APPENDIX D

System Rules and Reports

This appendix presents the list of system rules and reports and provides a brief description of their intended use.

This chapter contains the following topics:

System Rules by Category

This topic identifies the categories in which the system rules issued with this release are organized.

System: Access

This category contains the following system rules:

System Rule: Password Attack: Remote VPN Access - Success Likely

This correlation rule detects a password guessing attack while authenticating to a remote access service (e.g. Windows L2TP, PPTP based RAS, IPSec etc.), followed by a successful logon. A password guessing attack consists of multiple login failures and may sometimes be caused by a user forgetting the password.

System Rule: Password Attack: System - Success Likely

This correlation rule detects a successful password attack to gain system level access to a host or to a windows domain- such an attack consists of a successful login occurring after attempts to retrieve passwords or guess passwords while authenticating to that host. The password attack may be preceded by reconnaissance attacks to the host. Authentication failures may sometimes be caused by a user forgetting the password.

System Rule: Password Attack: Database - Attempt

This correlation rule detects a password guessing attack to a database server, preceded by reconnaissance attacks to the host, if any. A password guessing attack consists of multiple login failures and may sometimes be caused by a user forgetting the password.

System Rule: Password Attack: Database - Success Likely

This correlation rule detects a password guessing attack on a database server followed by a successful logon. The attack may be preceded by reconnaissance attacks to the host. A password guessing attack consists of multiple login failures and may sometimes be caused by a user forgetting the password.

System Rule: Password Attack: FTP Server - Attempt

This correlation rule detects a password guessing attack to an FTP server, preceded by reconnaissance attacks to the host, if any. A password guessing attack consists of multiple login failures and may sometimes be caused by a user forgetting the password.

System Rule: Password Attack: Mail Server - Attempt

This correlation rule detects a password guessing attack on a mail server (SMTP, POP, IMAP), preceded by reconnaissance attacks to the host, if any. A password guessing attack consists of multiple login failures and may sometimes be caused by a user forgetting the password.

System Rule: Password Attack: Remote VPN Access - Attempt

This correlation rule detects a password guessing attack while authenticating to a remote access service (e.g. Windows L2TP, PPTP based RAS, IPSec etc.), preceded by reconnaissance attacks, if any. A password guessing attack consists of multiple login failures and may sometimes be caused by a user forgetting the password.

System Rule: Password Attack: Network Share - Attempt

This correlation rule detects a password guessing attack on a network share, preceded by reconnaissance attacks, if any. A password guessing attack consists of multiple login failures and may sometimes be caused by a user forgetting the password.

System Rule: Password Attack: SNMP - Attempt

This correlation rule detects attempts to retrieve SNMP community strings or access SNMP information by guessing SNMP community strings. Many SNMP installations have easily guessable passwords by default. The password attack may be preceded by reconnaissance attacks to the host.

System Rule: Password Attack: System - Attempt

This correlation rule detects attempts a to retrieve system passwords or multiple login failures while authenticating to a particular system/domain via telnet, SSH or local console/terminal logon. These attempts can be optionally preceded by reconnaissance attempts. Authentication failures may sometimes be caused by a user forgetting the password.

System Rule: Password Attack: Misc. Application - Attempt

This correlation rule detects attempts to retrieve application passwords or multiple login failures while authenticating to a particular application. These attempts can be optionally preceded by reconnaissance attempts. Authentication failures may sometimes be caused by a user forgetting the password. The applications covered by this rule exclude common ones such as Mail, FTP, SSH, Telnet, SNMP, Network/File/Print share, for which there are special rules.

System Rule: Password Attack: Web Server - Attempt

This correlation rule detects a password guessing attack to a Web server, preceded by reconnaissance attacks to the host, if any. A password guessing attack consists of multiple login failures and may sometimes be caused by a user forgetting the password.

System Rule: Password Attack: FTP Server - Success Likely

This correlation rule detects a password guessing attack on a FTP server followed by a successful logon. The attack may be preceded by reconnaissance attacks to the host. A password guessing attack consists of multiple login failures and may sometimes be caused by a user forgetting the password.

System Rule: Password Attack: Mail Server - Success Likely

This correlation rule detects a password guessing attack on a mail server (SMTP, POP, IMAP) followed by a successful logon. The password attack may be preceded by reconnaissance attacks to the host. A password guessing attack consists of multiple login failures and may sometimes be caused by a user forgetting the password.

System Rule: Password Attack: Network Share - Success Likely

This correlation rule detects a password guessing attack on a network share, followed by a successful logon. The password attack may be preceded by reconnaissance attacks to the host. A password guessing attack consists of multiple login failures and may sometimes be caused by a user forgetting the password.

System Rule: Password Attack: SNMP - Success Likely

This correlation rule detects a likely successful SNMP community string guessing attack - such an attack consists of a community string guessing attempt followed by a SNMP modification at the target host. The attack may be preceded by reconnaissance attacks to the host.

System Rule: Password Attack: Disabled Accounts

This rule detects repeated failed password attempts on locked, expired or disabled accounts on a host

System Rule: Password Scan: Disabled Accounts: Distinct Hosts

This rule detects repeated failed password attempts on locked, expired or disabled accounts on distinct hosts.

System Rule: Password Scan: Disabled Accounts: Same Host

This rule detects repeated failed password attempts on distinct locked, expired or disabled accounts on a host.

System Rule: Password Scan: Distinct Hosts

This rule detects repeated failed password attempts on distinct hosts.

System Rule: Password Scan: Same Host

This rule detects repeated failed password attempts on multiple distinct accounts on the same host.

System: CS-MARS Distributed Threat Mitigation (Cisco DTM)

This category contains the following system rules:

- System Rule: Connectivity Issue: IOS IPS DTM, page D-16
- System Rule: Resource Issue: IOS IPS DTM, page D-18

System Rule: Connectivity Issue: IOS IPS DTM

This rule detects connectivity issues between CS-MARS and IOS - CS-MARS may not be able to dynamically turn on ACTIVE signatures on IOS.

System Rule: Resource Issue: IOS IPS DTM

This rule detects that a Cisco IOS router has too little memory for running the required set of ACTIVE IPS signatures. CS-MARS was not successful in downloading the complete ACTIVE signature set.

System: CS-MARS Incident Response

This category contains the following system rules:

- System Rule: CS-MARS Host Mitigation - Failure, page D-5
- System Rule: CS-MARS Host Mitigation - Success, page D-5
- System Rule: Connectivity Issue: IOS IPS DTM, page D-16
- System Rule: Resource Issue: IOS IPS DTM, page D-18

System Rule: CS-MARS Host Mitigation - Failure

This rule triggers when CS-MARS is unable to successfully mitigate a host after having tried a few times.

System Rule: CS-MARS Host Mitigation - Success

This rule triggers when CS-MARS is able to successfully mitigate a host.

System Rule: Connectivity Issue: IOS IPS DTM

This rule detects connectivity issues between CS-MARS and IOS - CS-MARS may not be able to dynamically turn on ACTIVE signatures on IOS.

System Rule: Resource Issue: IOS IPS DTM

This rule detects that a Cisco IOS router has too little memory for running the required set of ACTIVE IPS signatures. CS-MARS was not successful in downloading the complete ACTIVE signature set.

System: CS-MARS Issue

This category contains the following system rules:

- System Rule: CS-MARS Database Partition Usage, page D-16
- System Rule: Resource Issue: CS-MARS, page D-18
- System Rule: CS-MARS Failure Saving Certificates/Fingerprints, page D-16
- System Rule: CS-MARS Authentication Method Modifed - AAA to Local, page D-7
- System Rule: CS-MARS IPS Signature Update Failure, page D-17
- System Rule: CS-MARS LC-GC Communication Failure - Certificate Mismatch, page D-17
- System Rule: CS-MARS LC-GC Communication Failure - Connectivity Issue, page D-17
- System Rule: CS-MARS LC-GC Communication Failure - Incompatible Versions, page D-17
- System Rule: CS-MARS Login Failures - Admin User, page D-7
- System Rule: CS-MARS Login Failures - Non-Admin User, page D-7

System Rule: CS-MARS Database Partition Usage

This rule indicates that the current CS-MARS database partition filled up to 75% of its capacity and the next database partition will be purged soon to create space for new events. The estimated purge times are in the event message. This is normal CS-MARS activity and will result in old events and incidents to purged from CS-MARS database. Users are urged to archive CS-MARS data to prevent permanent data loss.

System Rule: Resource Issue: CS-MARS

This rule detects resource issues with the CS-MARS device, e.g. dropped events or netflow, etc.

System Rule: CS-MARS Failure Saving Certificates/Fingerprints

This rule indicates a CS-MARS failure to save a new or changed device SSL certificate or SSH key fingerprint based on explicit user action or automatic accept due to SSL/SSH Settings.

System Rule: CS-MARS Authentication Method Modifed - AAA to Local

This rule indicates that CS-MARS authentication method was changed from AAA based authentication to Local authentication. Note that a prior change from to Local to AAA would have invalidated the passwords in the local CS-MARS database for all but user: pnadmin. Therefore, administrative action is needed on an incident for this rule to re-enable local users if it is intended for them to access CS-MARS

System Rule: CS-MARS IPS Signature Update Failure

This rule indicates that one or more errors were encountered while attempting to automatically download and update CS-MARS with a new IPS signature package. The cause of error can range from failure to download IPS signature package due to connectivity issues with CCO or local server, corrupted signature package or other errors while updating signatures in CS-MARS database.

System Rule: CS-MARS LC-GC Communication Failure - Certificate Mismatch

This rule indicates that the current CS-MARS Local Controller failed to communicate with its Global Controller due to a certificate mismatch after 3 retries over the past 6 minutes. Prior to the past 6 minutes, communication was either healthy or the status was not known.

System Rule: CS-MARS LC-GC Communication Failure - Connectivity Issue

This rule indicates that the current CS-MARS Local Controller failed to communicate with its Global Controller due to a connectivity issue after 6 retries over the past 12 minutes. Prior to the past 12 minutes, communication was either healthy or the status was not known.

System Rule: CS-MARS LC-GC Communication Failure - Incompatible Versions

This rule indicates that the current CS-MARS Local Controller failed to communicate with its Global Controller due to incompatible software or data versions after 3 retries over the past 6 minutes. Prior to the past 6 minutes, communication was either healthy or the status was not known.

System Rule: CS-MARS Login Failures - Admin User

This correlation rule detects a CS-MARS admin user being locked out after several failed login attempts via the GUI. In addition to this, the rule detects 3 login failures via the CLI (count of 2 is used due to idiosyncrasies of CS-MARS/Linux login failure syslogs) as well as failed attempts to switch to expert mode. Note that the pnadmin user is never locked out from the CLI. Authentication failures may sometimes be caused by a user forgetting the password.

System Rule: CS-MARS Login Failures - Non-Admin User

This correlation rule detects a CS-MARS admin user being locked out after several failed login attempts. Authentication failures may sometimes be caused by a user forgetting the password.

System: Client Exploits, Virus, Worm and Malware

This category contains the following system rules:

System Rule: Backdoor: Connect

This correlation rule detects a connection to a backdoor server or a response from a backdoor server in your network - there may or may not be any follow-up activity on the destination host. Backdoors (e.g. Rootkits, Trojan Horse programs) and command shells provide extensive remote control of a host and may be left by an attacker on a compromised host to maintain future remote access.

System Rule: Client Exploit - Attempt

This rule detects a client workstation exploit - this means a workstation is either downloading executable content via Web or email or sending web requests that contain scripts or is the target of an (client side) exploit via protocols such as IRC, DHCP, DNS, P2P Worms.

System Rule: Backdoor: Covert Channel

This correlation rule detects communication over covert channels - this means DMZ services such as HTTP, DNS, ICMP, FTP, SMTP etc. are being misused to tunnel inappropriate traffic via those ports. DMZ services are chosen since firewalls permit them but may not perform deep protocol inspection. Either the source or the destination in this event may be compromised.

System Rule: Worm Propagation - Success Likely

This correlation rule detects worm propagation via means such as SMTP, TFTP, and network shares accompanied by suspicious follow-up activity at the target destination host. Suspicious follow-up activity may include the host scanning the network, creating excessive firewall deny traffic, a backdoor opening up at the server etc.

System Rule: Client Exploit - Sysbug Trojan

This correlation rule detects a Sysbug Trojan exploit on a client workstation - the workstation downloaded executable content via email and the code executed and likely opened up Sysbug Trojan service on port 5555 to which other machines attempted to connect. Here, the source represents the client workstation and the destination represents the systems to which a connection is made after the trojan is installed.

System Rule: Backdoor: Spyware

This rule detects spyware e.g. Gator, Bonzi etc. installed on hosts or requests to hosts with spyware installed. Spyware are malicious applications that can be installed on a computer without the knowledge of the user, e.g. when one visits a web site or clicks on an advertising link or installs file sharing freeware such as KaZaA, iMesh, and AudioGalaxy. Once installed, the spyware automatically runs each time the host PC is started and records URLs visited, the username, password, and credit card information used, and then sends this information to the spyware writers.

System Rule: Network Activity: Windows Popup Spam

This correlation detects excessive traffic (likely pop up spam) from the same source to the Windows Messenger service.

System Rule: Worm Propagation - Attempt

This correlation rule detects worm propagation via means such as SMTP, TFTP, and network shares.

System Rule: Backdoor: Active

This correlation rule detects a connection to a backdoor server or a response from a backdoor server in your network accompanied by malicious follow-up activity on the server hosting the backdoor - this may indicate that a malicious backdoor service is likely running in your network. Malicious follow-up activity includes excessive scans, denied packets, installation of malicious services, local buffer overflow attacks etc. Backdoors such as Unix rootkits or Trojan horses are malicious programs that offer extensive remote control of a host and may be left by an attacker on a compromised host to maintain future remote access.

