INDEX

Numerics

802.1x, logging in Cisco Secure ACS 14-5

A

AAA devices 14-1
Action 19-3
Activate button 21-18, 21-19, 21-21, 21-23, 23-1
  activating reporting devices 2-27
  what it does 2-27
  when to use 2-27
adding
  cell phone number 22-11, 23-11
  CSV file 2-20
  devices 2-18
    manually 2-18
    seed file 2-20
  drop rules 21-22
  event groups 23-3
  inspection rules 21-19
  pager number 22-11, 23-11
  seed file 2-20
  service 23-8
  user 22-10, 23-9
  user group 23-12
adding IP groups 23-4
adding service provider 22-11, 23-11
admin roles, see user management 23-9
Adobe SVG 17-10
alert
  action 21-15
    Distributed Threat Management 21-15
    Email 21-15
    NONE 21-15
    Page 21-15
    SMS 21-15
    SNMP 21-15
    Syslog 21-15
  hard drive 24-21
alerts 22-1
all matching event raw messages 20-7
all matching events 20-7
all matching sessions 20-7
anomaly detection, see NetFlow 2-31
archive server
  retrieving raw messages 24-3
attack diagram 17-9
attack paths
  L2 19-5
  L3 19-5
audit trail 24-3

B

beep code 24-31
boostrap
  devices 1-5
bytes transmitted 20-8

C

cell phone paging 22-11, 23-11
certificate
  monitor status 24-11
  upgrading from expired or fingerprint 24-11

changing
drop rule status 21-21
inspection rule status 21-17
Cisco Adaptive Security Appliance, see Cisco ASA 4-1
Cisco ASA
add to MARS 4-8
bootstrapping 4-2
security context
add discovered 4-12
define reporting options for 4-13
make MARS aware of 4-11
Cisco Firewall Services Modules, see Cisco FWSM 4-1
Cisco FWSM
add to MARS 4-8
bootstrapping 4-2
security context
add discovered 4-12
define reporting options for 4-13
make MARS aware of 4-11
Cisco Secure ACS, 802.1x feature support 14-5
Cisco Secure ACS, 802.1x support 14-1
Cisco Secure ACS, audit logs required by MARS 14-3
Cisco Secure ACS, bootstrap 14-3
Cisco Secure ACS, event logs studied by MARS 14-1
Cisco Secure ACS, MARS agent 14-7
Cisco Secure ACS, NAC support 14-1
Cisco Secure ACS, representing in MARS 14-12
Cisco Secure ACS, sever support 14-2
Cisco Secure ACS, solution engine support 14-2
Cisco Secure ACS, supported versions 14-1
Cisco Secure ACS, TACACS+ command authorization 14-7
Collapse All 19-5
columns
seed file 2-22
Common Vulneratbilities and Exposures 23-2
community strings 2-37
configuration
NetFlow 2-30
creating
report 20-25
CSV files 2-20
custom log parser
selecting traffic type 15-14
CVE 23-2

D

data reduction 17-9
default certificate response
change 24-10
default fingerprint response
change 24-10
default password
change 24-8
deleting service 23-8
destination IP address ranking 20-6
destination network group ranking 20-6
destination network ranking 20-6
destination ranking 20-6
device,re-add 2-19
devices
bootstrap overview 1-5
define
overview 1-6, 16-10
deleting 2-19
deleting all displayed 2-20
edit 2-18
diagnostics
beep codes 24-31
diagrams
attack 17-9
discovering networks
automatic 2-39
discovery
scheduling 2-39
updating 2-39
display format

query 20-5
distributed threat mitigation, taskflow order 1-7
drop rule
activate and inactive 21-21
drop rules
adding 21-22
editing 21-22
drop rule status
changing 21-21
DTM, See distributed threat mitigation. 1-7
dynamic information 19-10
dynamic vulnerability scanning 2-29

E

editing
drop rules 21-22
host information 23-6
inspection rules 21-18
IP groups 23-4
service 23-8
user 23-12
error messages, list of 14-14
event groups 23-3
event log
changing pulling time interval for Windows 10-11
event management 23-1
editing 23-2
Event Type 19-3
event type group ranking 20-6
event type ranking 20-5
Expand All 19-5
expired certificate 24-11

