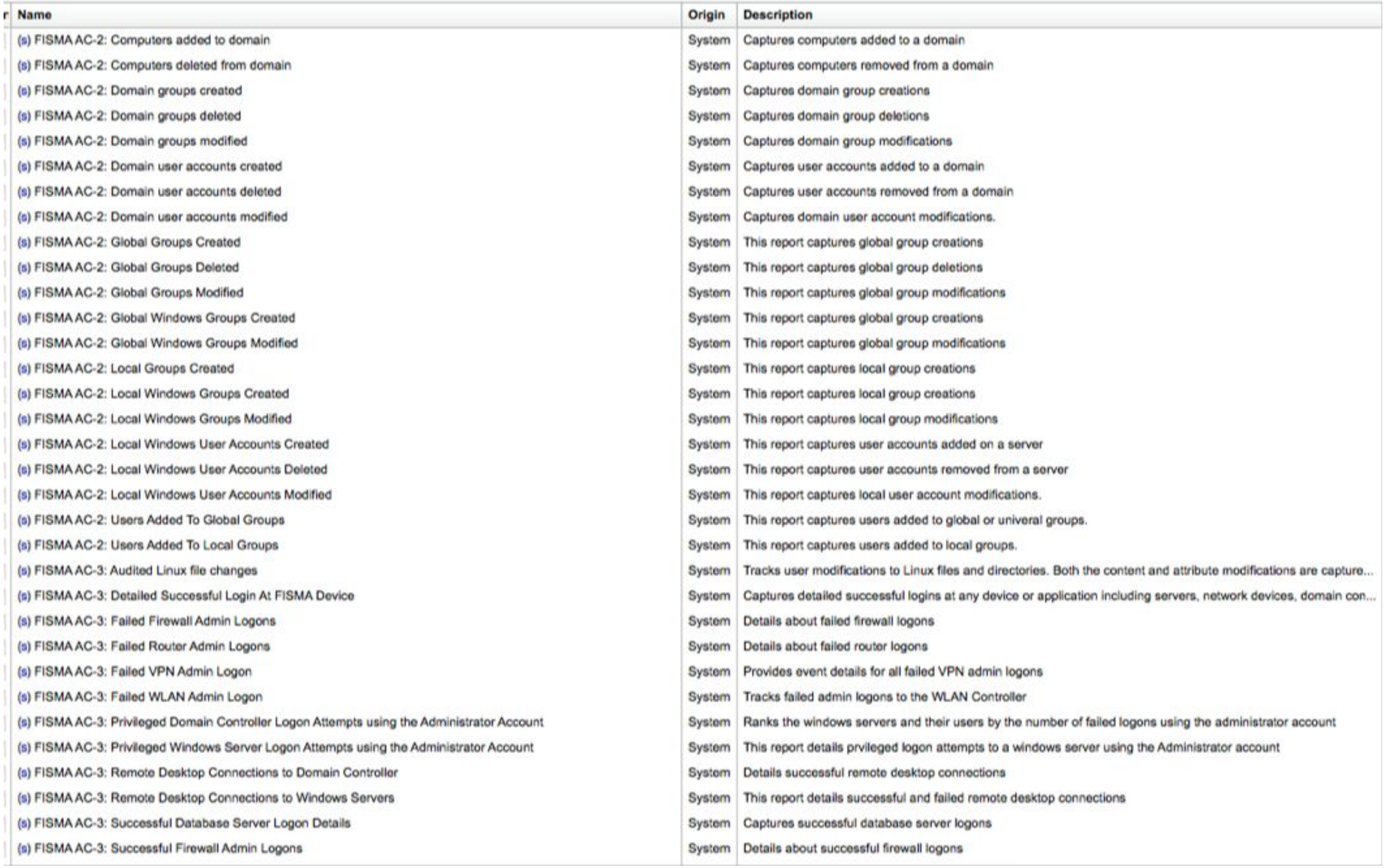
StratoZen SIEM Report Categories

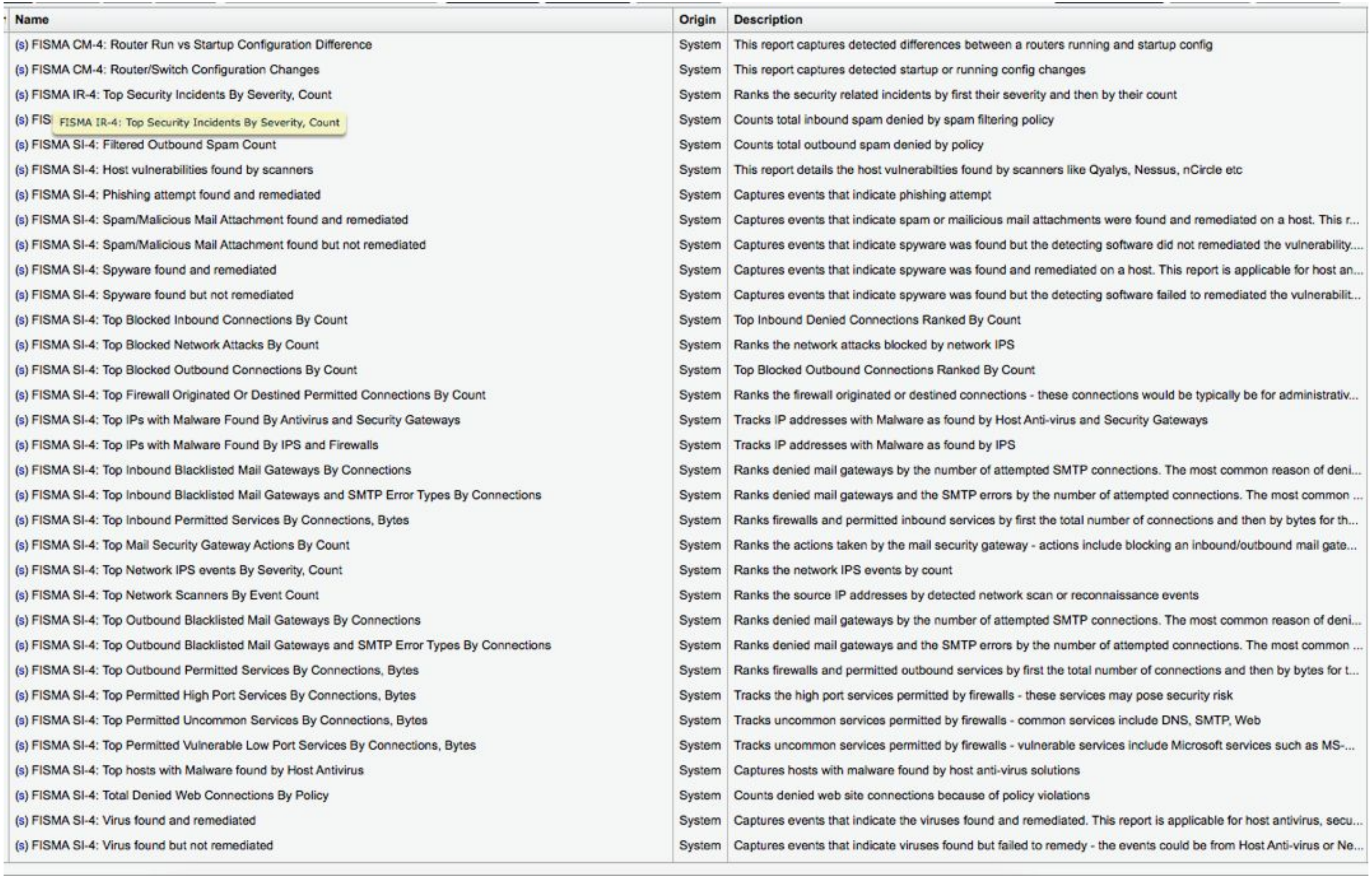
- COBIT
- FISMA
- GLBA
- GPG13
- HIPAA
- ITIL
- ISO
- ISO 27001
- NERC
- NIST 800-53
- NIST 800-171
- PCI
- SANS Critical Control
- SOX

StratoZen FISMA Reports 1 of 2



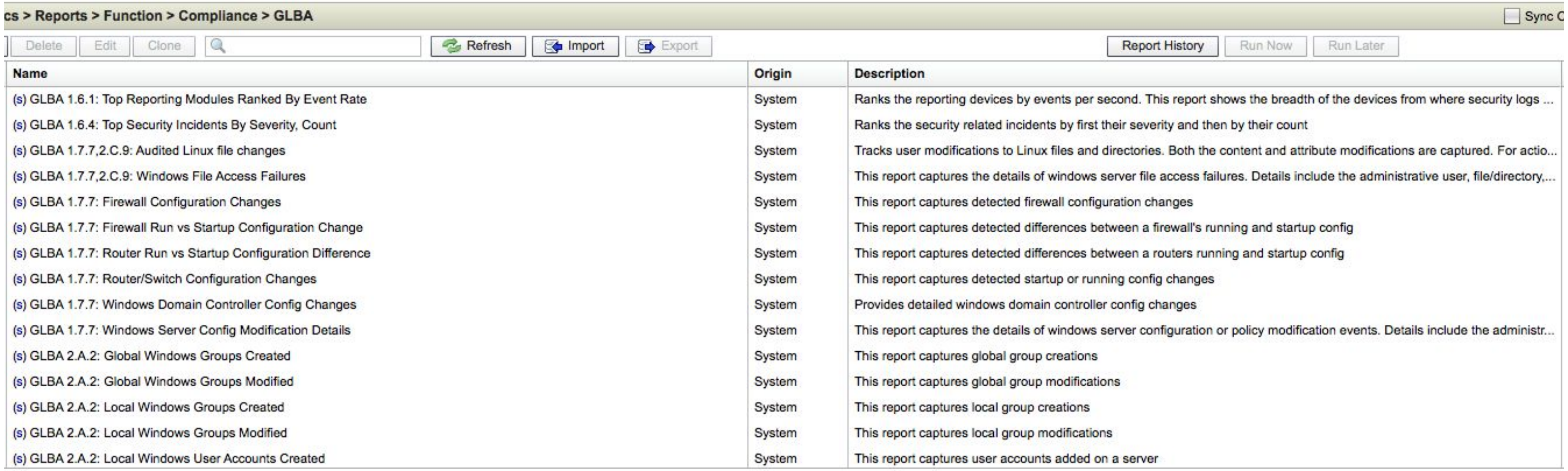
Name	Origin	Description
(s) FISMA AC-2: Computers added to domain	System	Captures computers added to a domain
(s) FISMA AC-2: Computers deleted from domain	System	Captures computers removed from a domain
(s) FISMA AC-2: Domain groups created	System	Captures domain group creations
(s) FISMA AC-2: Domain groups deleted	System	Captures domain group deletions
(s) FISMA AC-2: Domain groups modified	System	Captures domain group modifications
(s) FISMA AC-2: Domain user accounts created	System	Captures user accounts added to a domain
(s) FISMA AC-2: Domain user accounts deleted	System	Captures user accounts removed from a domain
(s) FISMA AC-2: Domain user accounts modified	System	Captures domain user account modifications.
(s) FISMA AC-2: Global Groups Created	System	This report captures global group creations
(s) FISMA AC-2: Global Groups Deleted	System	This report captures global group deletions
(s) FISMA AC-2: Global Groups Modified	System	This report captures global group modifications
(s) FISMA AC-2: Global Windows Groups Created	System	This report captures global group creations
(s) FISMA AC-2: Global Windows Groups Modified	System	This report captures global group modifications
(s) FISMA AC-2: Local Groups Created	System	This report captures local group creations
(s) FISMA AC-2: Local Windows Groups Created	System	This report captures local group creations
(s) FISMA AC-2: Local Windows Groups Modified	System	This report captures local group modifications
(s) FISMA AC-2: Local Windows User Accounts Created	System	This report captures user accounts added on a server
(s) FISMA AC-2: Local Windows User Accounts Deleted	System	This report captures user accounts removed from a server
(s) FISMA AC-2: Local Windows User Accounts Modified	System	This report captures local user account modifications.
(s) FISMA AC-2: Users Added To Global Groups	System	This report captures users added to global or univeral groups.
(s) FISMA AC-2: Users Added To Local Groups	System	This report captures users added to local groups.
