–108
 three server, 108–109
 two server, 108
SETUP.EXE, 142
 command-line parameters, 143–144
 uninstall, 144–148

intellectual properties, protection, 33

inventories, information gathering, 249

K-L

Kernel Protection rule, 21

laptops, implementation environment, 38–39

applications, 40–41
operating system support, 39

layout.bin file, 141

legislation, 10–11

HIPAA (Health Insurance Portability and
Accountability Act), 11–12
Sarbanes-Oxley, 12
Senate Bill 1386, 12–13
Visa PCI, 13

licensing

Cisco.com, 241
troubleshooting, 217–219

Linux

CSA requirements, 133
desktop security policies, 165
network shim, 221
operating system requirements, 16
troubleshooting event logs, 223

local users, security policies, 156

log files, troubleshooting CSA, 232

logs

application testing, 256–258
project implementation plan, 76
system monitoring, 262

M

maintenance

implementation

Application Deployment Unprotected
 Hosts report, 264
 CSA upgrades, 264–265
 database, 263
 patch testing, 263–264
 system backups, 263
project implementation plan
 backups, 76
 database maintenance, 76
 event logs, 77
 logs, 76
 policy exports, 77
 policy updates, 77

malicious codes, 5

Adware, 8
bots, 7
spyware, 8
trojans, 7
viruses, 6
worms, 6–7

mandatory groups, 20

metrics, project implementation plan, 52–59

Microsoft, operating system requirements, 16

**Microsoft SQL Server 2000-Windows rule
module, 170**

**Microsoft SQL Server Desktop Engine (MSDE),
19**

modules, rules, 23

Monitor Rules, custom policies, 196–197

Monitoring Filter, 210–212**Most Active section (CSA Status Summary screen), 269–270****MS SQL 2000**

- multiple server installation, 122–129
- single server installation with, 122
- upgrading MSDE installation, 119–122

MS SQL Database, 201**MSDE (Microsoft SQL Server Desktop Engine)**

- CSA MC (Cisco Security Agent Management Console), 19
- single server installation, 111–119

N

- NAC, custom policies, 189–190
- name resolution, troubleshooting CSA, 219
- net stop crmdmgt command, 119
- net stop csagent command, 119
- NetCat (nc), troubleshooting CSA, 227
- Network Access Control rule, 22, 176
- Network Interface Control rule, 22
- network shim, troubleshooting CSA, 220–221
- Network Status section (CSA Status Summary screen), 268–269
- networks
 - CSA communication, 19
 - implementation environment, 35–37
 - remote security, 187–189
- NMAP, troubleshooting CSA, 227**
- NOC, troubleshooting CSA, 221–222**
- NT Event Log rule, 22**

O**ODBC, troubleshooting, 236****operating systems**

- built-in security policies, 160–161
- CSA, 16, 267
- desktop support, 39

organizations, CSA implementation impact, 250–251**P****patches**

- cycle extensions, 251
- reduced testing time, 32
- system maintenance, 263–264

Pathping, troubleshooting CSA, 226**phased approach**

- project implementation plan, 62–63
- software rollout, 34–35

pilot

- groups, success metrics, 51
- implementation, 252
 - agent deployment in test mode, 255–256*
 - condition determination, 253–254*
 - determining scope, 252–253*
 - documentation, 259–260*
 - policies, 254–255*
 - protection capability testing, 258–259*
- project implementation plan, 65
 - common mistakes, 68–72*
 - expectation defining, 65–67*
 - success criteria, 73*
 - support model, 67–68*
 - testing methods, 72*

Ping, troubleshooting CSA, 225**policies, 21**

- application association, 157–159
- building exceptions, 262–263
- custom
 - Application Behavior Investigation, 197*
 - Monitor Rules, 196–197*
 - reasons for default change, 173–175*
 - samples, 182–196*
 - tuning process, 175–182*
- defaults, 159–160
 - applications, 166–170*
 - desktops, 162–166*
 - operating systems, 160–161*
- documentation, 81–88
- implementation, 254–255
- project implementation plan, 77
- purpose, 154–155
 - audit trail, 155*
 - preventing vulnerability exploitation, 157*