System Rule: Client Exploit - Success Likely

This correlation rule detects a client workstation exploit followed by the client performing anomalous activities. Client exploits include download of dynamically executable content via Web or email, web requests containing scripts, client side exploits via protocols such as IRC, DHCP, DNS, P2P Worms.

Client anomalous activities include the client originating excessive denies and scans, attempting to connect to backdoors, propagating worms over the network. The presence of such activities may indicate that the client exploit is successful.

System Rule: Network Activity: Excessive Denies - Host Compromise Likely

This correlation rule detects a large frequency (excess of 10/sec) of denies from a particular host to a particular destination port. This is a typical behavior of a compromised host looking to exploit hosts with a specififc vulnerability.

System Rule: Client Exploit - Mass Mailing Worm

This signature detects excessive amount of e-mail (at least 20/min) from a single host. To sharpen this rule for non-mail server hosts, create a group of mail server hosts and then create an exception by excluding these hosts in the source of this rule.

System Rule: Client Exploit - Sasser Worm

This correlation rule detects a successful infection spread of the Sasser worm - an attack on port 445 followed by the any of the following (a)command shell connection to the victim on port 9996, (b) an FTP connection back to the victim on port 5554, (c) excessive scans on port 445 from the victim. This indicates that both the source and the destinations are likely infected with the Sasser worm. This worm exploits the Microsoft Windows vulnerability as described in Microsoft Security Bulletin MS04-011

System Rule: Virus Found - Cleaned

This rule indicates that virus scanning software detected and was able to clean a virus.

System Rule: Virus Found - Not Cleaned

This rule indicates that virus scanning software detected but was unable to clean a virus.

System Rule: New Malware Discovered

This rule detects that Cisco Incident Control Server (ICS) has received information about a new virus/worm/malware outbreak. ICS is going to deploy ACLs or signatures to routers and IPS devices

System Rule: New Malware Prevention Deployed

This rule detects that Cisco Incident Control Server (ICS) has successfully deployed ACLs or signatures to routers and IPS devices in an attempt to prevent a newly discovered virus/worm/malware outbreak.

System Rule: New Malware Prevention Deployment Failed

This rule detects that Cisco Incident Control Server (ICS) has failed to deploy ACLs or signatures to routers and IPS devices for preventing a new virus/worm/malware outbreak.

System Rule: New Malware Traffic Match

This correlated rule detects a traffic pattern that (a) matches a worm pattern: same source to many distinct destinations and (b) matches the ACLs and signatures deployed by Cisco Incident Control Server (ICS) in response to a newly discovered virus/worm/malware outbreak.

System: Configuration Issue

This category contains the following system rules:

- System Rule: Configuration Issue: Firewall, page D-11
- System Rule: Configuration Issue: Server, page D-11
- System Rule: Modify Network Config, page D-11
- System Rule: Modify Server: SCADA Modbus, page D-11

System Rule: Configuration Issue: Firewall

This rule detects configuration errors reported by a firewall - this may cause certain traffic to be dropped by the firewall.

System Rule: Configuration Issue: Server

This rule detects configuration errors reported by a server - this may cause certain services to be not available at the server.

System Rule: Modify Network Config

This rule detects attempts to modify the configurations on a network device such as routers, switches, firewalls etc.

System Rule: Modify Server: SCADA Modbus

This rule detects attempts to modify the counters and diagnostics on a Modbus Servers. Modbus protocol is the defacto standard in industrial control communications and is the protocol of choice in a Supervisory Control and Data Acquisition (SCADA) communications network, where the Programmable logic controllers (PLCs) act as Modbus servers.

System: Database Server Activity

This category contains the following system rules:

- System Rule: Database Privileged Command - Failures, page D-11

System Rule: Database Privileged Command - Failures

This correlation rule detects multiple failed attempts from the same database user to execute privileged database commands.

System: Host Activity

This category contains the following system rules:

- System Rule: Modify Host: Files, page D-12
- System Rule: Modify Host: Service, page D-12
- System Rule: Modify Host: Logs, page D-12
- System Rule: Modify Host: Registry, page D-12
- System Rule: Modify Host: Security, page D-12
- System Rule: Modify Host: User Group, page D-12
- System Rule: Modify Host: Database Object - Failures, page D-12
- System Rule: Modify Host: Database User/Group - Failures, page D-12

System Rule: Modify Host: Files

This rule detects attempts to modify files on a host.

System Rule: Modify Host: Service

This rule detects attempts to modify the settings of services on a host.

System Rule: Modify Host: Logs

This rule detects attempts to modify log files on a host.

System Rule: Modify Host: Registry

This rule detects attempts to modify windows registry entries on a host.

System Rule: Modify Host: Security

This rule detects attempts to modify the security settings on a host.

System Rule: Modify Host: User Group

This rule detects attempts to modify the user group definitions on a host.

System Rule: Modify Host: Database Object - Failures

This correlation rule detects multiple failed attempts from the same database user to modify database objects such as tables, indices etc.

System Rule: Modify Host: Database User/Group - Failures

This correlation rule detects multiple failed attempts from the same database user to modify database user groups

System: Network Attacks and DoS

This category contains the following system rules:

System Rule: Sudden Traffic Increase To Port

This rule detects scans statistically significant increase in traffic to a particular port.

System Rule: DoS: Network - Attempt

This rule detects network level denial of service (DoS) attacks along with relevant reconnaissance activity that may have preceded the attacks. Such attacks can create a dramatic increase in overall network traffic.

System Rule: Misc. Attacks: ARP Poisoning

This correlation rule detects ARP Poisoning attacks preceded by reconnaissance attempts to that host, if any.

System Rule: Misc. Attacks: Session Hijacking

This correlation rule detects attempts to hijack a TCP connection to that host, preceded by reconnaissance attempts to that host, if any.

System Rule: Misc. Attacks: Identity Spoofing

This correlation rule detects attempts to used spoofed source IP addresses.

System Rule: DoS: Network - Success Likely

This correlation rule detects the simultaneous occurrence of network level denial of service (DoS) attacks along with related events such as traffic anomaly (e.g. ICMP echo request/reply or TCP SYN/FIN anomaly), network devices reporting high utilization, excessive scans or denies in the network etc. This may indicate that the network is under denial of service attack.

System Rule: DoS: Network Device - Attempt

This correlation rule detects attacks on network devices (such as switches, routers, firewalls) along with relevant reconnaissance activity that may have preceded these attacks. Such attacks if successful, can crash the network devices and create a denial of service for the network segment containing these devices.

System Rule: DoS: Network Device - Success Likely

This correlation rule detects attacks on network devices (such as switches, routers, firewalls) along with (a) local high usage conditions reported by the device and (b) relevant reconnaissance activity that may have preceded these attacks.

System Rule: WLAN DoS Attack Detected

This rule detects various Wireless-LAN denial of service (DoS) attacks (e.g. Broadcast Deauth, Null Probe, Association and other flood attacks) as reported by a Cisco WLAN Controller

System: New Malware Outbreak (Cisco ICS)

This category contains the following system rules:

System Rule: New Malware Discovered

This rule detects that Cisco Incident Control Server (ICS) has received information about a new virus/worm/malware outbreak. ICS is going to deploy ACLs or signatures to routers and IPS devices

System Rule: New Malware Prevention Deployed

This rule detects that Cisco Incident Control Server (ICS) has successfully deployed ACLs or signatures to routers and IPS devices in an attempt to prevent a newly discovered virus/worm/malware outbreak.

System Rule: New Malware Prevention Deployment Failed

This rule detects that Cisco Incident Control Server (ICS) has failed to deploy ACLs or signatures to routers and IPS devices for preventing a new virus/worm/malware outbreak.

System Rule: New Malware Traffic Match

This correlated rule detects a traffic pattern that (a) matches a worm pattern: same source to many distinct destinations and (b) matches the ACLs and signatures deployed by Cisco Incident Control Server (ICS) in response to a newly discovered virus/worm/malware outbreak.

System: Operational Issue

This category contains the following system rules:

System Rule: Network Errors - Likely Routing Related

This rule detects a large frequency of denied packets or ICMP destination unreachable events between the same source, destination pair - this may indicate a network routing error and may be caused by periodic retransmission attempts by TCP or the application itself (e.g. DNS).

System Rule: State Change: Host

This correlation rule detects significant host status change events such as system failing, rebooting, interface cards coming up and down, audit log filling up or getting deleted etc...

System Rule: State Change: SCADA Modbus

This rule detects Modbus servers restarting. Modbus protocol is the defacto standard in industrial control communications and is the protocol of choice in a Supervisory Control and Data Acquisition (SCADA) communications network, where the Programmable logic controllers (PLCs) act as Modbus servers.

System Rule: Operational Issue: Firewall

This rule detects operational errors (e.g. bad network connectivity, failover errors, internal software/hardware errors) reported by a firewall - this may indicate that the firewall is not functioning properly.

System Rule: Operational Issue: IDS

This rule detects operational errors reported by a intrusion detection system (IDS) - this may indicate that the device is not functioning properly.

System Rule: Operational Issue: Server

This rule detects operational errors reported by a host or by applications on a host - this may indicate that either the host or the specific application on the host is not functioning properly.

System Rule: Operational Issue: Router / Switch

This rule detects operational errors reported by non-security network devices such as routers and switches.

System Rule: State Change: Network Device

This correlation rule detects significant network status state change events such as system failing, failover occuring, interface cards coming up and down etc.

System Rule: Inactive CS-MARS Reporting Device

This rule detects reporting devices that have not reported an event in the last hour. For chatty devices such as firewalls and IDS, this may indicate connectivity issues or an issue with the device themselves. This rule should be scoped down to only include chatty network infrastructure devices.

System Rule: Connectivity Issue: IOS IPS DTM

This rule detects connectivity issues between CS-MARS and IOS - CS-MARS may not be able to dynamically turn on ACTIVE signatures on IOS.

System Rule: CS-MARS Database Partition Usage

This rule indicates that the current CS-MARS database partition filled up to 75% of its capacity and the next database partition will be purged soon to create space for new events. The estimated purge times are in the event message. This is normal CS-MARS activity and will result in old events and incidents to purged from CS-MARS database. Users are urged to archive CS-MARS data to prevent permanent data loss.

System Rule: CS-MARS Failure Saving Certificates/Fingerprints

This rule indicates a CS-MARS failure to save a new or changed device SSL certificate or SSH key fingerprint based on explicit user action or automatic accept due to SSL/SSH Settings.

System Rule: CS-MARS IPS Signature Update Failure

This rule indicates that one or more errors were encountered while attempting to automatically download and update CS-MARS with a new IPS signature package. The cause of error can range from failure to download IPS signature package due to connectivity issues with CCO or local server, corrupted signature package or other errors while updating signatures in CS-MARS database.

System Rule: CS-MARS LC-GC Communication Failure - Certificate Mismatch

This rule indicates that the current CS-MARS Local Controller failed to communicate with its Global Controller due to a certificate mismatch after 3 retries over the past 6 minutes. Prior to the past 6 minutes, communication was either healthy or the status was not known.

System Rule: CS-MARS LC-GC Communication Failure - Connectivity Issue

This rule indicates that the current CS-MARS Local Controller failed to communicate with its Global Controller due to a connectivity issue after 6 retries over the past 12 minutes. Prior to the past 12 minutes, communication was either healthy or the status was not known.

System Rule: CS-MARS LC-GC Communication Failure - Incompatible Versions

This rule indicates that the current CS-MARS Local Controller failed to communicate with its Global Controller due to incompatible software or data versions after 3 retries over the past 6 minutes. Prior to the past 6 minutes, communication was either healthy or the status was not known.

System Rule: Operational Issue: WLAN

This rule detects operational errors reported by a Cisco WLAN Controller - this may indicate that the device is not functioning properly.

System Rule: Rogue WLAN AP Detected

This rule detects Rogue Acccess Points as reported by high severity (RED) events from a Cisco WLAN Controller.

System: Reconnaissance

This category contains the following system rules:

- System Rule: Scans: SCADA Modbus, page D-18
- System Rule: Scans: Stealth, page D-18
- System Rule: Scans: Targeted, page D-18

System Rule: Scans: SCADA Modbus

This correlation rule detects scans targeted at Modbus servers. Modbus protocol is the defacto standard in industrial control communications and is the protocol of choice in a Supervisory Control and Data Acquisition (SCADA) communications network, where the Programmable logic controllers (PLCs) act as Modbus servers.

System Rule: Scans: Stealth

This rule detects highly suspicious scans that are performed by sending malformed TCP/IP packets with an intent to discover host and application characteristics such as OS name, OS version etc. A vulnerability assessment tool such as Nmap can generate such scans. The source of the scans, if from inside the trusted network, must be investigated to see if it is from an authorized source. A MARS appliance may be performing such a test as part of false positive analysis.

System Rule: Scans: Targeted

This rule detects scans that are either (a) targeted at a host to identify its operating environment, such as users on a host, DNS version, RPC services open etc. or (b) targeted at a well-known service to determine the set of host that offer that service.

System: Resource Issue

This category contains the following system rules:

- System Rule: Resource Issue: Host, page D-18
- System Rule: Resource Issue: Network Device, page D-18
- System Rule: Resource Issue: IOS IPS DTM, page D-18
- System Rule: Resource Issue: CS-MARS, page D-18

System Rule: Resource Issue: Host

This rule detects resource issues at a host, e.g. event log being full, disk near capacity, too many logged in users etc.

System Rule: Resource Issue: Network Device

This rule detects resource issues at a network device, e.g. router, switch, firewall or IDS. Such issues include high CPU usage, a firewall reaching session limit, insufficient memory etc.

System Rule: Resource Issue: IOS IPS DTM

This rule detects that a Cisco IOS router has too little memory for running the required set of ACTIVE IPS signatures. CS-MARS was not successful in downloading the complete ACTIVE signature set.