(s) FISMA AC-3: Audited Linux file changes	System	Tracks user modifications to Linux files and directories. Both the content and attribute modifications are capture...
(s) FISMA AC-3: Detailed Successful Login At FISMA Device	System	Captures detailed successful logins at any device or application including servers, network devices, domain con...
(s) FISMA AC-3: Failed Firewall Admin Logons	System	Details about failed firewall logons
(s) FISMA AC-3: Failed Router Admin Logons	System	Details about failed router logons
(s) FISMA AC-3: Failed VPN Admin Logon	System	Provides event details for all failed VPN admin logons
(s) FISMA AC-3: Failed WLAN Admin Logon	System	Tracks failed admin logons to the WLAN Controller
(s) FISMA AC-3: Privileged Domain Controller Logon Attempts using the Administrator Account	System	Ranks the windows servers and their users by the number of failed logons using the administrator account
(s) FISMA AC-3: Privileged Windows Server Logon Attempts using the Administrator Account	System	This report details prvileged logon attempts to a windows server using the Administrator account
(s) FISMA AC-3: Remote Desktop Connections to Domain Controller	System	Details successful remote desktop connections
(s) FISMA AC-3: Remote Desktop Connections to Windows Servers	System	This report details successful and failed remote desktop connections
(s) FISMA AC-3: Successful Database Server Logon Details	System	Captures successful database server logons
(s) FISMA AC-3: Successful Firewall Admin Logons	System	Details about successful firewall logons

StratoZen FISMA Reports 2 of 2



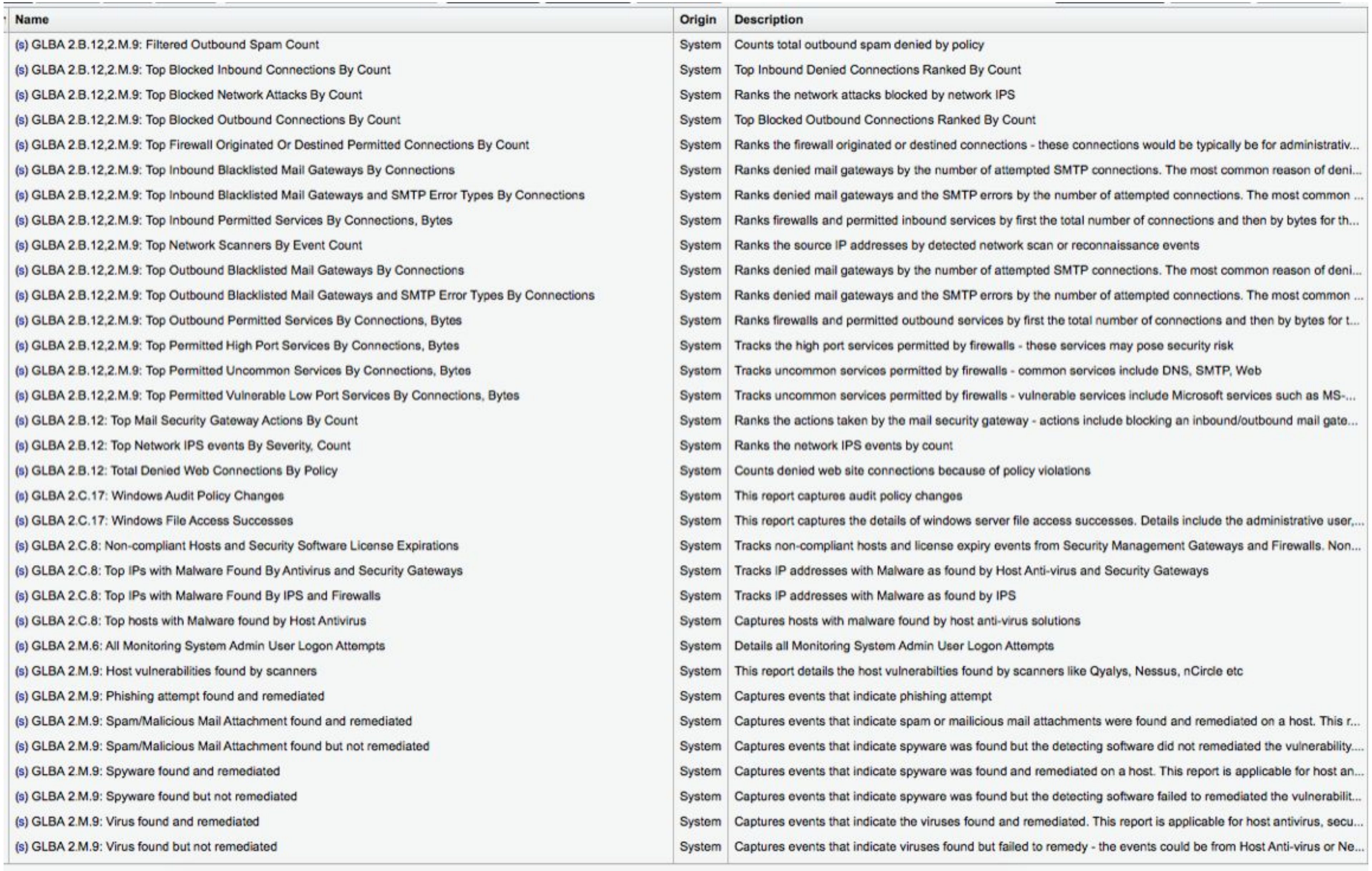
Name	Origin	Description
(s) FISMA CM-4: Router Run vs Startup Configuration Difference	System	This report captures detected differences between a routers running and startup config
(s) FISMA CM-4: Router/Switch Configuration Changes	System	This report captures detected startup or running config changes
(s) FISMA IR-4: Top Security Incidents By Severity, Count	System	Ranks the security related incidents by first their severity and then by their count
(s) FIS FISMA IR-4: Top Security Incidents By Severity, Count	System	Counts total inbound spam denied by spam filtering policy
(s) FISMA SI-4: Filtered Outbound Spam Count	System	Counts total outbound spam denied by policy
(s) FISMA SI-4: Host vulnerabilities found by scanners	System	This report details the host vulnerabilties found by scanners like Qyalys, Nessus, nCircle etc
(s) FISMA SI-4: Phishing attempt found and remediated	System	Captures events that indicate phishing attempt
(s) FISMA SI-4: Spam/Malicious Mail Attachment found and remediated	System	Captures events that indicate spam or mailicious mail attachments were found and remediated on a host. This r...