- protection from users, 156*
 - specifying acceptable uses, 155–156*
 - vulnerability protection, 156–157*
 - requirements, 153–154
 - rules, 21–22
 - modules, 23*
 - precedence, 24*
 - precedence rules, 24**
 - problems**
 - hackers, 9
 - insiders, 10*
 - script kiddies, 9*
 - targeted espionage, 9–10*
 - legislation, 10–11
 - HIPAA (Health Insurance Portability and Accountability Act), 11–12*
 - Sarbanes-Oxley, 12*
 - Senate Bill 1386, 12–13*
 - Visa PCI, 13*
 - malicious code, 5
 - Adware, 8*
 - bots, 7*
 - spyware, 8*
 - trojans, 7*
 - viruses, 6*
 - worms, 6–7*
 - processes, protection goals, 250**
 - project implementation plan**
 - contributors, 50
 - documentation, 75
 - implementation rollout, 73–74
 - maintenance
 - backups, 76*
 - database maintenance, 76*
 - event logs, 77*
 - logs, 76*
 - policy exports, 77*
 - policy updates, 77*
 - pilot, 65
 - common mistakes, 68–72*
 - expectation defining, 65–67*
 - success criteria, 73*
 - support model, 67–68*
 - testing methods, 72*
 - success criteria
 - metrics defining, 52–59*
 - phased approach, 62–63*
 - pilot group metrics, 51*
 - ROI, 59–62*
 - success defined, 50–51*
 - training requirements, 63–65*
 - timeline, 47–50
 - project managers**
 - implementation, 43
 - project implementation plan, 50
 - project teams, implementation, 43**
 - protect mode, implementation, 262–263**
 - Protected option, 279**
 - protection capabilities, pilot testing, 258–259**
-
- ## Q
-
- quality assurance, documentation, 93–94**
 - debugging, 94–99
 - hardware platform testing, 100
 - queries (SQL), troubleshooting, 233–237**
-
- ## R
-
- Registry Access Control rule, 22**
 - remote control, troubleshooting CSA, 223–225**
 - remote registry access, custom policies, 185–186**
 - remote users, security policies, 156**
 - Request Trace Files, 232**
 - Resource Access Control rule, 22**
 - review logs, application testing, 256–258**
 - ROI, project implementation plan, 59–62**
 - rollout phases, 34–35**
 - Rootkit/Kernel Protection rule, 22**
 - RTRFORMAT, troubleshooting CSA, 229**
 - rules**
 - CSA 5.0, 277–281
 - CSA 5.0 searches, 282
 - modules, 23, 276
 - policies, 21–22
 - precedence, 24
 - tuning process, 175–176