System Rule: Resource Issue: CS-MARS

This rule detects resource issues with the CS-MARS device, e.g. dropped events or netflow, etc.

System: Restricted Network Traffic

This category contains the following system rules:

System Rule: Network Activity: Excessive IRC

This correlation rule detects excessive Internet relay Chat (IRC) connections from the same source - this indicates that a Remote Admin Trojan (RAT) is likely running on the source and is likely compromised.

System Rule: Network Activity: Chat/IM - File Transfer

This rule detects file transfers via person-to-person Chat or Instant Messengers along with increase in network traffic if any. File transfer is not a normal use of Chat/IM and is suspicious. In addition, files shared with other IM users could contain viruses or other backdoor programs.

System Rule: Network Activity: P2P File Sharing - File Transfer

This rule detects a file transfer via a person-to-person file sharing application such as KaZaa, Napster, EDonkey, Gnutella, Bearshare etc. along with increase in network traffic if any. The programs may consume significant amount of network bandwidth and furthermore, inappropriate materials possibly containing viruses and backdoors may be distributed.

System Rule: Network Activity: Chat/IM - Active

This rule detects person-to-person Chat or Instant Messenger protocol activity.

System Rule: Network Activity: P2P File Sharing - Active

This rule detects person-to-person file sharing activity via applications such as KaZaa, Napster, EDonkey, Gnutella, Bearshare etc.

System Rule: Network Activity: Recreational

This rule detects recreational activities such as games, visiting adult web sites etc.

System Rule: Network Activity: Uncommon Traffic

This rule detects traffic that are not common in modern networks, for example (a) uncommon ICMP types - ICMP Router advertisement, ICMP Timestamp request/reply etc., (b) packets with uncommon TCP/IP options such source routing, timestamp etc, (c) standard protocols such as SMTP, HTTP, POP3 running on non-standard ports, (d) uncommon protocols such as FSP.

System: Security Posture Compliance (Cisco NAC)

This category contains the following system rules:

System Rule: Vulnerable Host Found

This rule detects a vulnerable host in the network - such hosts typically run old vulnerable protocols (e.g. SSH version 1, Rexec) or authenticate using plaintext passwords.

System Rule: Security Posture: Audit Server Issue - Network wide

This rule detects excessive number of logs indicating network wide audit server issues - the indications can come from many hosts staying in TRANSITION posture state for too long or many AAA server reporing Audit Server communication problems. These events may indicate that the audit server is having difficulty in auditing and updating the end host security posture status from TRANSITION state. A host enters the TRANSITION state when it is not running the Cisco Trust Agent (CTA) software and requires an out-of-band audit by an audit server to move it out of TRANSITION state to any one of HEALTHY, INFECTED, QUARANTINE, CHECKUP or UNKNOWN states. A host in a TRANSITION state is likely to have limited or no network access.

System Rule: Security Posture: Audit Server Issue - Single Host

This rule detects excessive number of logs indicating audit server issues for a single host - the indications can come from the host staying in TRANSITION posture state for too long or AAA server reporing Audit Server communication problems for the same host. These events may indicate that the audit server is having difficulty in auditing and updating the end host security posture status from TRANSITION state. A host enters the TRANSITION state when it is not running the Cisco Trust Agent (CTA) software and requires an out-of-band audit by an audit server to move it out of TRANSITION state to any one of HEALTHY, INFECTED, QUARANTINE, CHECKUP or UNKNOWN states. A host in a TRANSITION state is likely to have limited or no network access.

System Rule: Security Posture: Infected - Network wide

This rule detects that many distinct hosts are reporting INFECTED security posture status for an excessive period of time. This implies that a significant number of hosts are having trouble getting cleaned.

System Rule: Security Posture: Infected - Single Host

This rule detects that a particular host is reporting INFECTED security posture status for an excessive period of time. This implies that the host is having trouble getting cleaned.

System Rule: Security Posture: Excessive NAC Status Query Failures - Network wide

This rule detects excessive network-wide NAC status query failures reported by distinct end host, Network Access Device (NAD) combinations. A Status query failure indicates a change in posture detected by the Cisco Trust Agent (CTA) after the initial authorization. Excessive status query failures may indicate a sign of end point instability caused by the user enabling or disabling agents. Excessive status query failures reported by distinct NAD and end host combinations may indicate a critical software problem..

System Rule: Security Posture: Excessive NAC Status Query Failures - Single Host

This rule detects excessive NAC status query failures from the same end host. A Status query failure indicates a change in posture detected by the Cisco Trust Agent (CTA) after the initial authorization. Excessive status query failures may indicate a sign of end point instability caused by the user enabling or disabling agents. The end host may be compromised; at least this behavior is suspicious.

System Rule: Security Posture: Excessive NAC Status Query Failures - Single NAD

This rule detects excessive NAC status query failures from distinct hosts to the same Network Access Device (NAD). A Status query failure indicates a change in posture detected by the Cisco Trust Agent (CTA) after the initial authorization. Excessive status query failures may indicate a sign of end point instability caused by the user enabling or disabling agents. Excessive status query failures from distinct hosts reported by the same NAD may indicate a problem at the NAD.

System Rule: Security Posture: Quarantined - Network wide

This rule detects that many distinct hosts are reporting QUARANTINED security posture status for an excessive period of time. This implies that a significant number of hosts are having trouble getting DAT file updates.

System Rule: Security Posture: Quarantined - Single Host

This rule detects that a particular host is reporting QUARANTINE security posture status for an excessive period of time. This implies that the host is having trouble getting DAT file updates.

System: Server Exploits

This category contains the following system rules:

System Rule: Local Attack - Attempt

This correlation rule detects attacks on hosts by logged on users. Such attacks include local buffer overflow attacks, sym link attacks etc.

System Rule: Server Attack: Sniffer - Attempt

This correlation rule detects denial of service attacks on a host in promiscuous host (e.g. a network IDS host).

System Rule: Server Attack: Sniffer - Success Likely

This correlation rule detects denial of service attacks on a host in promiscuous host (e.g. a network IDS host) followed by the destination host reporting functionally anomalous behavior.

System Rule: Local Attack - Success Likely

This correlation rule detects attacks on hosts by locally logged on users followed by the server performing anomalous activities - such activities include excessive denies and scans, connection to backdoors, attempts to propagate worms etc. The presence of such activities may indicate that the host is compromised.

System Rule: Server Attack: SCADA Modbus - Attempt

This correlation rule detects attacks on Modbus servers, preceded by reconnaissance attempts targeted to that host, if any. The attacks include buffer overflows, denial of service attempts etc. Modbus protocol is the defacto standard in industrial control communications and is the protocol of choice in a Supervisory Control and Data Acquisition (SCADA) communications network, where the Programmable logic controllers (PLCs) act as Modbus servers.

System Rule: Misc. Attacks: Application Admin Escalation

This correlation rule detects attempts by a non-administrative user to perform administrative functions for Web applications by bypassing the required authentication. Several web applications have vulnerabilities that may allow an attacker to do so. These attempts may be preceded by reconnaissance attempts to that host.

System Rule: Misc. Attacks: Evasion

This correlation rule detects generic attempts by an attacker to bypass network IDS systems. The attempts may be preceded by reconnaissance attempts to that host.

System Rule: Misc. Attacks: TCP/IP Protocol Anomaly

This correlation rule detects events that indicate errors in standard TCP/IP headers - these may be caused by broken protocol implementations on the source host or may be malicious attempts by the source host to test the robustness of protocol implementations on the destination host.

System Rule: Misc. Attacks: Replay

This correlation rule detects replay attacks on a host, preceded by reconnaissance attempts to that host, if any. Successful replay attacks may allow the attacker to gain access by bypassing authentication.

System Rule: Server Attack: Database - Attempt

This correlation rule detects attacks on a database server, preceded by reconnaissance attempts targeted to that host, if any. The attacks include buffer overflows, denial of service attempts, SQL Injection and other remote command execution attempts using database server privileges.

System Rule: Server Attack: DNS - Attempt

This correlation rule detects specific attacks on a DNS host, preceded by reconnaissance attempts targeted to that host, if any. Attacks on a DNS host includes buffer overflow attempts, denial of service attempts.

System Rule: Server Attack: FTP - Attempt

This correlation rule detects attacks on a FTP server, preceded by reconnaissance attempts targeted to that host, if any. The attacks include buffer overflows, remote command execution attempts using FTP server privileges, denial of service attempts.

System Rule: Server Attack: Login - Attempt

This correlation rule detects attacks on login services on a host, preceded by reconnaissance attempts targeted to that host, if any. Login services include Telnet, SSH, R-protocols such as Rsh, Rlogin, Rexec etc. The attacks include buffer overflows, privilege escalation attempts to become root, denial of service attempts etc.

System Rule: Server Attack: Mail - Attempt

This correlation rule detects attacks on mail services (SMTP, POP, IMAP) on a host, preceded by reconnaissance attempts targeted to that host, if any. The attacks to mail services include buffer overflows, remote command execution attempts, privilege escalation attempts to become root, denial of service attempts etc.

System Rule: Server Attack: Misc. - Attempt

This correlation rule detects attacks on miscellaneous services (i.e. other than DNS, FTP, HTTP, Mail, FTP, RPC, Telnet, SSH, R-protocols) on a host, preceded by reconnaissance attempts targeted to that host, if any. The attacks include buffer overflows, remote command execution attempts, privilege escalation attempts to become root, denial of service attempts etc.

System Rule: Server Attack: RPC - Attempt

This correlation rule detects attacks on RPC services on a host, preceded by reconnaissance attempts targeted to that host, if any. The attacks include buffer overflows, remote command execution attempts, privilege escalation attempts to become root, denial of service attempts etc.

System Rule: Server Attack: SNMP - Attempt

This correlation rule detects attacks on SNMP implementation on a host, preceded by reconnaissance attempts targeted to that host, if any. The attacks include buffer overflows, privilege escalation attempts to become root, etc.

System Rule: Server Attack: Web - Attempt

This correlation rule detects attacks on a web server, preceded by reconnaissance attempts targeted to that host, if any. The attacks include buffer overflows, remote command execution attempts, denial of service attempts etc.

System Rule: Misc. Attacks: Access Web Customer Data

This correlation rule detects malicious attempts to access customer data stored by web applications, preceded by reconnaissance attempts to that host, if any. Customer data typically contains sensitive information such as purchasing history, credit card numbers etc.

System Rule: Server Attack: Database - Success Likely

This correlation rule detects specific attacks on a database server followed by suspicious activity on the targeted host. Suspicious activity may include the host scanning the network, creating excessive firewall deny traffic, a backdoor opening up at the server etc. The attack may be preceded by reconnaissance attempts targeted to that host. The attacks to a database server include buffer overflows, denial of service attempts, SQL Injection and other remote command execution attempts using database server privileges.

System Rule: Server Attack: DNS - Success Likely

This correlation rule detects likely successful attacks on a DNS host - an attack is successful if it is followed by suspicious activity on the targeted DNS server. Suspicious activity includes the host scanning the network, creating excessive firewall deny traffic, a backdoor opening up at the server etc. The attack may be preceded by reconnaissance attempts targeted to that host.

System Rule: Server Attack: FTP - Success Likely

This correlation rule detects specific attacks on a FTP server followed by suspicious activity on the targeted host. Suspicious activity may include the host scanning the network, creating excessive firewall deny traffic, a backdoor opening up at the server etc. The attack may be preceded by reconnaissance attempts targeted to that host. The attacks to a FTP server include buffer overflows, remote command execution attempts using FTP server privileges, denial of service attempts.

System Rule: Server Attack: Login - Success Likely

This correlation rule detects specific attacks on login services on a host (e.g. Telnet, SSH, R-protocols such as Rsh, Rlogin, Rexec etc.) followed by suspicious activity on the targeted host. Suspicious activity may include the host scanning the network, creating excessive firewall deny traffic, a backdoor opening up at the server etc. The attack may be preceded by reconnaissance attempts targeted to that host. The attacks to a login server include buffer overflows, remote command execution attempts using the server privileges, denial of service attempts.

System Rule: Server Attack: Mail - Success Likely

This correlation rule detects specific attacks on mail services (SMTP, POP, IMAP) on a host followed by suspicious activity on the targeted host. Suspicious activity may include the host scanning the network, creating excessive firewall deny traffic, a backdoor opening up at the server etc. The attack may be preceded by reconnaissance attempts targeted to that host. The attacks to a mail server include buffer overflows, remote command execution attempts using server privileges, denial of service attempts.

System Rule: Server Attack: Misc. - Success Likely

This correlation rule detects specific attacks on miscellaneous services (i.e. other than DNS, FTP, HTTP, Mail, FTP, RPC, Telnet, SSH, R-protocols) on a host followed by suspicious activity on the targeted host. Suspicious activity may include the host scanning the network, creating excessive firewall deny traffic, a backdoor opening up at the server etc. The attack may be preceded by reconnaissance attempts targeted to that host. The attacks include buffer overflows, remote command execution attempts using server privileges, denial of service attempts etc.

System Rule: Server Attack: RPC - Success Likely

This correlation rule detects specific attacks on RPC services on a host followed by suspicious activity on the targeted host. Suspicious activity may include the host scanning the network, creating excessive firewall deny traffic, a backdoor opening up at the server etc. The attack may be preceded by reconnaissance attempts targeted to that host. The attacks to RPC services include buffer overflows, remote command execution attempts using system privileges, denial of service attempts.

System Rule: Server Attack: SNMP - Success Likely

This correlation rule detects specific attacks on SNMP implementation on a host followed by suspicious activity on the targeted host. Suspicious activity may include the host scanning the network, creating excessive firewall deny traffic, a backdoor opening up at the server etc. The attack may be preceded by reconnaissance attempts targeted to that host. The attacks to RPC services include buffer overflows, remote command execution attempts using system privileges, denial of service attempts.