(s) FISMA SI-4: Spam/Malicious Mail Attachment found but not remediated	System	Captures events that indicate spyware was found but the detecting software did not remediated the vulnerability....
(s) FISMA SI-4: Spyware found and remediated	System	Captures events that indicate spyware was found and remediated on a host. This report is applicable for host an...
(s) FISMA SI-4: Spyware found but not remediated	System	Captures events that indicate spyware was found but the detecting software failed to remediated the vulnerabilit...
(s) FISMA SI-4: Top Blocked Inbound Connections By Count	System	Top Inbound Denied Connections Ranked By Count
(s) FISMA SI-4: Top Blocked Network Attacks By Count	System	Ranks the network attacks blocked by network IPS
(s) FISMA SI-4: Top Blocked Outbound Connections By Count	System	Top Blocked Outbound Connections Ranked By Count
(s) FISMA SI-4: Top Firewall Originated Or Destined Permitted Connections By Count	System	Ranks the firewall originated or destined connections - these connections would be typically be for administrativ...
(s) FISMA SI-4: Top IPs with Malware Found By Antivirus and Security Gateways	System	Tracks IP addresses with Malware as found by Host Anti-virus and Security Gateways
(s) FISMA SI-4: Top IPs with Malware Found By IPS and Firewalls	System	Tracks IP addresses with Malware as found by IPS
(s) FISMA SI-4: Top Inbound Blacklisted Mail Gateways By Connections	System	Ranks denied mail gateways by the number of attempted SMTP connections. The most common reason of deni...
(s) FISMA SI-4: Top Inbound Blacklisted Mail Gateways and SMTP Error Types By Connections	System	Ranks denied mail gateways and the SMTP errors by the number of attempted connections. The most common ...
(s) FISMA SI-4: Top Inbound Permitted Services By Connections, Bytes	System	Ranks firewalls and permitted inbound services by first the total number of connections and then by bytes for th...
(s) FISMA SI-4: Top Mail Security Gateway Actions By Count	System	Ranks the actions taken by the mail security gateway - actions include blocking an inbound/outbound mail gate...
(s) FISMA SI-4: Top Network IPS events By Severity, Count	System	Ranks the network IPS events by count
(s) FISMA SI-4: Top Network Scanners By Event Count	System	Ranks the source IP addresses by detected network scan or reconnaissance events
(s) FISMA SI-4: Top Outbound Blacklisted Mail Gateways By Connections	System	Ranks denied mail gateways by the number of attempted SMTP connections. The most common reason of deni...
(s) FISMA SI-4: Top Outbound Blacklisted Mail Gateways and SMTP Error Types By Connections	System	Ranks denied mail gateways and the SMTP errors by the number of attempted connections. The most common ...
(s) FISMA SI-4: Top Outbound Permitted Services By Connections, Bytes	System	Ranks firewalls and permitted outbound services by first the total number of connections and then by bytes for t...
(s) FISMA SI-4: Top Permitted High Port Services By Connections, Bytes	System	Tracks the high port services permitted by firewalls - these services may pose security risk
(s) FISMA SI-4: Top Permitted Uncommon Services By Connections, Bytes	System	Tracks uncommon services permitted by firewalls - common services include DNS, SMTP, Web
(s) FISMA SI-4: Top Permitted Vulnerable Low Port Services By Connections, Bytes	System	Tracks uncommon services permitted by firewalls - vulnerable services include Microsoft services such as MS-...
(s) FISMA SI-4: Top hosts with Malware found by Host Antivirus	System	Captures hosts with malware found by host anti-virus solutions