F

false positive
system determined 19-8
unconfirmed 19-8
user confirmed
false positive 19-8
positive 19-8
false positives
tuning 19-5
filter
modem 24-31
fingerprint validation 24-9

H

hard drive
failure alert 24-21
hotswap procedure for MARS 110R, 110, 210, GC2R, and GC2 24-26
raidstatus command 24-20
replacing in carrier 24-29
slot number diagram, MARS 110R, 110, 210, GC2R, and GC2 24-25
hardware maintenance
MARS 110, 110R, 210, GC2R, GC2 24-19
hosts
adding 23-5
editing 23-6
Hot Spot Graph 17-9
hotswap
hard drives 24-20
power supply 24-30
procedure for MARS 110R, 110, 210, GC2R, and GC2 24-26

I

incident count 20-8
Incident Details page 19-4
Incident ID 19-3
Incident Path 19-3
incidents 17-8

action 19-3
event type 19-3
incident ID 19-3
incident path 19-3
incident vector 19-3
instances 19-6
matched rule 19-3
severity 19-3
time 19-3
time ranges 19-4
incidents table
navigation 19-3
incident table 19-5
Incident Vector 19-3
inspection rule
activate and inactive 21-17
inspection rules
adding 21-19
editing 21-18
inspection rule status
changing 21-17
instances
incidents 19-6
IP groups
adding 23-4
editing 23-4
IP management 23-3
adding
hosts 23-5
IP range 23-4
network 23-4
variable 23-4

L

L2 attack path 19-5
L3 attack path 19-5
Linux host, bootstrap 10-2
loading
MARS
seed file 2-24
log files 24-2

M

MAC address report 20-7
management
events 23-1
IP 23-3
service 23-7
user 23-8
MARS
audit trail 24-3
log files 24-2
matched incident ranking 20-7
Matched Rule 19-3
matched rule ranking 20-7
Microsoft Windows host, bootstrap 10-4
mitigate 19-5
mitigation policy
suggested content 1-1
Modems
line impedance matching filter 24-31
monitoring policy
suggested content 1-1

N

NAC, AAA server support 14-1
NAT connection report 20-7
NetFllow, enable processing 2-34
NetFlow 2-30
configuration 2-30
Global NetFlow UPD Port 2-35
NetFlow, bootstrap reporting devices 2-32
NetFlow,enable processing 2-35
NetFlow,examined networks 2-35

NetFlow,guidelines 2-32
NetFlow,how it is used 2-31
NetFlow,performance tuning 2-35
NetFlow,supported versions 2-31
network group ranking 20-6
network ranking 20-6
Network Status tab
  Incidents 17-12
  Top Destinations 17-13
  Top Event Types 17-12
  Top Sources 17-13

O

Order/Rank By 20-7
order by 20-7
  bytes transmitted 20-8
  incident count 20-8
  session count 20-7
  time 20-8

P

pager 22-11, 23-11
password
  change default 24-8
PIX
  add to MARS 4-8
  bootstrapping 4-2
  security context
    add discovered 4-12
    define reporting options for 4-13
    make MARS aware of 4-11
PIX Security Appliance, see PIX 4-1
PN Log agent 14-7
PN Log Agent, error messages 14-10
PN MARS
  seed file columns 2-22
post NAT destination addresses 20-11
post NAT source addresses 20-10
pre NAT destination addresses 20-11
pre NAT source addresses 20-10
protocol ranking 20-6
public networks 2-38

Q

queries
  action
    ANY 20-12
  actions 20-12
  destination IP 20-11
    ANY 20-11
    devices 20-11
    IP addresses 20-11
    IP ranges 20-11
    networks 20-11
    post NAT destination addresses 20-11
    pre NAT destination addresses 20-11
  devices 20-11
  display format
    all matching event raw messages 20-7
    all matching events 20-7
    all matching sessions 20-7
    destination IP address ranking 20-6
    destination ranking 20-6
    event type group ranking 20-6
    MAC address report 20-7
    matched incident ranking 20-7
    matched rule ranking 20-7
    NAT connection report 20-7
    protocol ranking 20-6
    reporting device ranking 20-7
    reporting device type ranking 20-7
    source IP address ranking 20-6
    source port ranking 20-6
    unknown event report 20-7