System Rule: Server Attack: Web - Success Likely

This correlation rule detects specific attacks on a web server followed by suspicious activity on the targeted host. Suspicious activity may include the host scanning the network, creating excessive firewall deny traffic, a backdoor opening up at the server etc. The attack may be preceded by reconnaissance attempts targeted to that host. The attacks include buffer overflows, remote command execution attempts, denial of service attempts etc.

System Reports by Category

This topic defines the complete list of system reports, organized by category, issued with this release.

- System: Access, page D-27
- System: All Events - Aggregate View, page D-30
- System: All Exploits - Aggregate View, page D-32

- System: COBIT DS3.3 - Monitoring and Reporting, page D-33
- System: COBIT DS5.10: Security Violations, page D-35
- System: COBIT DS5.19: Malicious software, page D-38
- System: COBIT DS5.20: Firewall control, page D-40
- System: COBIT DS5.2: Authentication and Access, page D-41
- System: COBIT DS5.4: User Account Changes, page D-43
- System: COBIT DS5.7: Security Surveillance, page D-43
- System: COBIT DS9.4: Configuraton Control, page D-44
- System: COBIT DS9.5: Unauthorized Software, page D-45
- System: CS-MARS Distributed Threat Mitigation (Cisco DTM), page D-46
- System: CS-MARS Incident Response, page D-46
- System: CS-MARS Issue, page D-47
- System: Client Exploits, Virus, Worm and Malware, page D-49
- System: Configuration Changes, page D-52
- System: Configuration Issue, page D-52
- System: Database Server Activity, page D-53
- System: Host Activity, page D-55
- System: Network Attacks and DoS, page D-56
- System: New Malware Outbreak (Cisco ICS), page D-57
- System: Operational Issue, page D-58
- System: Reconnaissance, page D-59
- System: Resource Issue, page D-60
- System: Resource Usage, page D-62
- System: Restricted Network Traffic, page D-63
- System: SOX 302(a)(4)(A), page D-65
- System: SOX 302(a)(4)(D), page D-66
- System: Security Posture Compliance (Cisco NAC), page D-67
- System: Server Exploits, page D-70

System: Access

This category contains the following system reports:

- Attacks: Password - Top Event Types, page D-28
- Activity: Host Login Failures - Top Destinations, page D-28
- Activity: Host Login Failures - Top Users, page D-28
- Activity: Host Login Success - Top Host, page D-41
- Attacks: Password - Top Destinations, page D-28
- Activity: Host Privilege Escalation - Top Hosts, page D-42

- Activity: Remote Access Login - Top User, page D-42
- Activity: Database Login Failures - All Events, page D-29
- Activity: Database Login Failures - Top Servers, page D-29
- Activity: Database Login Successes - Top Servers, page D-29
- Activity: Database Login Successes - Top Users, page D-29
- Activity: Host Login Failures - All Events, page D-38
- Activity: Host Login Success - All Events, page D-66
- Activity: Host Privilege Escalation - All Events, page D-42
- Activity: Remote Access Login - All Events, page D-42
- Activity: Remote Access Login Failures - All Events, page D-38
- Activity: AAA Based Access Failure - All Events, page D-42
- Activity: Accounts Locked - All Events, page D-42
- Activity: Accounts Locked - Top Hosts, page D-42
- Attacks: Password: Locked Accounts - All Events, page D-42
- Attacks: Password: Restricted Times - All Events, page D-43
- Activity: AAA Based Access - All Events, page D-43
- Activity: Database Login Failures - Top Users, page D-30
- Activity: Database Login Successes - All Events, page D-66
- Activity: CS-MARS Login Failures, page D-49

Attacks: Password - Top Event Types

This report ranks password retrieving and guessing attacks. The password can be system passwords or application passwords.

Activity: Host Login Failures - Top Destinations

This report ranks hosts by the number of logon failures recorded.

Activity: Host Login Failures - Top Users

This report ranks host users by failed login attempts.

Activity: Host Login Success - Top Host

This report ranks hosts by successful logins.

Attacks: Password - Top Destinations

This report ranks hosts by the number of password attacks attempted on them. Passwords attacks include attempts to (a) capture passwords, either remotely or locally and (b) guess passwords. Password guessing attempts are recorded as authentication failures by IDS and hosts.

Activity: Host Privilege Escalation - Top Hosts

This report records ranks the hosts by access privilege escalation attempts attempted against them. Such attempts can happen remotely or from the local console and can be reported by Network or Host IDS devices or the hosts themselves

Activity: Remote Access Login - Top User

This report ranks users by remote access logins (PPP, L2TP, PPTP, IPSec).

Activity: Database Login Failures - All Events

This report lists the event details for all database login failure events.

Activity: Database Login Failures - Top Servers

This report ranks the database servers by the number of login failures.

Activity: Database Login Successes - Top Servers

This report ranks the database server hosts by the number of successful logins.

Activity: Database Login Successes - Top Users

This report ranks the database users by the number of successful logins.

Activity: Host Login Failures - All Events

This report records all host login failure details.

Activity: Host Login Success - All Events

This report details all host login success event details

Activity: Host Privilege Escalation - All Events

This report provides details for events that represent an user attempting to increase access rights on a particular host. Such attempts can happen remotely or from the local console and can be reported by Network or Host IDS devices or the hosts themselves

Activity: Remote Access Login - All Events

This report details of remote access login events (IPSec, SSLVPN, PPP, L2TP etc)

Activity: Remote Access Login Failures - All Events

This event details all failed remote access login event details.

Activity: AAA Based Access Failure - All Events

This report details all failed AAA (e.g. RADIUS, TACACS) based access attempts. Typically mechanisms such as 802.1x, network device access, Cisco NAC use AAA servers for access control.

Activity: Accounts Locked - All Events

This report details events that indicate locked computer accounts because of excessive login failures.

Activity: Accounts Locked - Top Hosts

This report ranks the hosts by the accounts locked.

Attacks: Password: Locked Accounts - All Events

This report details password attacks on locked/disabled/expired accounts.

Attacks: Password: Restricted Times - All Events

This report details all events that indicate login failures at restricted times - the hosts are specifically configured to disallow access at these hours.

Activity: AAA Based Access - All Events

This report details AAA based access (e.g. to the network or to specific devices).

Activity: Database Login Failures - Top Users

This report ranks the users by the number of login failures.

Activity: Database Login Successes - All Events

This report lists event details for all successful database login events.

Activity: CS-MARS Login Failures

This report details events due to CS-MARS LC login failures

System: All Events - Aggregate View

This category contains the following system reports:

- Activity: All - Top Destination Ports, page D-31
- Activity: All - Top Destinations, page D-62
- Activity: All - Top Event Type Groups, page D-31
- Activity: All - Top Event Types, page D-44

- Activity: All - Top Reporting Devices, page D-62
- Activity: All - Top Sources, page D-62
- Activity: All - Top Users, page D-31
- Activity: All - NAT Connections, page D-31
- Activity: All - Top Reporting Device Types, page D-62
- Activity: All Sessions - Top Destinations by Bytes, page D-63
- Detailed NAC Report, page D-32

Activity: All - Top Destination Ports

This report ranks the UDP and TCP destination ports of all events seen by MARS over the past hour. This report is used by pages in the Summary tab.

Activity: All - Top Destinations

This report ranks the session destinations of all events seen by MARS over the past hour. This report is used by pages in the Summary tab.

Activity: All - Top Event Type Groups

This report ranks event type groups by reported events that belong to each group. The event type groups give a general feeling about the type of network activity reported to MARS.

Activity: All - Top Event Types

This report ranks the event types of all events seen by MARS over the past hour. This report is used by pages in the Summary tab.

Activity: All - Top Reporting Devices

This report ranks security devices by the total number of events reported by each device. This report is used by pages in the Summary tab.

Activity: All - Top Sources

This report ranks the session sources of all events seen by MARS over the past hour. This report is used by pages in the Summary tab.

Activity: All - Top Users

This report tracks the most frequent logins and other user activity by showing the most active user names.

Activity: All - NAT Connections

This report lists Network Address Translations performed on non-denied sessions as reported to MARS.

Activity: All - Top Reporting Device Types

This report ranks security device types by the number events reported by devices of each particular type.

Activity: All Sessions - Top Destinations by Bytes

This report ranks all destinations by bytes transferred.

Detailed NAC Report

Detailed NAC Report

System: All Exploits - Aggregate View

This category contains the following system reports:

- Activity: Attacks Prevented - Top Reporting Devices, page D-40
- Activity: Attacks Seen - Top Reporting Devices, page D-44
- Attacks: All - Top Sources, page D-32
- Attacks: SANS Top 20 - Top Event Types, page D-71
- Attacks: All - Top Event Type Groups, page D-37
- Attacks: All - All Events, page D-37
- Activity: Attacks Seen - Top Event Types, page D-33
- Attacks: All - Top Destinations, page D-33
- Activity: Attacks Prevented by Cisco IPS - All Events, page D-41
- Activity: Attacks Prevented by Cisco IPS - Top Event Types, page D-41

Activity: Attacks Prevented - Top Reporting Devices

This report ranks security devices by the number of attacks prevented.

Activity: Attacks Seen - Top Reporting Devices

This report ranks security devices by the number of attack events logged. The security devices can be firewalls, NIDS and HIDS.

Attacks: All - Top Sources

This report ranks the sources of attack events seen by MARS over the past hour.

Attacks: SANS Top 20 - Top Event Types

This report ranks the attacks that have been included in SANS Top 20 list.

Attacks: All - Top Event Type Groups

This report ranks event type groups that appear in fired correlation rules. The event type groups give a general feeling about the network activity classified as part of an attack by MARS.

Attacks: All - All Events

This event details details (event type, destination, source) for all attack events.

Activity: Attacks Seen - Top Event Types

This report ranks the top attack event types.

Attacks: All - Top Destinations

This report ranks hosts by the number of attacks targetted at each host.

Activity: Attacks Prevented by Cisco IPS - All Events

This report contains all Cisco IPS events for which attacks (or attempts) were prevented.

Activity: Attacks Prevented by Cisco IPS - Top Event Types

This report ranks the top Cisco IPS event types for which attacks (or attempts) were prevented

System: COBIT DS3.3 - Monitoring and Reporting

This category contains the following system reports:

- Operational Issues: Network - Top Reporting Devices, page D-58
- Operational Issues: Server - Top Reporting Devices, page D-58
- Resource Issues: Network - Top Reporting Devices, page D-61
- Resource Issues: Server - Top Reporting Devices, page D-61
- Resource Utilization: Bandwidth: Inbound - Top Interfaces, page D-63
- Resource Utilization: CPU - Top Devices, page D-63
- Resource Utilization: Bandwidth: Outbound - Top Interfaces, page D-63
- Resource Utilization: Concurrent Connections - Top Devices, page D-63
- Resource Utilization: Errors: Inbound - Top Interfaces, page D-58
- Resource Utilization: Errors: Outbound - Top Interfaces, page D-58
- Resource Utilization: Memory - Top Devices, page D-63
- Activity: Sudden Traffic Increase To Port - All Destinations, page D-56
- Activity: Sudden Traffic Increase To Port - All Sources, page D-56
- Operational Issues: Network - All Events, page D-59
- Operational Issues: Server - All Events, page D-59

- Resource Issues: Network - All Events, page D-61
- Resource Issues: Server - All Events, page D-61

Operational Issues: Network - Top Reporting Devices

This report summarizes the events that may indicate operational issues with network devices such as routers, firewalls and Network IDS systems.

Operational Issues: Server - Top Reporting Devices

This report summarizes the events that may indicate operational issues with servers.

Resource Issues: Network - Top Reporting Devices

This report summarizes the events that represent resource issues with network devices such as firewalls, routers and switches.

Resource Issues: Server - Top Reporting Devices

This report summarizes the events that represent resource issues with servers. These are likely to be Host IDS events.

Resource Utilization: Bandwidth: Inbound - Top Interfaces

This report ranks the inbound bandwidth utilization of the interfaces on the devices managed by PN-MARS.

Resource Utilization: CPU - Top Devices

This report ranks the CPU utilization of the devices managed by PN-MARS.

Resource Utilization: Bandwidth: Outbound - Top Interfaces

This report ranks the outbound bandwidth utilization of interfaces on devices managed by Pn-MARS.

Resource Utilization: Concurrent Connections - Top Devices

This report ranks the number of concurrent connections established through the devices managed by PN-MARS.

Resource Utilization: Errors: Inbound - Top Interfaces

This report ranks by error rate on the inbound interfaces of the devices managed by PN-MARS.

Resource Utilization: Errors: Outbound - Top Interfaces

This report ranks by error rate on the outbound interfaces of the devices managed by PN-MARS.

Resource Utilization: Memory - Top Devices

This report ranks the memory utilization of the devices managed by PN-MARS.

Activity: Sudden Traffic Increase To Port - All Destinations

This report lists hosts that exhibit anomalous behavior by suddenly receiving statistically significant volume on a TCP/UDP port or ICMP traffic.

Activity: Sudden Traffic Increase To Port - All Sources

This report lists hosts that exhibit anomalous behavior by suddenly sending statistically significant volume on a TCP/UDP port or ICMP traffic.

Operational Issues: Network - All Events

This report lists details about all operational issues on network devices.

Operational Issues: Server - All Events

This report lists details about events that indicate operational errors on hosts or host applications.

Resource Issues: Network - All Events

This report lists event details for all events related to resource issues on network devices such as IDS, routers, firewalls etc.

Resource Issues: Server - All Events

This report lists event details for all resource issues on hosts. These are reported by Host IDS or Operating System logs.