(s) FISMA SI-4: Total Denied Web Connections By Policy	System	Counts denied web site connections because of policy violations
(s) FISMA SI-4: Virus found and remediated	System	Captures events that indicate the viruses found and remediated. This report is applicable for host antivirus, secu...
(s) FISMA SI-4: Virus found but not remediated	System	Captures events that indicate viruses found but failed to remedy - the events could be from Host Anti-virus or Ne...

StratoZen GLBA Reports 1 of 2



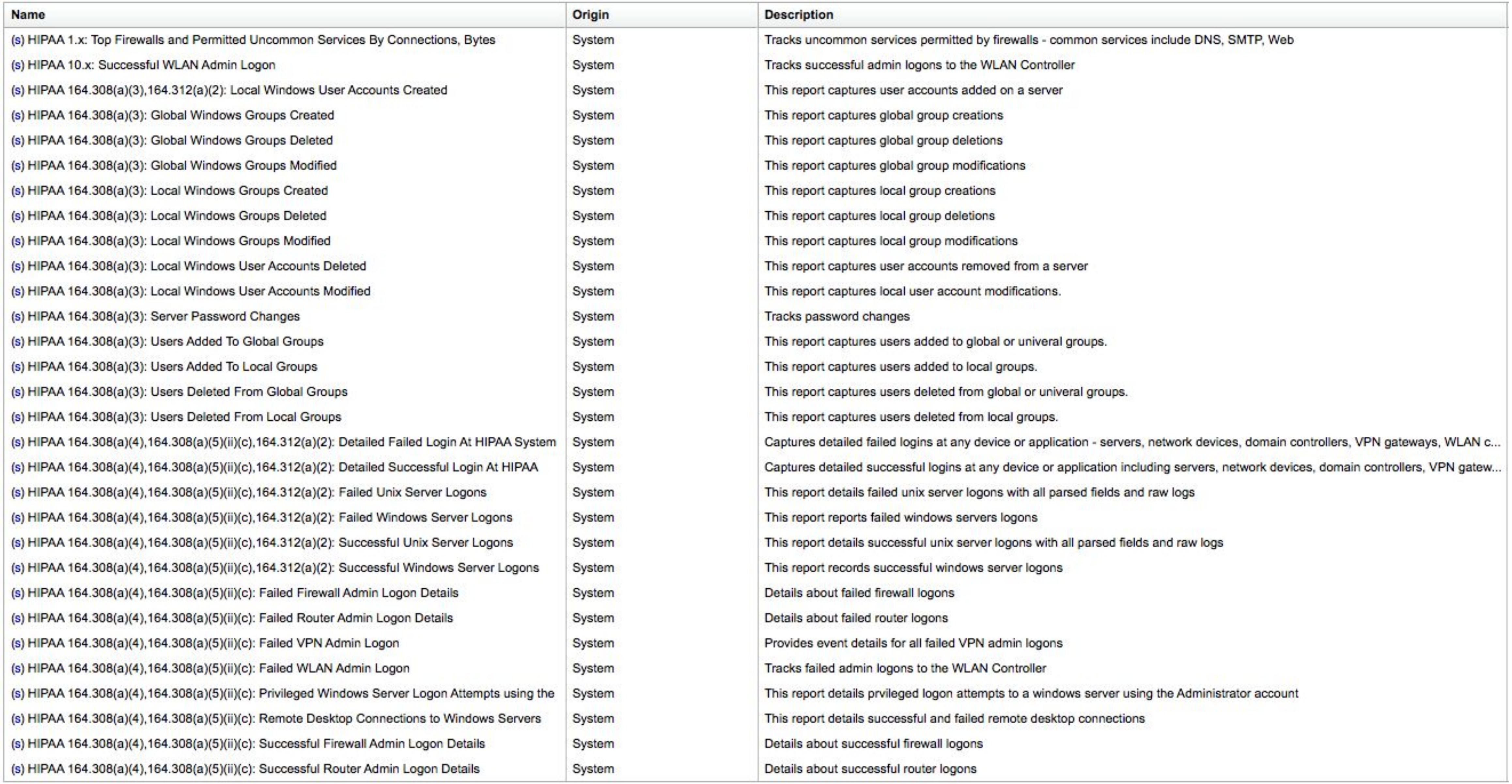
Name	Origin	Description
(s) GLBA 1.6.1: Top Reporting Modules Ranked By Event Rate	System	Ranks the reporting devices by events per second. This report shows the breadth of the devices from where security logs ...
(s) GLBA 1.6.4: Top Security Incidents By Severity, Count	System	Ranks the security related incidents by first their severity and then by their count
(s) GLBA 1.7.7,2.C.9: Audited Linux file changes	System	Tracks user modifications to Linux files and directories. Both the content and attribute modifications are captured. For actio...
(s) GLBA 1.7.7,2.C.9: Windows File Access Failures	System	This report captures the details of windows server file access failures. Details include the administrative user, file/directory,...
(s) GLBA 1.7.7: Firewall Configuration Changes	System	This report captures detected firewall configuration changes
(s) GLBA 1.7.7: Firewall Run vs Startup Configuration Change	System	This report captures detected differences between a firewall's running and startup config
(s) GLBA 1.7.7: Router Run vs Startup Configuration Difference	System	This report captures detected differences between a routers running and startup config
(s) GLBA 1.7.7: Router/Switch Configuration Changes	System	This report captures detected startup or running config changes
(s) GLBA 1.7.7: Windows Domain Controller Config Changes	System	Provides detailed windows domain controller config changes
(s) GLBA 1.7.7: Windows Server Config Modification Details	System	This report captures the details of windows server configuration or policy modification events. Details include the administr...
(s) GLBA 2.A.2: Global Windows Groups Created	System	This report captures global group creations
(s) GLBA 2.A.2: Global Windows Groups Modified	System	This report captures global group modifications
(s) GLBA 2.A.2: Local Windows Groups Created	System	This report captures local group creations
(s) GLBA 2.A.2: Local Windows Groups Modified	System	This report captures local group modifications
(s) GLBA 2.A.2: Local Windows User Accounts Created	System	This report captures user accounts added on a server

StratoZen GLBA Reports 2 of 2



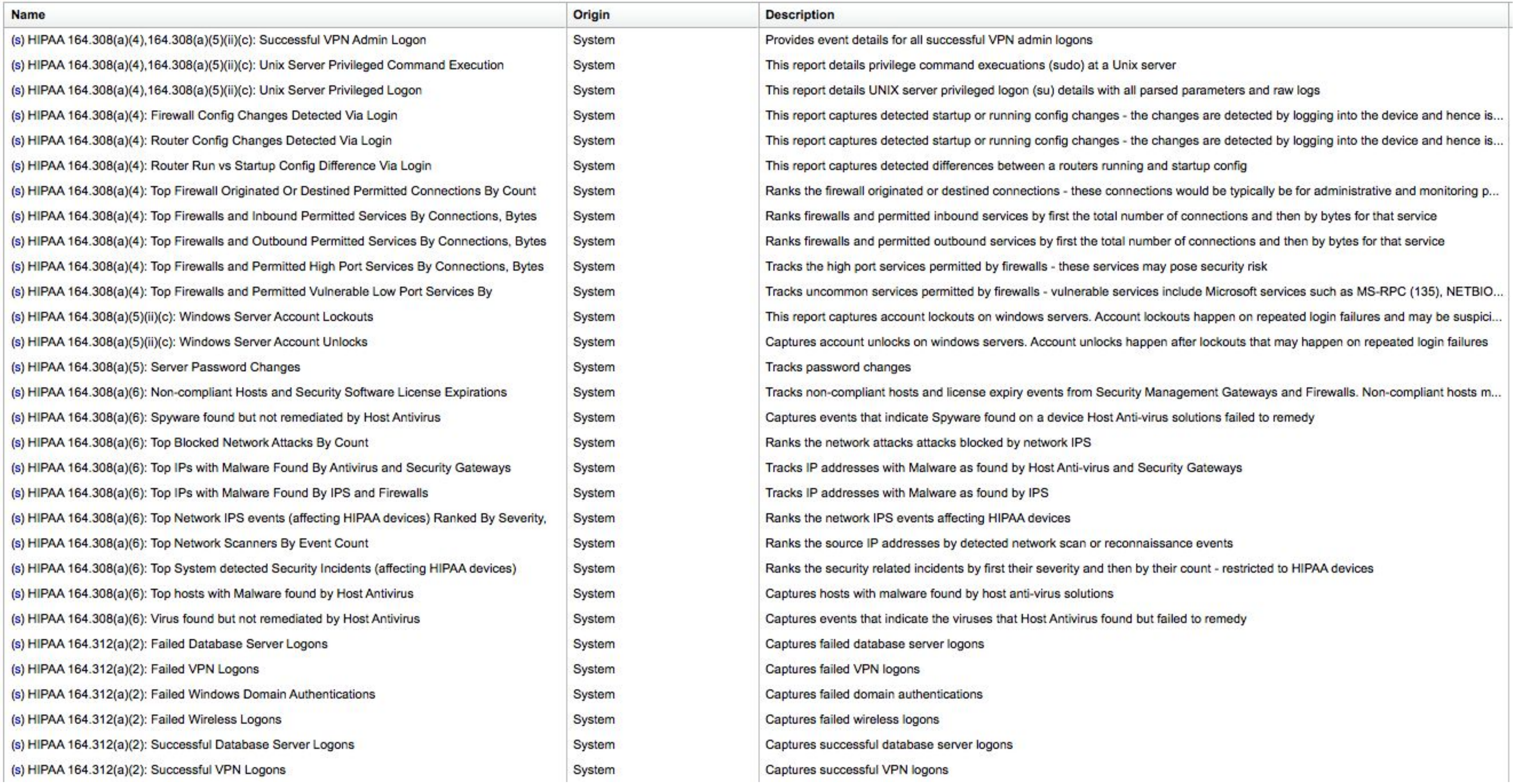
Name	Origin	Description
(s) GLBA 2.B.12,2.M.9: Filtered Outbound Spam Count	System	Counts total outbound spam denied by policy
(s) GLBA 2.B.12,2.M.9: Top Blocked Inbound Connections By Count	System	Top Inbound Denied Connections Ranked By Count
(s) GLBA 2.B.12,2.M.9: Top Blocked Network Attacks By Count	System	Ranks the network attacks blocked by network IPS
(s) GLBA 2.B.12,2.M.9: Top Blocked Outbound Connections By Count	System	Top Blocked Outbound Connections Ranked By Count
(s) GLBA 2.B.12,2.M.9: Top Firewall Originated Or Destined Permitted Connections By Count	System	Ranks the firewall originated or destined connections - these connections would be typically be for administrativ...
(s) GLBA 2.B.12,2.M.9: Top Inbound Blacklisted Mail Gateways By Connections	System	Ranks denied mail gateways by the number of attempted SMTP connections. The most common reason of deni...
(s) GLBA 2.B.12,2.M.9: Top Inbound Blacklisted Mail Gateways and SMTP Error Types By Connections	System	Ranks denied mail gateways and the SMTP errors by the number of attempted connections. The most common ...