use only firing events 20-8
event type grouping 20-11
event types 20-11
ANY 20-11
operation
AND 20-12, 21-13
FOLLOWED-BY 20-12, 21-13
none 20-12, 21-13
OR 20-12, 21-13
result format
destination network group ranking 20-6
destination network ranking 20-6
event type ranking 20-5
network group ranking 20-6
network ranking 20-6
reported user ranking 20-7
source network group ranking 20-6
source network ranking 20-6
rule 20-12
ANY 20-12
save as
reports 20-13
rules 20-13
service
ANY 20-11
defined services 20-11
service variables 20-11
severity
ANY 20-12
green 20-12
red 20-12
yellow 20-12
source IP
ANY 20-10
devices 20-10
IP addresses 20-10
IP ranges 20-10
networks 20-10
post NAT source addresses 20-10
pre NAT source addresses 20-10
variables 20-10
time range
last 20-8
start and end times 20-8
zone 20-12
query
display format 20-5
reporting device ranking 2-27
Query page 20-1

R

rank by 20-7
bytes transmitted 20-8
incident count 20-8
session count 20-7
time 20-8
raw messages
archive folder location 24-4
file name format 24-4
maximum size stored 24-4
retrieve from local controller database 24-6
retrieving from archive server 24-3
remediation policy
suggested content 1-1
removing
user 23-12
report
adding 20-25
delete 20-26
edit 20-26
new 20-25
reported user ranking 20-7
reporting device ranking 20-7
reporting device type ranking 20-7
reports
viewing 20-19, 20-25
reports, view type, CSV 20-24

reports, view type, recent 20-24
reports,view type, total 20-24
report views, CSV 20-24
report views, peak, reports, view type, peak 20-24
report views, recent 20-24
report views, total 20-24
rules
destination IP
ANY 21-8
devices 21-8
DISTINCT 21-8
IP addresses 21-8
IP ranges 21-8
Network Groups 21-8
networks 21-8
SAME 21-8
variables 21-8
device 21-11
ANY 21-11
Unknown Reporting Device 21-11
variables 21-11
event type grouping 21-10
event types 21-10
ANY 21-10
variables 21-10
reported user
ANY 21-11
Invalid User Name 21-11
NONE 21-11
variables 21-11
service
ANY 21-9
defined groups 21-10
defined services 21-10
service variables 21-9
severity
ANY 21-12
green 21-12
red 21-12
yellow 21-12
source IP
devices 21-7
IP addresses 21-7
IP ranges 21-7
Network Groups 21-7
networks 21-7
variables 21-7
runtime logging 24-1

S

scheduling
discovery 2-39
security contexts
add discovered 4-12
define reporting options 4-13
make MARS aware of 4-11
security policies
objectives of 1-1
security policy
suggested content 1-1
see CVE 23-2
seed file
CSV file 2-20
loading 2-24
service
adding 23-8
deleting 23-8
editing 23-8
editing groups 23-7
service group
adding 23-7
service management 23-7
service provider
adding 22-11, 23-11
services
adding group 23-7
session count 20-7

setting
runtime logging levels 24-1
Severity icons 19-3
Short Message Service
See SMS. 21-15
Simple Network Management Protocol
See SNMP. 21-15
SNMP RO, unsupported characters 2-9, 2-22, 2-29
Solaris host, bootstrap 10-2
source IP address ranking 20-6
source network group ranking 20-6
source network ranking 20-6
source port ranking 20-6
SSH
fingerprint validation 24-9
SSL
certificate validation 24-9
stacked charts 17-13
static information 19-10
system determined false positive type 19-8

T

table
incidents 19-5
Time 19-3
time ranges
incidents 19-4
Topology
toggle device display 17-12
traffic flows
identify and enable 1-4, 16-8
troubleshoot
error messages 14-14
troubleshoot,cannot add device 2-19
troubleshoot,cannot re-add device 2-19
troubleshooting
Cisco Secure ACS integration 14-13
tuning
false positives 19-5, 19-9

U

unconfirmed false positive type 19-8
unknown event report 20-7
use only firing events 20-8
user
adding 22-10, 23-9
editing 23-12
removing 23-12
user confirmed false positive type 19-8
user confirmed positive type 19-8
user group
adding 23-12
user management 23-8
roles defined 23-9

V

validation
fingerprint 24-9
valid networks 2-38
variables 20-10, 20-11, 21-7, 21-8