System: COBIT DS5.10: Security Violations

This category contains the following system reports:

- Activity: IDS Evasion - Top Event Types, page D-70
- Activity: Scans - Top Destination Ports, page D-60
- Activity: Scans - Top Destinations, page D-60
- Activity: Stealth Scans - Top Sources, page D-60
- Attacks: Database Server - Top Event Types, page D-70
- Attacks: FTP Server - Top Event Types, page D-71
- Attacks: Identity Spoofing - Top Event Types, page D-71
- Attacks: Login Services - Top Event Types, page D-71
- Attacks: Mail Server - Top Event Types, page D-71

- Attacks: Network DoS - Top Event Types, page D-56
- Attacks: RPC Services - Top Event Types, page D-71
- Attacks: SANS Top 20 - Top Event Types, page D-71
- Attacks: SNMP - Top Event Types, page D-71
- Attacks: Web Server/App - Top Event Types, page D-71
- Attacks: All - Top Event Type Groups, page D-37
- Attacks: All - All Events, page D-37
- Attacks: Uncommon or Anomalous Traffic - Top Event Types, page D-71
- Activity: Database Privileged Command Failures - All Events, page D-54
- Activity: Database User/Group Change Failures - All Events, page D-54
- Activity: Host Login Failures - All Events, page D-38
- Activity: Remote Access Login Failures - All Events, page D-38
- Activity: Sudden Traffic Increase To Port - All Destinations, page D-56
- Activity: Sudden Traffic Increase To Port - All Sources, page D-56
- Attacks: Password - All Events, page D-38
- Activity: Security Posture: Not Healthy - All Events, page D-69

Activity: IDS Evasion - Top Event Types

This report ranks the events that detect an attempt by an attacker to evade detection by Network IDS systems. This may be web-based obfuscation attacks, fragmentation attacks or TCP/IP based attacks.

Activity: Scans - Top Destination Ports

This report ranks destination ports by the total number of events detecting scanning activity for that port. Scans involve activities such as searching for alive hosts, open services on such hosts and detecting host configuration and application settings.

Activity: Scans - Top Destinations

This report ranks hosts by the total number of events detecting scanning activity directed to that host. Scans involve activities such as searching for alive hosts, open services on such hosts and detecting host configuration and application settings.

Activity: Stealth Scans - Top Sources

This report ranks attackers by the amount of stealth scanning activity. Such activities include sending crafted packets to detect host operating systems and other vulnerabilities. Vulnerability scanners may generate such events.

Attacks: Database Server - Top Event Types

This report ranks attacks on database servers such as MS SQL Server, Oracle and Sybase.

Attacks: FTP Server - Top Event Types

This report ranks attacks on FTP servers.

Attacks: Identity Spoofing - Top Event Types

This report ranks events that represent attempts by an attacker to spoof his/her identity over the past hour.

Attacks: Login Services - Top Event Types

This report ranks attacks on servers providing login services and remote shells. Examples include Telnet, SSH and Berkeley r-protocols.

Attacks: Mail Server - Top Event Types

This report ranks attacks on Mail servers (SMTP, POP, IMAP).

Attacks: Network DoS - Top Event Types

This report ranks attacks that represent network wide denial of service attempts. Such attacks may include crashing or rebooting an inline network device such as router, firewall or switch or increasing network load by creating TCP, UDP or ICMP traffic.

Attacks: RPC Services - Top Event Types

This report ranks attacks on RPC based applications.

Attacks: SANS Top 20 - Top Event Types

This report ranks the attacks that have been included in SANS Top 20 list.

Attacks: SNMP - Top Event Types

This report ranks SNMP based attacks over the past hour.

Attacks: Web Server/App - Top Event Types

This report ranks attacks on web servers or applications built on top of web servers over the past hour.

Attacks: All - Top Event Type Groups

This report ranks event type groups that appear in fired correlation rules. The event type groups give a general feeling about the network activity classified as part of an attack by MARS.

Attacks: All - All Events

This event details details (event type, destination, source) for all attack events.

Attacks: Uncommon or Anomalous Traffic - Top Event Types

This report ranks the events that represent uncommon or anomalous traffic. Uncommon traffic involves ICMP types and TCP/IP options not in common usage or standard traffic on non-standard ports. Anomalous traffic includes traffic that violate IETF or other well known protocol specifications.

Activity: Database Privileged Command Failures - All Events

This report lists event details for all privileged database command execution failures.

Activity: Database User/Group Change Failures - All Events

This report lists the event details for all failed database user/group modification attempts.

Activity: Host Login Failures - All Events

This report records all host login failure details.

Activity: Remote Access Login Failures - All Events

This event details all failed remote access login event details.

Activity: Sudden Traffic Increase To Port - All Destinations

This report lists hosts that exhibit anomalous behavior by suddenly receiving statistically significant volume on a TCP/UDP port or ICMP traffic.

Activity: Sudden Traffic Increase To Port - All Sources

This report lists hosts that exhibit anomalous behavior by suddenly sending statistically significant volume on a TCP/UDP port or ICMP traffic.

Attacks: Password - All Events

This report details all password attack events.

Activity: Security Posture: Not Healthy - All Events

This report lists the detailed events for users whose security posture is not up to date, ie. in either a CHECKUP, QUARANTINE or INFECTED state. The software on these hosts need to be upgraded. The CHECKUP hosts may need DAT file updates, the QUARANTINE hosts must do DAT file updates before network access and the INFECTED hosts must be remediated before network access.

System: COBIT DS5.19: Malicious software

This category contains the following system reports:

- Activity: Backdoor - Top Event Types, page D-50

Activity: Backdoor - Top Event Types

This report ranks the events that detect some form of backdoor activity. A backdoor may be created by an attacker on a compromised host. A backdoor event can be either an attempt to connect to a backdoor or a response from a server running a backdoor.

Activity: Virus/Worms - Top Event Types

This report ranks the events that detect virus or worm activity in the network.

Attacks: Virus/Worms - Top Sources

This report ranks addresses that are the source of virus/worm propagation attempts.

Activity: Backdoor - Top Destinations

This report ranks the hosts that respond to backdoor connection attempts.

Activity: Backdoor - Top Hosts

This report ranks the hosts that respond to backdoor connection attempts. This means that the hosts are likely infected and running backdoors.

Activity: Spyware - Top Hosts

This report ranks the hosts running spyware applications. Spywares are malicious applications that installs and runs on hosts, collect the username, passwords, and credit card information and send this information to the spyware writers.

Activity: Virus/Worms - Top Infected Hosts

This report ranks hosts that are propagating virus and worms via SMTP, POP, IMAP, network shares etc.

Activity: Virus: Detected - Top Users

This report ranks users/workstations by viruses detected.

Activity: Virus: Infections - Top Users

This report ranks users/workstations by viruses detected and not cleaned.

System: COBIT DS5.20: Firewall control

This category contains the following system reports:

- Activity: Attacks Prevented - Top Reporting Devices, page D-40
- Activity: Denies - Top Destination Ports, page D-60
- Activity: Denies - Top Destinations, page D-60
- Activity: Web Usage - Top Sources, page D-40
- Activity: Network Usage - Top Destination Ports, page D-62
- Activity: Web Usage - Top Destinations by Bytes, page D-40
- Activity: Web Usage - Top Destinations by Sessions, page D-41
- Resource Utilization: Concurrent Connections - Top Devices, page D-63
- Activity: Network Usage - Top Destination Ports By Bytes, page D-63
- Activity: Attacks Prevented by Cisco IPS - All Events, page D-41
- Activity: Attacks Prevented by Cisco IPS - Top Event Types, page D-41

Activity: Attacks Prevented - Top Reporting Devices

This report ranks security devices by the number of attacks prevented.

Activity: Denies - Top Destination Ports

This report ranks the destination ports to which attacks have been targetted but denied.

Activity: Denies - Top Destinations

This report ranks the destination hosts to which attacks have been targeted but denied.

Activity: Web Usage - Top Sources

This signature ranks source addresses based on web use.

Activity: Network Usage - Top Destination Ports

This report ranks destination ports by number of network sessions. This report requires that the syslog level of routers or firewalls be set to high to be able to capture session events. This report provides a general usage pattern of the network.

Activity: Web Usage - Top Destinations by Bytes

This report ranks the web servers by bytes transferred.

Activity: Web Usage - Top Destinations by Sessions

This report ranks the top web destinations by session count.

Resource Utilization: Concurrent Connections - Top Devices

This report ranks the number of concurrent connections established through the devices managed by PN-MARS.

Activity: Network Usage - Top Destination Ports By Bytes

This report ranks the top destination ports by bytes sent and transmitted.

Activity: Attacks Prevented by Cisco IPS - All Events

This report contains all Cisco IPS events for which attacks (or attempts) were prevented.

Activity: Attacks Prevented by Cisco IPS - Top Event Types

This report ranks the top Cisco IPS event types for which attacks (or attempts) were prevented

System: COBIT DS5.2: Authentication and Access

This category contains the following system reports:

- Activity: Host Login Success - Top Host, page D-41
- Activity: Host Privilege Escalation - Top Hosts, page D-42
- Activity: Remote Access Login - Top User, page D-42
- Activity: Host Login Success - All Events, page D-66
- Activity: Host Admin Login Success - All Events, page D-66
- Activity: Host Privilege Escalation - All Events, page D-42
- Activity: Remote Access Login - All Events, page D-42
- Activity: AAA Based Access Failure - All Events, page D-42
- Activity: Accounts Locked - All Events, page D-42
- Activity: Accounts Locked - Top Hosts, page D-42
- Attacks: Password: Locked Accounts - All Events, page D-42
- Attacks: Password: Restricted Times - All Events, page D-43
- Activity: AAA Based Access - All Events, page D-43
- Activity: Database Login Successes - All Events, page D-66
- Activity: CS-MARS Login Failures, page D-49

Activity: Host Login Success - Top Host

This report ranks hosts by successful logins.

Activity: Host Privilege Escalation - Top Hosts

This report records ranks the hosts by access privilege escalation attempts attempted against them. Such attempts can happen remotely or from the local console and can be reported by Network or Host IDS devices or the hosts themselves

Activity: Remote Access Login - Top User

This report ranks users by remote access logins (PPP, L2TP, PPTP, IPSec).

Activity: Host Login Success - All Events

This report details all host login success event details

Activity: Host Admin Login Success - All Events

This report details successful administrative login events to hosts.

Activity: Host Privilege Escalation - All Events

This report provides details for events that represent an user attempting to increase access rights on a particular host. Such attempts can happen remotely or from the local console and can be reported by Network or Host IDS devices or the hosts themselves

Activity: Remote Access Login - All Events

This report details of remote access login events (IPSec, SSLVPN, PPP, L2TP etc)

Activity: AAA Based Access Failure - All Events

This report details all failed AAA (e.g. RADIUS, TACACS) based access attempts. Typically mechanisms such as 802.1x, network device access, Cisco NAC use AAA servers for access control.

Activity: Accounts Locked - All Events

This report details events that indicate locked computer accounts because of excessive login failures.

Activity: Accounts Locked - Top Hosts

This report ranks the hosts by the accounts locked.

Attacks: Password: Locked Accounts - All Events

This report details password attacks on locked/disabled/expired accounts.

Attacks: Password: Restricted Times - All Events

This report details all events that indicate login failures at restricted times - the hosts are specifically configured to disallow access at these hours.

Activity: AAA Based Access - All Events

This report details AAA based access (e.g. to the network or to specific devices).

Activity: Database Login Successes - All Events

This report lists event details for all successful database login events.

Activity: CS-MARS Login Failures

This report details events due to CS-MARS LC login failures

System: COBIT DS5.4: User Account Changes

This category contains the following system reports:

- Activity: Host User/Group Management - All Events, page D-66
- Activity: Host User/Group Management - Top hosts, page D-56
- Activity: Database User/Group Change Successes - All Events, page D-66
- Activity: Database User/Group Change Successes - Top Users, page D-55

Activity: Host User/Group Management - All Events

This report recordss user group management events reported by hosts.

Activity: Host User/Group Management - Top hosts

This report ranks hosts by user group management events reported.

Activity: Database User/Group Change Successes - All Events

This report lists the event details for all successful database user/group modifications.

Activity: Database User/Group Change Successes - Top Users

This report ranks the users by the successful database user/group modifications performed.

System: COBIT DS5.7: Security Surveillance

This category contains the following system reports:

- Activity: All - Top Event Types, page D-44

- Activity: All - Top Reporting Devices, page D-62
- Activity: Attacks Seen - Top Reporting Devices, page D-44
- Activity: All - Top Reporting Device Types, page D-62
- Activity: Inactive Reporting Device - Top Devices, page D-58

Activity: All - Top Event Types

This report ranks the event types of all events seen by MARS over the past hour. This report is used by pages in the Summary tab.

Activity: All - Top Reporting Devices

This report ranks security devices by the total number of events reported by each device. This report is used by pages in the Summary tab.

Activity: Attacks Seen - Top Reporting Devices

This report ranks security devices by the number of attack events logged. The security devices can be firewalls, NIDS and HIDS.

Activity: All - Top Reporting Device Types

This report ranks security device types by the number events reported by devices of each particular type.

Activity: Inactive Reporting Device - Top Devices

This report lists devices that are configured to be reporting to CS-MARS bt haven’t reported any event in the last hour.

System: COBIT DS9.4: Configuraton Control

This category contains the following system reports:

- Activity: Host Registry Changes - All Events, page D-66
- Activity: Database Object Modification Successes - All Events, page D-65
- Configuration Changes: Network - All Events, page D-52
- Configuration Changes: Server - All Events, page D-52
- Activity: Host Security Policy Changes - All Events, page D-66

Activity: Host Registry Changes - All Events

This report records the events signalling Microsoft Windows registry changes.

Activity: Database Object Modification Successes - All Events

This report lists the event details for all successful database object modification attempts.

Configuration Changes: Network - All Events

This event details all the configuration changes in network devices.

Configuration Changes: Server - All Events

This event details all configuration changes on hosts (reported by OS or Host IDS agents)

Activity: Host Security Policy Changes - All Events

This report lists all policy changes on a host affecting host security. These events are typically reported by Host IDS and host agents.