(s) GLBA 2.B.12,2.M.9: Top Inbound Permitted Services By Connections, Bytes	System	Ranks firewalls and permitted inbound services by first the total number of connections and then by bytes for th...
(s) GLBA 2.B.12,2.M.9: Top Network Scanners By Event Count	System	Ranks the source IP addresses by detected network scan or reconnaissance events
(s) GLBA 2.B.12,2.M.9: Top Outbound Blacklisted Mail Gateways By Connections	System	Ranks denied mail gateways by the number of attempted SMTP connections. The most common reason of deni...
(s) GLBA 2.B.12,2.M.9: Top Outbound Blacklisted Mail Gateways and SMTP Error Types By Connections	System	Ranks denied mail gateways and the SMTP errors by the number of attempted connections. The most common ...
(s) GLBA 2.B.12,2.M.9: Top Outbound Permitted Services By Connections, Bytes	System	Ranks firewalls and permitted outbound services by first the total number of connections and then by bytes for t...
(s) GLBA 2.B.12,2.M.9: Top Permitted High Port Services By Connections, Bytes	System	Tracks the high port services permitted by firewalls - these services may pose security risk
(s) GLBA 2.B.12,2.M.9: Top Permitted Uncommon Services By Connections, Bytes	System	Tracks uncommon services permitted by firewalls - common services include DNS, SMTP, Web
(s) GLBA 2.B.12,2.M.9: Top Permitted Vulnerable Low Port Services By Connections, Bytes	System	Tracks uncommon services permitted by firewalls - vulnerable services include Microsoft services such as MS-...
(s) GLBA 2.B.12: Top Mail Security Gateway Actions By Count	System	Ranks the actions taken by the mail security gateway - actions include blocking an inbound/outbound mail gate...
(s) GLBA 2.B.12: Top Network IPS events By Severity, Count	System	Ranks the network IPS events by count
(s) GLBA 2.B.12: Total Denied Web Connections By Policy	System	Counts denied web site connections because of policy violations
(s) GLBA 2.C.17: Windows Audit Policy Changes	System	This report captures audit policy changes
(s) GLBA 2.C.17: Windows File Access Successes	System	This report captures the details of windows server file access successes. Details include the administrative user,...
(s) GLBA 2.C.8: Non-compliant Hosts and Security Software License Expirations	System	Tracks non-compliant hosts and license expiry events from Security Management Gateways and Firewalls. Non...
(s) GLBA 2.C.8: Top IPs with Malware Found By Antivirus and Security Gateways	System	Tracks IP addresses with Malware as found by Host Anti-virus and Security Gateways
(s) GLBA 2.C.8: Top IPs with Malware Found By IPS and Firewalls	System	Tracks IP addresses with Malware as found by IPS
(s) GLBA 2.C.8: Top hosts with Malware found by Host Antivirus	System	Captures hosts with malware found by host anti-virus solutions
(s) GLBA 2.M.6: All Monitoring System Admin User Logon Attempts	System	Details all Monitoring System Admin User Logon Attempts
(s) GLBA 2.M.9: Host vulnerabilities found by scanners	System	This report details the host vulnerabilties found by scanners like Qyalys, Nessus, nCircle etc
(s) GLBA 2.M.9: Phishing attempt found and remediated	System	Captures events that indicate phishing attempt
(s) GLBA 2.M.9: Spam/Malicious Mail Attachment found and remediated	System	Captures events that indicate spam or mailicious mail attachments were found and remediated on a host. This r...
(s) GLBA 2.M.9: Spam/Malicious Mail Attachment found but not remediated	System	Captures events that indicate spyware was found but the detecting software did not remediated the vulnerability....