S

Sans Institute website, 247

Sarbanes-Oxley, 12

script kiddies, hackers, 9

searches, CSA 5.0, 281–283

Secure option, 278

Secure Shell. *See* SSH

security

 problems, 248–249

 threats

hackers, 9–10

legislation, 10–13

malicious code, 5–8

Security Agent software, CSA components, 16

Security level option, 279

security policies

 application association, 157–159

 defaults, 159–160

 desktops, 162–166

 documentation, 81–88

 information gathering, 247

 operating systems, 160–161

 purpose, 154–155

audit trail, 155

preventing vulnerability exploitation, 157

protection from users, 156

specifying acceptable uses, 155–156

vulnerability protection, 156–157

 requirements, 153–154

Senate Bill 1386, 12–13

servers

 desktop security policies

Linux, 165

Solaris, 165–166

Windows, 162–165

 hardware requirements, 109–110

 implementation environment, 37–38

 implementation options, 107

single server, 107–108

three server, 108–109

two server, 108

 installation, 110

multiple server, 122–129

single server, 110–122

service control, troubleshooting CSA, 232–233

Service Restart rule, 22

Set action, 278–281

SETUP.EXE, installation, 142

 command-line parameters, 143–144

 uninstall, 144–148

setup.ibt file, 141

setup.ini file, 141

setup.inx file, 141

setup.iss file, 141

SHRINKFILE, 239

single servers

 implementation options, 107–108

 installation, 110

upgrading to MS SQL 2000, 119–122

with MS SQL 2000, 122

with MSDE (Microsoft SQL Server

Desktop Engine), 111–112, 115–119

Smartnet, 241

Sniffer and Protocol Detection rule, 22

social engineering, 10

Solaris

 CSA requirements, 132

 desktop security policies, 165–166

 operating system requirements, 16

SOX (Sarbanes-Oxley/Sarbanes-Oxley), 12

spyware, malicious code, 8

SQL, troubleshooting, 233

 deleting events, 237–239

 queries, 233–237

SQL Enterprise Manager, 234

SQL Query Analyzer Tool, 234

SQL Server, troubleshooting event logs, 223

SSH (Secure Shell), 224

sslca.cer file, 141

state sets, custom policies, 176–179

state-based policies

 NAC policies, 189–190

 network security, 187–189

 remote registry access, 185–186

 technician agent control, 183–185

Status Summary screen, 268

 Most Active section, 269–270

 Network Status section, 268–269

success criteria

- project implementation plan
 - metrics defining*, 52–59
 - phased approach*, 62–63
 - pilot group metrics*, 51
 - ROI*, 59–62
 - success defined*, 50–51
 - training requirements*, 63–65

Sun operating system requirements, 16**support documentation, contact lists, 100–101****support model, pilot project implementation plan, 67–68****support staff, access, 32****support teams**

- implementation, 44–45
- project implementation plan, 50
- Syslog Control rule, 22
- System API Control rule, 175
- System state sets, 178–179
- systems
 - activity monitoring, 262
 - backups, 263
 - protection goals, 250
 - stability, 252
 - warnings, 267

T**TAC (Cisco), 240–241****targeted espionage, hackers, 9–10****teams**

- executive sponsor, 43
- project implementation, 43
- project implementation plan, 50
- project manager, 43
- support teams, 44–45

technicians, agent control policies, 183–185**Telnet remote control, 224****Terminal services, remote control, 223****test mode**

- agent deployment, 255–256
- implementation, 260–262

testing

- applications, 256–258
- pilot project implementation plan, 72
- system patches, 263–264

threats

- hackers, 9
 - insiders*, 10
 - script kiddies*, 9
 - targeted espionage*, 9–10
- legislation, 10–11
 - HIPAA (Health Insurance Portability and Accountability Act)*, 11–12
 - Sarbanes-Oxley*, 12
 - Senate Bill 1386*, 12–13
 - Visa PCI*, 13
- malicious code, 5–8

three servers

- implementation options, 108–109
- installation, 122
 - MS SQL 2000*, 122–127
 - two CSA MC*, 127–129

timelines, project implementation plan, 47–50**traceroute, troubleshooting CSA, 226****tracking applications, 31****training requirements, project implementation plan, 63–65****trojans, malicious code, 7****troubleshooting**

- CSA, 217
 - event logs*, 222–223
 - licensing*, 217–219
 - name resolution*, 219
 - network shim*, 220–221
 - NOC*, 221–222
 - remote control*, 223–225
 - tools*, 225, 228
- SQL, 233
 - deleting events*, 237–239
 - queries*, 233–237

tuning processes

- best practices, 180–182
- custom policies, 175
 - dynamic application classes*, 179–180
 - rule capabilities*, 175–176
 - state sets*, 176–179

two servers

- implementation options, 108
- installation, 122
 - MS SQL 2000*, 122–127
 - two CSA MC*, 127–129

U

Unix

- network shim, 221
- rules, 22

Unix NT, troubleshooting event logs, 223

Unprotected option, 279

Untrusted Host option, 279

upgrades

- CSA maintenance, 264–265
- custom policies, 181–182
- lab testing, 264
- User state sets, 177

V

variables, custom policies, 182

viruses, malicious code, 6

Visa PCI (Protected Cardholder Information), 13

VNC remote control, 224–225

vulnerabilities

- preventing exploitation, 157
- protection goals, 252
- security policies, 156–157

W

warnings, system, 267

Web Server-Apache rule module, 169–170

Web Server-iPlanet-Solaris rule module, 168

Web Server-Microsoft-IIS-Windows rule module, 167–168

websites

- Cisco, 15, 246
- CMS ARS document, 11
- Sans Institute, 247

Windows

- CSA requirements, 131
- desktop security policies, 162–165
- network shim, 220
- rules, 21–22

worms, malicious code, 6–7