System: COBIT DS9.5: Unauthorized Software

This category contains the following system reports:

- Activity: IRC - All Events, page D-64
- Activity: Recreational - All Events, page D-64
- Activity: Spyware - All Events, page D-64
- Activity: P2P Filesharing/Chat - All Events, page D-64
- Activity: Uncommon or Anomalous Traffic - All Events, page D-65

Activity: IRC - All Events

This report lists all IRC activities. Typically, worms deposit executables on infected hosts that initiate IRC connections.

Activity: Recreational - All Events

This event details all users involved in recreational activities such as games, specific web sites such as gambling etc.

Activity: Spyware - All Events

This event details all spyware events.

Activity: P2P Filesharing/Chat - All Events

This event details all P2P File sharing or Chat event details.

Activity: Uncommon or Anomalous Traffic - All Events

This report details uncommon or anomalous traffic such as unused TCP options, uncommon ICMP traffic, non-standard traffic on standard port, tunneled traffic etc.

System: CS-MARS Distributed Threat Mitigation (Cisco DTM)

This category contains the following system reports:

- Activity: IOS IPS DTM Successful Signature Tuning - All Events, page D-47
- Connectivity Issue: IOS IPS DTM - All Events, page D-59
- Resource Issues: IOS IPS DTM - Top Devices, page D-61
- Resource Issues: IOS IPS DTM - All Events, page D-61

Activity: IOS IPS DTM Successful Signature Tuning - All Events

This report lists all successful IOS IPS signature download activities - both adition and deletion. CS-MARS Distributed Threat Mitigation (DTM) turns on ACTIVE IPS signatures on IOS routers.

Connectivity Issue: IOS IPS DTM - All Events

This report lists connectivity issues between CS-MARS and IOS IPS devices. Connectivity issues may prevent CS-MARS from turning on ACTIVE signatures on IOS IPS.

Resource Issues: IOS IPS DTM - Top Devices

This report lists IOS IPS routers that are running low on memory for CS-MARS Distributed Threat Mitigation (DTM). Because of low memory, CS-MARS may not be able to download and activate the complete set of ACTIVE IPS signatures to IOS IPS devices.

Resource Issues: IOS IPS DTM - All Events

This report lists event details that indicate certin IOS IPS routers running low on memory for CS-MARS Distributed Threat Mitigation (DTM). Because of low memory, CS-MARS may not be able to download and activate the complete set of ACTIVE IPS signatures to those IOS IPS devices.

System: CS-MARS Incident Response

This category contains the following system reports:

- Activity: CS-MARS Host Mitigation - Failure - All Events, page D-46
- Activity: CS-MARS Host Mitigation - Success - All Events, page D-47
- Activity: IOS IPS DTM Successful Signature Tuning - All Events, page D-47
- Activity: WLAN Successful Mitigations, page D-47

Activity: CS-MARS Host Mitigation - Failure - All Events

This report lists failed CS-MARS mitigation attempts - these can result from improper network connectivity or device access credentials.

Activity: CS-MARS Host Mitigation - Success - All Events

This report lists successful mitigations from CS-MARS.

Activity: IOS IPS DTM Successful Signature Tuning - All Events

This report lists all successful IOS IPS signature download activities - both adition and deletion. CS-MARS Distributed Threat Mitigation (DTM) turns on ACTIVE IPS signatures on IOS routers.

Activity: WLAN Successful Mitigations

This reports lists all misbehaved Wireless-LAN hosts, APs and Adhoc hosts that were mitigated from accessing the network as reported by a Cisco WLAN Controller

System: CS-MARS Issue

This category contains the following system reports:

- Activity: Unknown Events - All Events, page D-47
- Resource Issues: CS-MARS - All Events, page D-61
- Resource Utilization: CS-MARS - All Events, page D-59
- Activity: CS-MARS Accepted New Certificates/Fingerprints, page D-48
- Activity: CS-MARS Accepted Conflicting Certificates/Fingerprints, page D-48
- Activity: CS-MARS Detected Conflicting Certificates/Fingerprints, page D-48
- Activity: CS-MARS Failure Saving Certificates/Fingerprints, page D-59
- Activity: CS-MARS Device Connectivity Errors, page D-59
- Activity: CS-MARS Authentication Method Modifications, page D-48
- Activity: CS-MARS pnadmin User Password Status, page D-48
- Activity: CS-MARS Accounts Locked, page D-49
- Activity: CS-MARS IPS Signature Update Success - All Events, page D-49
- Activity: CS-MARS Successful Logins, page D-49
- Activity: CS-MARS IPS Signature Update Failure - All Events, page D-59
- Activity: CS-MARS Login Failures, page D-49
- Activity: CS-MARS LC-GC Communication Recovered, page D-49
- Activity: CS-MARS Accounts Unlocked, page D-49
- Activity: CS-MARS LC-GC Communication Failures, page D-59

Activity: Unknown Events - All Events

This report tracks the events that are unknown to MARS.

Resource Issues: CS-MARS - All Events

This report lists event details for all events related to resource issues with the CS-MARS device, e.g. dropped events or netflow, etc.

Resource Utilization: CS-MARS - All Events

This report lists event details for all events related to CS-MARS resource utilization, e.g. database partitions, etc.

Activity: CS-MARS Accepted New Certificates/Fingerprints

This report lists event details due to CS-MARS accepting new SSL certificates or SSH Key Fingerprints when connecting to remote devices.

Activity: CS-MARS Accepted Conflicting Certificates/Fingerprints

This report lists event details due to CS-MARS accepting conflicting SSL certificates or SSH Key Fingerprints when connecting to remote devices.

Activity: CS-MARS Detected Conflicting Certificates/Fingerprints

This report lists event details due to CS-MARS detecting conflicting SSL certificates or SSH Key Fingerprints when connecting to remote devices.

Activity: CS-MARS Failure Saving Certificates/Fingerprints

This report lists event details due to CS-MARS failure to save new or changed SSL certificates or SSH Key Fingerprints based on explicit user action or automatic accept due to SSL/SSH Settings.

Activity: CS-MARS Device Connectivity Errors

This report lists event details of CS-MARS device connectivity errors due to various reasons (e.g. conflicting SSL certificates or SSH key fingerprints, network timeout etc.). This includes both transient and persisting errors.

Activity: CS-MARS Authentication Method Modifications

This report details events due to CS-MARS LC activity due to authentication method changes from Local DB to AAA or AAA to Local DB

Activity: CS-MARS pnadmin User Password Status

This report details events due to CS-MARS LC ’pnadmin’ user account password activity such as change in password or if the password continues to remain factory default which is checked once in 24 hours

Activity: CS-MARS Accounts Locked

This report details events due to CS-MARS LC accounts that are locked due to excessive login failures or explicit admin user action

Activity: CS-MARS IPS Signature Update Success - All Events

This report lists event details of all success events that occur during auto update of an IPS signature package in CS-MARS. The included events indicate intermediate success steps in auto update or complete/partial success of updating the CS-MARS database with the downloaded IPS signature package.

Activity: CS-MARS Successful Logins

This report details events due to CS-MARS LC successful logins

Activity: CS-MARS IPS Signature Update Failure - All Events

This report lists event details of all failure events that occur during auto update of an IPS signature package in CS-MARS. The included events indicate intermediate errors such as failing to add or update one or more CS-MARS event types corresponding to some IPS signature as well as complete failure to download/parse/update (or partial update) the CS-MARS database with the signature package.

Activity: CS-MARS Login Failures

This report details events due to CS-MARS LC login failures

Activity: CS-MARS LC-GC Communication Recovered

This reports lists event details over the past hour due to all restored communications between CS-MARS Local Controller with its Global Controller that had failed due to various reasons such as connectivity issues, certificate mismatch or incompatible software or data versions

Activity: CS-MARS Accounts Unlocked

This report details events due to CS-MARS LC accounts that are unlocked by an admin user

Activity: CS-MARS LC-GC Communication Failures

This reports lists event details over the past hour due to all communication failures between CS-MARS Local Controller with its Global Controller for various reasons such as connectivity issues, certificate mismatch or incompatible software or data versions

System: Client Exploits, Virus, Worm and Malware

This category contains the following system reports:

- Activity: Backdoor - Top Event Types, page D-50

- Activity: Virus/Worms - Top Event Types, page D-50
- Attacks: Virus/Worms - Top Sources, page D-50
- Activity: Backdoor - Top Destinations, page D-50
- Activity: Backdoor - Top Hosts, page D-50
- Attacks: Client Exploits - Top Sources, page D-50
- Activity: Virus/Worms - Top Infected Hosts, page D-51
- Activity: Virus: Detected - Top Users, page D-51
- Activity: Virus: Infections - Top Users, page D-51
- Activity: New Malware Discovered - All Events, page D-57
- Activity: New Malware Prevention Deployment Failure - All Events, page D-57
- Activity: New Malware Prevention Deployment Success - All Events, page D-57
- Activity: New Malware Traffic Match - All Events, page D-57
- Activity: New Malware Traffic Match - Top Sources, page D-58
- Activity: Sudden Traffic Increase To Port - All Destinations, page D-56
- Activity: Sudden Traffic Increase To Port - All Sources, page D-56

Activity: Backdoor - Top Event Types

This report ranks the events that detect some form of backdoor activity. A backdoor may be created by an attacker on a compromised host. A backdoor event can be either an attempt to connect to a backdoor or a response from a server running a backdoor.

Activity: Virus/Worms - Top Event Types

This report ranks the events that detect virus or worm activity in the network.

Attacks: Virus/Worms - Top Sources

This report ranks addresses that are the source of virus/worm propagation attempts.

Activity: Backdoor - Top Destinations

This report ranks the hosts that respond to backdoor connection attempts.

Activity: Backdoor - Top Hosts

This report ranks the hosts that respond to backdoor connection attempts. This means that the hosts are likely infected and running backdoors.

Attacks: Client Exploits - Top Sources

This report ranks hosts by the number of exploits originating from each host.

Activity: Virus/Worms - Top Infected Hosts

This report ranks hosts that are propagating virus and worms via SMTP, POP, IMAP, network shares etc.

Activity: Virus: Detected - Top Users

This report ranks users/workstations by viruses detected.

Activity: Virus: Infections - Top Users

This report ranks users/workstations by viruses detected and not cleaned.

Activity: New Malware Discovered - All Events

This report lists all the new virus/worm/malware outbreaks discovered by Cisco Incident Control Server.

Activity: New Malware Prevention Deployment Failure - All Events

This report lists all devices to which ACL and signature deployment attempts by a Cisco Incident Control Server, in response to a new virus/worm/malware outbreak, failed.

Activity: New Malware Prevention Deployment Success - All Events

This report lists all destinations (Cisco IOS IPS devices and IPS appliances) to which Cisco Incident Control Server has deployed new ACLs and signatures in respond to a new virus/worm/malware outbreak.

Activity: New Malware Traffic Match - All Events

This report details the traffic sources and the enforcing devices that match the ACLs and signatures deployed by the Cisco Incident Control Server in response to a newly discovered malware outbreak.

Activity: New Malware Traffic Match - Top Sources

This report lists the top sources that match the ACLs or signatures dynamically deployed by Cisco Incident Control Server in response to a new virus/worm/malware outbreak. This indicates that these sources are likely infected.

Activity: Sudden Traffic Increase To Port - All Destinations

This report lists hosts that exhibit anomalous behavior by suddenly receiving statistically significant volume on a TCP/UDP port or ICMP traffic.

Activity: Sudden Traffic Increase To Port - All Sources

This report lists hosts that exhibit anomalous behavior by suddenly sending statistically significant volume on a TCP/UDP port or ICMP traffic.

System: Configuration Changes

This category contains the following system reports:

- Configuration Changes: Network - Top Event Types, page D-52
- Configuration Changes: Server - Top Event Types, page D-52
- Configuration Changes: Server - Top Reporting Devices, page D-52
- Configuration Changes: Network - All Events, page D-52
- Configuration Changes: Server - All Events, page D-52

Configuration Changes: Network - Top Event Types

This report summarizes configuration changes to network devices such as firewalls, routers and switches over the past hour.

Configuration Changes: Server - Top Event Types

This report summarizes configuration changes to servers over the past hour.

Configuration Changes: Server - Top Reporting Devices

This report summarizes the configuration changes per server over the past hour.

Configuration Changes: Network - All Events

This event details all the configuration changes in network devices.

Configuration Changes: Server - All Events

This event details all configuration changes on hosts (reported by OS or Host IDS agents)

System: Configuration Issue

This category contains the following system reports:

- Configuration Issues: Network - Top Reporting Devices, page D-52
- Configuration Issues: Server - Top Reporting Devices, page D-53
- Configuration Issues: Network - All Events, page D-53
- Configuration Issues: Server - All Events, page D-53

Configuration Issues: Network - Top Reporting Devices

This report summarizes the events that may indicate certain configuration related problems in network devices such as firewalls, routers and switches.

Configuration Issues: Server - Top Reporting Devices

This report summarizes the events that may indicate certain configuration related problems in servers. These are likely to be Host IDS events.

Configuration Issues: Network - All Events

This report lists details for events that indicate configuration error on network devices.

Configuration Issues: Server - All Events

This report lists details for all events that indicate configuration errors on hosts or host applications.