(s) GLBA 2.M.9: Spyware found and remediated	System	Captures events that indicate spyware was found and remediated on a host. This report is applicable for host an...
(s) GLBA 2.M.9: Spyware found but not remediated	System	Captures events that indicate spyware was found but the detecting software failed to remediated the vulnerabilit...
(s) GLBA 2.M.9: Virus found and remediated	System	Captures events that indicate the viruses found and remediated. This report is applicable for host antivirus, secu...
(s) GLBA 2.M.9: Virus found but not remediated	System	Captures events that indicate viruses found but failed to remedy - the events could be from Host Anti-virus or Ne...

StratoZen HIPAA Reports 1 of 3



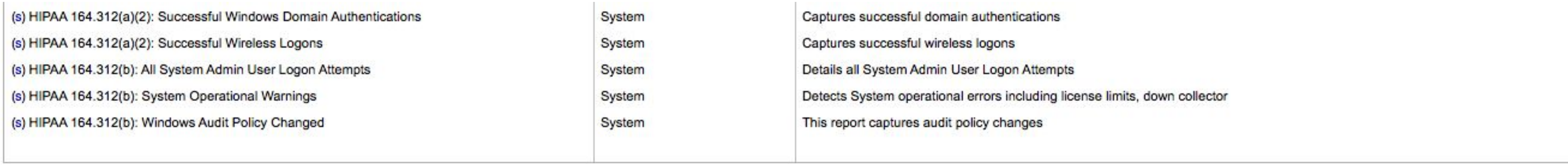
Name	Origin	Description
(s) HIPAA 1.x: Top Firewalls and Permitted Uncommon Services By Connections, Bytes	System	Tracks uncommon services permitted by firewalls - common services include DNS, SMTP, Web
(s) HIPAA 10.x: Successful WLAN Admin Logon	System	Tracks successful admin logons to the WLAN Controller
(s) HIPAA 164.308(a)(3),164.312(a)(2): Local Windows User Accounts Created	System	This report captures user accounts added on a server
(s) HIPAA 164.308(a)(3): Global Windows Groups Created	System	This report captures global group creations
(s) HIPAA 164.308(a)(3): Global Windows Groups Deleted	System	This report captures global group deletions
(s) HIPAA 164.308(a)(3): Global Windows Groups Modified	System	This report captures global group modifications
(s) HIPAA 164.308(a)(3): Local Windows Groups Created	System	This report captures local group creations
(s) HIPAA 164.308(a)(3): Local Windows Groups Deleted	System	This report captures local group deletions
(s) HIPAA 164.308(a)(3): Local Windows Groups Modified	System	This report captures local group modifications
(s) HIPAA 164.308(a)(3): Local Windows User Accounts Deleted	System	This report captures user accounts removed from a server
(s) HIPAA 164.308(a)(3): Local Windows User Accounts Modified	System	This report captures local user account modifications.
(s) HIPAA 164.308(a)(3): Server Password Changes	System	Tracks password changes
(s) HIPAA 164.308(a)(3): Users Added To Global Groups	System	This report captures users added to global or univeral groups.
(s) HIPAA 164.308(a)(3): Users Added To Local Groups	System	This report captures users added to local groups.
(s) HIPAA 164.308(a)(3): Users Deleted From Global Groups	System	This report captures users deleted from global or univeral groups.
(s) HIPAA 164.308(a)(3): Users Deleted From Local Groups	System	This report captures users deleted from local groups.
(s) HIPAA 164.308(a)(4),164.308(a)(5)(ii)(c),164.312(a)(2): Detailed Failed Login At HIPAA System	System	Captures detailed failed logins at any device or application - servers, network devices, domain controllers, VPN gateways, WLAN c...
(s) HIPAA 164.308(a)(4),164.308(a)(5)(ii)(c),164.312(a)(2): Detailed Successful Login At HIPAA	System	Captures detailed successful logins at any device or application including servers, network devices, domain controllers, VPN gatew...
(s) HIPAA 164.308(a)(4),164.308(a)(5)(ii)(c),164.312(a)(2): Failed Unix Server Logons	System	This report details failed unix server logons with all parsed fields and raw logs
(s) HIPAA 164.308(a)(4),164.308(a)(5)(ii)(c),164.312(a)(2): Failed Windows Server Logons	System	This report reports failed windows servers logons
(s) HIPAA 164.308(a)(4),164.308(a)(5)(ii)(c),164.312(a)(2): Successful Unix Server Logons	System	This report details successful unix server logons with all parsed fields and raw logs
(s) HIPAA 164.308(a)(4),164.308(a)(5)(ii)(c),164.312(a)(2): Successful Windows Server Logons	System	This report records successful windows server logons
(s) HIPAA 164.308(a)(4),164.308(a)(5)(ii)(c): Failed Firewall Admin Logon Details	System	Details about failed firewall logons