System: Database Server Activity

This category contains the following system reports:

- Activity: Database Object Modification Failures - All Events, page D-53
- Activity: Database Object Modification Failures - Top Users, page D-53
- Activity: Database Object Modification Successes - All Events, page D-65
- Activity: Database Object Modification Successes - Top Users, page D-54
- Activity: Database Privileged Command Failures - All Events, page D-54
- Activity: Database Privileged Command Failures - Top Users, page D-54
- Activity: Database Privileged Command Successes - All Events, page D-66
- Activity: Database Privileged Command Successes - Top Users, page D-54
- Activity: Database Regular Command Failures - All Events, page D-54
- Activity: Database Regular Command Failures - Top Users, page D-54
- Activity: Database Regular Command Successes - All Events, page D-54
- Activity: Database Regular Command Successes - Top Users, page D-54
- Activity: Database User/Group Change Failures - All Events, page D-54
- Activity: Database User/Group Change Failures - Top Users, page D-54
- Activity: Database User/Group Change Successes - All Events, page D-66
- Activity: Database User/Group Change Successes - Top Users, page D-55

Activity: Database Object Modification Failures - All Events

This report lists the event details for all failed database object modification attempts.

Activity: Database Object Modification Failures - Top Users

This report ranks the users by the number of failed database object modification attempts.

Activity: Database Object Modification Successes - All Events

This report lists the event details for all successful database object modification attempts.

Activity: Database Object Modification Successes - Top Users

This report ranks the number of users by the number of successful database object modifications.

Activity: Database Privileged Command Failures - All Events

This report lists event details for all privileged database command execution failures.

Activity: Database Privileged Command Failures - Top Users

This report ranks the users by failed privileged database command execution attempts.

Activity: Database Privileged Command Successes - All Events

This report lists the event details for all successful privileged database commands executed.

Activity: Database Privileged Command Successes - Top Users

This report ranks the users by successful privileged database commands executed.

Activity: Database Regular Command Failures - All Events

This report lists the event details for all failed non-privileged database command execution attempts.

Activity: Database Regular Command Failures - Top Users

This report ranks the users by the number of non-privileged database command execution attempts.

Activity: Database Regular Command Successes - All Events

This report lists the event details for all successful non-privileged database command executions.

Activity: Database Regular Command Successes - Top Users

This report ranks the users by successful non-privileged database command executions.

Activity: Database User/Group Change Failures - All Events

This report lists the event details for all failed database user/group modification attempts.

Activity: Database User/Group Change Failures - Top Users

This report ranks the users by the number of failed database user/group modification attempts.

Activity: Database User/Group Change Successes - All Events

This report lists the event details for all successful database user/group modifications.

Activity: Database User/Group Change Successes - Top Users

This report ranks the users by the successful database user/group modifications performed.

System: Host Activity

This category contains the following system reports:

- Activity: Host Object Access - All Events, page D-55
- Activity: Host Privileged Access - All Events, page D-55
- Activity: Host Registry Changes - All Events, page D-66
- Activity: Host Registry Changes - Top Host, page D-55
- Activity: Host Security Policy Changes - Top Host, page D-55
- Activity: Host System Events - All Events, page D-56
- Activity: Host User/Group Management - All Events, page D-66
- Activity: Host User/Group Management - Top hosts, page D-56
- Activity: Host Process Tracking - All Events, page D-56

Activity: Host Object Access - All Events

This report records all Microsoft Windows Object Access events from Windows Event Logs.

Activity: Host Privileged Access - All Events

This report records all Microsoft Windows Host Privileged Access events from Windows Event Logs.

Activity: Host Registry Changes - All Events

This report records the events signalling Microsoft Windows registry changes.

Activity: Host Registry Changes - Top Host

This report ranks hosts by the number of Microsoft Windows registry changes reported.

Activity: Host Security Policy Changes - Top Host

This report ranks hosts by the number of security policy changes on that host.

Activity: Host System Events - All Events

This report records the Microsoft Windows system events, e.g. startup, shutdown, LSA registration, audit event discards, etc.

Activity: Host User/Group Management - All Events

This report recordss user group management events reported by hosts.

Activity: Host User/Group Management - Top hosts

This report ranks hosts by user group management events reported.

Activity: Host Process Tracking - All Events

This report records all Microsoft Windows Detailed Process Tracking events from Windows Event Logs.

System: Network Attacks and DoS

This category contains the following system reports:

- Attacks: Network DoS - Top Event Types, page D-56
- Activity: Sudden Traffic Increase To Port - All Destinations, page D-56
- Activity: Sudden Traffic Increase To Port - All Sources, page D-56
- Activity: WLAN DoS Attacks Detected, page D-57
- Activity: WLAN Probes Detected, page D-57
- Activity: WLAN Rogue AP or Adhoc Hosts Detected, page D-57

Attacks: Network DoS - Top Event Types

This report ranks attacks that represent network wide denial of service attempts. Such attacks may include crashing or rebooting an inline network device such as router, firewall or switch or increasing network load by creating TCP, UDP or ICMP traffic.

Activity: Sudden Traffic Increase To Port - All Destinations

This report lists hosts that exhibit anomalous behavior by suddenly receiving statistically significant volume on a TCP/UDP port or ICMP traffic.

Activity: Sudden Traffic Increase To Port - All Sources

This report lists hosts that exhibit anomalous behavior by suddenly sending statistically significant volume on a TCP/UDP port or ICMP traffic.

Activity: WLAN DoS Attacks Detected

This reports lists all the Wireless-LAN denial of service (DoS) attacks (e.g. Broadcast Deauth, Null Probe, Association and other flood attacks) as reported by a Cisco WLAN Controller

Activity: WLAN Probes Detected

This reports lists all the Wireless-LAN probes (e.g. Netstumbler and Wellenreiter scanners) as reported by a Cisco WLAN Controller

Activity: WLAN Rogue AP or Adhoc Hosts Detected

This reports lists all misbehaved Wireless-LAN hosts, APs and Adhoc hosts as detected and reported by a Cisco WLAN Controller

System: New Malware Outbreak (Cisco ICS)

This category contains the following system reports:

Activity: New Malware Discovered - All Events

This report lists all the new virus/worm/malware outbreaks discovered by Cisco Incident Control Server.

Activity: New Malware Prevention Deployment Failure - All Events

This report lists all devices to which ACL and signature deployment attempts by a Cisco Incident Control Server, in response to a new virus/worm/malware outbreak, failed.

Activity: New Malware Prevention Deployment Success - All Events

This report lists all destinations (Cisco IOS IPS devices and IPS appliances) to which Cisco Incident Control Server has deployed new ACLs and signatures in respond to a new virus/worm/malware outbreak.

Activity: New Malware Traffic Match - All Events

This report details the traffic sources and the enforcing devices that match the ACLs and signatures deployed by the Cisco Incident Control Server in response to a newly discovered malware outbreak.

Activity: New Malware Traffic Match - Top Sources

This report lists the top sources that match the ACLs or signatures dynamically deployed by Cisco Incident Control Server in response to a new virus/worm/malware outbreak. This indicates that these sources are likely infected.

System: Operational Issue

This category contains the following system reports:

- Operational Issues: Network - Top Reporting Devices, page D-58
- Operational Issues: Server - Top Reporting Devices, page D-58
- Resource Utilization: Errors: Inbound - Top Interfaces, page D-58
- Resource Utilization: Errors: Outbound - Top Interfaces, page D-58
- Activity: Inactive Reporting Device - Top Devices, page D-58
- Operational Issues: Network - All Events, page D-59
- Operational Issues: Server - All Events, page D-59
- Connectivity Issue: IOS IPS DTM - All Events, page D-59
- Resource Utilization: CS-MARS - All Events, page D-59
- Activity: CS-MARS Failure Saving Certificates/Fingerprints, page D-59
- Activity: CS-MARS Device Connectivity Errors, page D-59
- Activity: CS-MARS IPS Signature Update Failure - All Events, page D-59
- Activity: CS-MARS LC-GC Communication Failures, page D-59

Operational Issues: Network - Top Reporting Devices

This report summarizes the events that may indicate operational issues with network devices such as routers, firewalls and Network IDS systems.

Operational Issues: Server - Top Reporting Devices

This report summarizes the events that may indicate operational issues with servers.

Resource Utilization: Errors: Inbound - Top Interfaces

This report ranks by error rate on the inbound interfaces of the devices managed by PN-MARS.

Resource Utilization: Errors: Outbound - Top Interfaces

This report ranks by error rate on the outbound interfaces of the devices managed by PN-MARS.

Activity: Inactive Reporting Device - Top Devices

This report lists devices that are configured to be reporting to CS-MARS bt haven't reported any event in the last hour.

Operational Issues: Network - All Events

This report lists details about all operational issues on network devices.

Operational Issues: Server - All Events

This report lists details about events that indicate operational errors on hosts or host applications.

Connectivity Issue: IOS IPS DTM - All Events

This report lists connectivity issues between CS-MARS and IOS IPS devices. Connectivity issues may prevent CS-MARS from turning on ACTIVE signatures on IOS IPS.

Resource Utilization: CS-MARS - All Events

This report lists event details for all events related to CS-MARS resource utilization, e.g. database partitions, etc.

Activity: CS-MARS Failure Saving Certificates/Fingerprints

This report lists event details due to CS-MARS failure to save new or changed SSL certificates or SSH Key Fingerprints based on explicit user action or automatic accept due to SSL/SSH Settings.

Activity: CS-MARS Device Connectivity Errors

This report lists event details of CS-MARS device connectivity errors due to various reasons (e.g. conflicting SSL certificates or SSH key fingerprints, network timeout etc.). This includes both transient and persisting errors.

Activity: CS-MARS IPS Signature Update Failure - All Events

This report lists event details of all failure events that occur during auto update of an IPS signature package in CS-MARS. The included events indicate intermediate errors such as failing to add or update one or more CS-MARS event types corresponding to some IPS signature as well as complete failure to download/parse/update (or partial update) the CS-MARS database with the signature package.

Activity: CS-MARS LC-GC Communication Failures

This reports lists event details over the past hour due to all communication failures between CS-MARS Local Controller with its Global Controller for various reasons such as connectivity issues, certificate mismatch or incompatible software or data versions

System: Reconnaissance

This category contains the following system reports:

- Activity: Denies - Top Destination Ports, page D-60
- Activity: Denies - Top Destinations, page D-60

- Activity: Denies - Top Sources, page D-60
- Activity: Scans - Top Destination Ports, page D-60
- Activity: Scans - Top Destinations, page D-60
- Activity: Scans - Top Sources, page D-60
- Activity: Stealth Scans - Top Sources, page D-60

Activity: Denies - Top Destination Ports

This report ranks the destination ports to which attacks have been targetted but denied.

Activity: Denies - Top Destinations

This report ranks the destination hosts to which attacks have been targeted but denied.

Activity: Denies - Top Sources

This report ranks attack sources by the number of denied connection attempts.

Activity: Scans - Top Destination Ports

This report ranks destination ports by the total number of events detecting scanning activity for that port. Scans involve activities such as searching for alive hosts, open services on such hosts and detecting host configuration and application settings.

Activity: Scans - Top Destinations

This report ranks hosts by the total number of events detecting scanning activity directed to that host. Scans involve activities such as searching for alive hosts, open services on such hosts and detecting host configuration and application settings.

Activity: Scans - Top Sources

This report ranks an attack sources by the total number of events detecting scanning activity for certain services. Scans involve activities such as searching for alive hosts, open services on such hosts and detecting host configuration and application settings.

Activity: Stealth Scans - Top Sources

This report ranks attackers by the amount of stealth scanning activity. Such activities include sending crafted packets to detect host operating systems and other vulnerabilities. Vulnerability scanners may generate such events.

System: Resource Issue

This category contains the following system reports:

- Resource Issues: Network - Top Reporting Devices, page D-61

Resource Issues: Network - Top Reporting Devices

This report summarizes the events that represent resource issues with network devices such as firewalls, routers and switches.

Resource Issues: Server - Top Reporting Devices

This report summarizes the events that represent resource issues with servers. These are likely to be Host IDS events.

Resource Issues: Network - All Events

This report lists event details for all events related to resource issues on network devices such as IDS, routers, firewalls etc.

Resource Issues: Server - All Events

This report lists event details for all resource issues on hosts. These are reported by Host IDS or Operating System logs.

Resource Issues: IOS IPS DTM - Top Devices

This report lists IOS IPS routers that are running low on memory for CS-MARS Distributed Threat Mitigation (DTM). Because of low memory, CS-MARS may not be able to download and activate the complete set of ACTIVE IPS signatures to IOS IPS devices.

Resource Issues: IOS IPS DTM - All Events

This report lists event details that indicate certin IOS IPS routers running low on memory for CS-MARS Distributed Threat Mitigation (DTM). Because of low memory, CS-MARS may not be able to download and activate the complete set of ACTIVE IPS signatures to those IOS IPS devices.

Resource Issues: CS-MARS - All Events

This report lists event details for all events related to resource issues with the CS-MARS device, e.g. dropped events or netflow, etc.

System: Resource Usage

This category contains the following system reports:

- Activity: All - Top Destinations, page D-62
- Activity: All - Top Reporting Devices, page D-62
- Activity: All - Top Sources, page D-62
- Activity: All - Top Reporting Device Types, page D-62
- Activity: Network Usage - Top Destination Ports, page D-62
- Activity: All Events and Netflow - Top Destination Ports, page D-63
- Activity: All Sessions - Top Destination Ports by Bytes, page D-63
- Activity: All Sessions - Top Destinations by Bytes, page D-63
- Resource Utilization: Bandwidth: Inbound - Top Interfaces, page D-63
- Resource Utilization: CPU - Top Devices, page D-63
- Resource Utilization: Bandwidth: Outbound - Top Interfaces, page D-63
- Resource Utilization: Concurrent Connections - Top Devices, page D-63
- Resource Utilization: Memory - Top Devices, page D-63
- Activity: Network Usage - Top Destination Ports By Bytes, page D-63

Activity: All - Top Destinations

This report ranks the session destinations of all events seen by MARS over the past hour. This report is used by pages in the Summary tab.

Activity: All - Top Reporting Devices

This report ranks security devices by the total number of events reported by each device. This report is used by pages in the Summary tab.

Activity: All - Top Sources

This report ranks the session sources of all events seen by MARS over the past hour. This report is used by pages in the Summary tab.

Activity: All - Top Reporting Device Types

This report ranks security device types by the number events reported by devices of each particular type.

Activity: Network Usage - Top Destination Ports

This report ranks destination ports by number of network sessions. This report requires that the syslog level of routers or firewalls be set to high to be able to capture session events. This report provides a general usage pattern of the network.

Activity: All Events and Netflow - Top Destination Ports

This report ranks the UDP and TCP destination ports of all events (including Netflow events) seen by MARS over the past hour. This report is used by pages in the Summary tab.

Activity: All Sessions - Top Destination Ports by Bytes

This report ranks all destination ports by bytes transferred.

Activity: All Sessions - Top Destinations by Bytes

This report ranks all destinations by bytes transferred.

Resource Utilization: Bandwidth: Inbound - Top Interfaces

This report ranks the inbound bandwidth utilization of the interfaces on the devices managed by PN-MARS.

Resource Utilization: CPU - Top Devices

This report ranks the CPU utilization of the devices managed by PN-MARS.

Resource Utilization: Bandwidth: Outbound - Top Interfaces

This report ranks the outbound bandwidth utilization of interfaces on devices managed by Pn-MARS.

Resource Utilization: Concurrent Connections - Top Devices

This report ranks the number of concurrent connections established through the devices managed by PN-MARS.

Resource Utilization: Memory - Top Devices

This report ranks the memory utilization of the devices managed by PN-MARS.

Activity: Network Usage - Top Destination Ports By Bytes

This report ranks the top destination ports by bytes sent and transmitted.

System: Restricted Network Traffic

This category contains the following system reports:

- Activity: P2P Filesharing/Chat - Top Event Types, page D-64
- Activity: IRC - All Events, page D-64
- Activity: Spyware - Top Hosts, page D-64
- Activity: P2P Filesharing/Chat - Top Hosts, page D-64

Activity: P2P Filesharing/Chat - Top Event Types

This event ranks events detecting person-to-person file sharing protocol and chat protocol activity. File sharing protocols such as KaZaa, Napster, EDonkey and chat protocols such as IRC, Hotline and instant messaging protocols may not be suitable in business environments.

Activity: IRC - All Events

This report lists all IRC activities. Typically, worms deposit executables on infected hosts that initiate IRC connections.

Activity: Spyware - Top Hosts

This report ranks the hosts running spyware applications. Spywares are malicious applications that installs and runs on hosts, collect the username, passwords, and credit card information and send this information to the spyware writers.

Activity: P2P Filesharing/Chat - Top Hosts

This report ranks hosts involved in P2P Filesharing and chat protocol activity. Such protocols may not be suitable in business environments.

Activity: Recreational - Top Sources

This report ranks the source addesses involved in recreational activities such as games, adult web sites, stock sites etc.

Activity: Recreational - All Events

This event details all users involved in recreational activities such as games, specific web sites such as gambling etc.

Activity: Spyware - All Events

This event details all spyware events.

Activity: P2P Filesharing/Chat - All Events

This event details all P2P File sharing or Chat event details.

Activity: Uncommon or Anomalous Traffic - All Events

This report details uncommon or anomalous traffic such as unused TCP options, uncommon ICMP traffic, non-standard traffic on standard port, tunneled traffic etc.

System: SOX 302(a)(4)(A)

This category contains the following system reports:

- Activity: Database Object Modification Successes - All Events, page D-65
- Activity: Database Privileged Command Successes - All Events, page D-66
- Activity: Database User/Group Change Successes - All Events, page D-66
- Activity: Host Login Success - All Events, page D-66
- Activity: Host Admin Login Success - All Events, page D-66
- Activity: Host Security Policy Changes - All Events, page D-66
- Activity: Database Login Successes - All Events, page D-66

Activity: Database Object Modification Successes - All Events

This report lists the event details for all successful database object modification attempts.

Activity: Database Privileged Command Successes - All Events

This report lists the event details for all successful privileged database commands executed.

Activity: Database User/Group Change Successes - All Events

This report lists the event details for all successful database user/group modifications.

Activity: Host Login Success - All Events

This report details all host login success event details

Activity: Host Admin Login Success - All Events

This report details successful administrative login events to hosts.

Activity: Host Security Policy Changes - All Events

This report lists all policy changes on a host affecting host security. These events are typically reported by Host IDS and host agents.

Activity: Database Login Successes - All Events

This report lists event details for all successful database login events.

System: SOX 302(a)(4)(D)

This category contains the following system reports:

- Activity: Host Registry Changes - All Events, page D-66
- Activity: Host User/Group Management - All Events, page D-66
- Activity: Database Privileged Command Successes - All Events, page D-66
- Activity: Database User/Group Change Successes - All Events, page D-66
- Activity: Host Login Success - All Events, page D-66
- Activity: Host Admin Login Success - All Events, page D-66
- Activity: Host Security Policy Changes - All Events, page D-66
- Activity: Database Login Successes - All Events, page D-66

Activity: Host Registry Changes - All Events

This report records the events signalling Microsoft Windows registry changes.

Activity: Host User/Group Management - All Events

This report recordss user group management events reported by hosts.

Activity: Database Privileged Command Successes - All Events

This report lists the event details for all successful privileged database commands executed.

Activity: Database User/Group Change Successes - All Events

This report lists the event details for all successful database user/group modifications.

Activity: Host Login Success - All Events

This report details all host login success event details

Activity: Host Admin Login Success - All Events

This report details successful administrative login events to hosts.

Activity: Host Security Policy Changes - All Events

This report lists all policy changes on a host affecting host security. These events are typically reported by Host IDS and host agents.

Activity: Database Login Successes - All Events

This report lists event details for all successful database login events.

System: Security Posture Compliance (Cisco NAC)

This category contains the following system reports:

Activity: Vulnerable Host Found via VA Scanner

This report lists vulnerable hosts and associated vulnerabilities found by importing information from Vulnerability Analysis (VA) scanners.

Activity: Vulnerable Host Found

This host lists all vulnerable hosts found by IDS or VA scanners

Activity: Security Posture: Healthy - Top Users

This report lists the users in a HEALTHY Security Posture State. A Healthy security posture implies that the posture of the host is up to date, policy compliant and does not need attention.

Activity: Security Posture: NAC - Top NADs

This report ranks the network access devices (NADs) handling Network Admission Control transcations.

Activity: Security Posture: NAC - Top Tokens

This report shows the network wide distribution of NAC tokens. The possible token values are HEALTHY, CHECKUP, INFECTED, QUARANTINE, UNKNOWN. The TRANSITION token is excluded since it is an intermediate state.

Activity: Security Posture: NAC L2IP - Top Tokens

This report captures the distribution of NAC tokens for end hosts that use Layer 2 IP method to validate their posture. The possible NAC tokens values in this report are HEALTHY, CHECKUP, INFECTED, QUARANTINE, UNKNOWN. The TRANSITION token is excluded since it is an intermediate state.

Activity: Security Posture: NAC Audit Server Issues - All Events

This report ranks the end hosts for which the AAA server is having an issue with obtaining the right security posture token from the audit server. These hoend sts do not have the Cisco Trust Agent (CTA) running and they depend on an Audit Server for obtaining the proper Security Posture Token.

Activity: Security Posture: NAC Infected/Quarantine - All Events

This report reports the event details for the hosts that are in an INFECTED or QUARANTINE state. The QUARANTINE hosts must do Anti-virus DAT file updates before network access and the INFECTED hosts must be cleaned before network access.

Activity: Security Posture: NAC Infected/Quarantine - Top Hosts

This report details the hosts that are in an INFECTED or QUARANTINE state. The QUARANTINE hosts must do Anti-virus DAT file updates before network access and the INFECTED hosts must be cleaned before network access.

Activity: Security Posture: NAC L2 802.1x - Top Tokens

This report captures the distribution of NAC tokens for end hosts that use Layer 2 IEEE 802.1x method to validate their posture. The possible NAC tokens values in this report are HEALTHY, CHECKUP, INFECTED, QUARANTINE, UNKNOWN. The TRANSITION token is excluded since it is an intermediate state.

Activity: Security Posture: NAC Static Auth - Top Hosts

This report captures the hosts that are configured as static exceptions on the Network Access Device (NAD). For these hosts, the NAD directly permits network access without consulting the posture validation server.

Activity: Security Posture: NAC Static Auth - Top NADs

This report captures the Network Access Device (NAD) that are permitting end hosts into the network as static exceptions. For these end hosts, the NAD directly permits network access without consulting the posture validation server.

Activity: Security Posture: NAC Status Query Failure - Top Hosts

This report details the top hosts that failed the status queries from the Network Access Devices (NAD). Such failures occur after initial authorization whenever there is a change in posture detected by the Cisco Trust Agent (CTA) on the end host. Such failures may be caused by user frequently enabling or disabling CTA agents.

Activity: Security Posture: Not Healthy - All Events

This report lists the detailed events for users whose security posture is not up to date, ie. in either a CHECKUP, QUARANTINE or INFECTED state. The software on these hosts need to be upgraded. The CHECKUP hosts may need DAT file updates, the QUARANTINE hosts must do DAT file updates before network access and the INFECTED hosts must be remediated before network access.

Activity: Security Posture: NAC - Top NADs and Tokens

This report displays the Network Access Devices (NADs) handling Network Admission Control transcations along with the tokens assigned by each of them.

Activity: Security Posture: NAC Agentless - Top Tokens

This report captures the distribution of NAC tokens for end hosts that do not have Cisco Trust Agent (CTA) software. In this case, the posture validation is done either locally by the Network Access Device or via the Audit Server. The possible NAC tokens values in this report are HEALTHY, CHECKUP, INFECTED, QUARANTINE, UNKNOWN. The TRANSITION token is excluded since it is an intermediate state.

Activity: Security Posture: NAC End Host Details - All Events

This report details all the NAC related messages from the Network Access Devices (NAD) and AAA servers. Choose a source IP address or user to see the messages for one end host.

Activity: AAA Failed Auth - All Events

This report displays event details on failed AAA authentications. This report covers the following cases: regular AAA auth, 802.1x auth, L2 IP and L3 IP auth, L2 802.1x auth. An authentication may fail because of policy misconfiguration on the AAA server or wrong user credentials.

Activity: AAA Failed Auth - Top NADs

This report ranks the Network Access Devices (NADs) based on failed AAA authentications. This report covers the following cases: regular AAA auth, 802.1x auth, L2 IP and L3 IP auth, L2 802.1x auth. An authentication may fail because of policy misconfiguration on the AAA server or wrong user credentials.

Activity: AAA Failed Auth - Top Users

This report ranks the users based on failed AAA authentications. This report covers the following cases: regular AAA auth, 802.1x auth, L2 IP and L3 IP auth, L2 802.1x auth. An authentication may fail because of policy misconfiguration on the AAA server or wrong user credentials.

Activity: Security Posture: NAC Agentless - Top Hosts

This report captures the distribution of NAC tokens for end hosts that do not have Cisco Trust Agent (CTA) software. In this case, the posture validation is done either locally by the Network Access Device or via the Audit Server. The possible NAC tokens values in this report are HEALTHY, CHECKUP, INFECTED, QUARANTINE, UNKNOWN. The TRANSITION token is excluded since it is an intermediate state.

Activity: Security Posture: NAC Agentless - Top NADs

This report captures the distribution of NAC tokens for end hosts that do not have Cisco Trust Agent (CTA) software. In this case, the posture validation is done either locally by the Network Access Device or via the Audit Server. The possible NAC tokens values in this report are HEALTHY, CHECKUP, INFECTED, QUARANTINE, UNKNOWN. The TRANSITION token is excluded since it is an intermediate state.

System: Server Exploits

This category contains the following system reports:

- Activity: IDS Evasion - Top Event Types, page D-70
- Attacks: Database Server - Top Event Types, page D-70
- Attacks: FTP Server - Top Event Types, page D-71
- Attacks: Identity Spoofing - Top Event Types, page D-71
- Attacks: Login Services - Top Event Types, page D-71
- Attacks: Mail Server - Top Event Types, page D-71
- Attacks: RPC Services - Top Event Types, page D-71
- Attacks: SANS Top 20 - Top Event Types, page D-71
- Attacks: SNMP - Top Event Types, page D-71
- Attacks: Web Server/App - Top Event Types, page D-71
- Attacks: Uncommon or Anomalous Traffic - Top Event Types, page D-71

Activity: IDS Evasion - Top Event Types

This report ranks the events that detect an attempt by an attacker to evade detection by Network IDS systems. This may be web-based obfuscation attacks, fragmentation attacks or TCP/IP based attacks.

Attacks: Database Server - Top Event Types

This report ranks attacks on database servers such as MS SQL Server, Oracle and Sybase.

Attacks: FTP Server - Top Event Types

This report ranks attacks on FTP servers.

Attacks: Identity Spoofing - Top Event Types

This report ranks events that represent attempts by an attacker to spoof his/her identity over the past hour.

Attacks: Login Services - Top Event Types

This report ranks attacks on servers providing login services and remote shells. Examples include Telnet, SSH and Berkeley r-protocols.

Attacks: Mail Server - Top Event Types

This report ranks attacks on Mail servers (SMTP, POP, IMAP).

Attacks: RPC Services - Top Event Types

This report ranks attacks on RPC based applications.

Attacks: SANS Top 20 - Top Event Types

This report ranks the attacks that have been included in SANS Top 20 list.

Attacks: SNMP - Top Event Types

This report ranks SNMP based attacks over the past hour.

Attacks: Web Server/App - Top Event Types

This report ranks attacks on web servers or applications built on top of web servers over the past hour.

Attacks: Uncommon or Anomalous Traffic - Top Event Types

This report ranks the events that represent uncommon or anomalous traffic. Uncommon traffic involves ICMP types and TCP/IP options not in common usage or standard traffic on non-standard ports. Anomalous traffic includes traffic that violate IETF or other well known protocol specifications.