(s) HIPAA 164.308(a)(4),164.308(a)(5)(ii)(c): Failed Router Admin Logon Details	System	Details about failed router logons
(s) HIPAA 164.308(a)(4),164.308(a)(5)(ii)(c): Failed VPN Admin Logon	System	Provides event details for all failed VPN admin logons
(s) HIPAA 164.308(a)(4),164.308(a)(5)(ii)(c): Failed WLAN Admin Logon	System	Tracks failed admin logons to the WLAN Controller
(s) HIPAA 164.308(a)(4),164.308(a)(5)(ii)(c): Privileged Windows Server Logon Attempts using the	System	This report details prvileged logon attempts to a windows server using the Administrator account
(s) HIPAA 164.308(a)(4),164.308(a)(5)(ii)(c): Remote Desktop Connections to Windows Servers	System	This report details successful and failed remote desktop connections
(s) HIPAA 164.308(a)(4),164.308(a)(5)(ii)(c): Successful Firewall Admin Logon Details	System	Details about successful firewall logons
(s) HIPAA 164.308(a)(4),164.308(a)(5)(ii)(c): Successful Router Admin Logon Details	System	Details about successful router logons

StratoZen HIPAA Reports 2 of 3



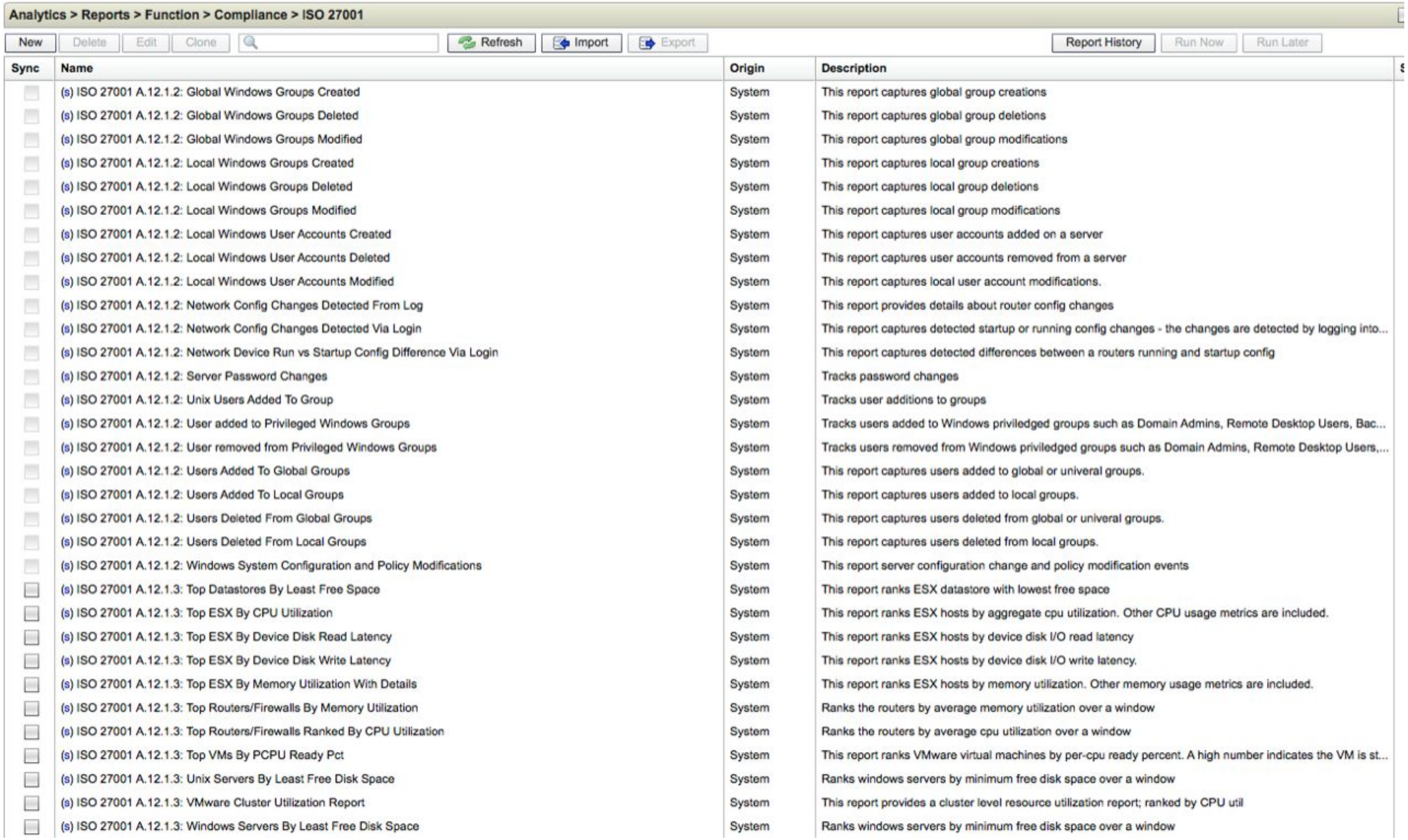
Name	Origin	Description
(s) HIPAA 164.308(a)(4),164.308(a)(5)(ii)(c): Successful VPN Admin Logon	System	Provides event details for all successful VPN admin logons
(s) HIPAA 164.308(a)(4),164.308(a)(5)(ii)(c): Unix Server Privileged Command Execution	System	This report details privilege command execuations (sudo) at a Unix server
(s) HIPAA 164.308(a)(4),164.308(a)(5)(ii)(c): Unix Server Privileged Logon	System	This report details UNIX server privileged logon (su) details with all parsed parameters and raw logs
(s) HIPAA 164.308(a)(4): Firewall Config Changes Detected Via Login	System	This report captures detected startup or running config changes - the changes are detected by logging into the device and hence is...
(s) HIPAA 164.308(a)(4): Router Config Changes Detected Via Login	System	This report captures detected startup or running config changes - the changes are detected by logging into the device and hence is...
(s) HIPAA 164.308(a)(4): Router Run vs Startup Config Difference Via Login	System	This report captures detected differences between a routers running and startup config
(s) HIPAA 164.308(a)(4): Top Firewall Originated Or Destined Permitted Connections By Count	System	Ranks the firewall originated or destined connections - these connections would be typically be for administrative and monitoring p...
(s) HIPAA 164.308(a)(4): Top Firewalls and Inbound Permitted Services By Connections, Bytes	System	Ranks firewalls and permitted inbound services by first the total number of connections and then by bytes for that service
(s) HIPAA 164.308(a)(4): Top Firewalls and Outbound Permitted Services By Connections, Bytes	System	Ranks firewalls and permitted outbound services by first the total number of connections and then by bytes for that service
(s) HIPAA 164.308(a)(4): Top Firewalls and Permitted High Port Services By Connections, Bytes	System	Tracks the high port services permitted by firewalls - these services may pose security risk
(s) HIPAA 164.308(a)(4): Top Firewalls and Permitted Vulnerable Low Port Services By	System	Tracks uncommon services permitted by firewalls - vulnerable services include Microsoft services such as MS-RPC (135), NETBIO...
(s) HIPAA 164.308(a)(5)(ii)(c): Windows Server Account Lockouts	System	This report captures account lockouts on windows servers. Account lockouts happen on repeated login failures and may be suspici...
(s) HIPAA 164.308(a)(5)(ii)(c): Windows Server Account Unlocks	System	Captures account unlocks on windows servers. Account unlocks happen after lockouts that may happen on repeated login failures
(s) HIPAA 164.308(a)(5): Server Password Changes	System	Tracks password changes
(s) HIPAA 164.308(a)(6): Non-compliant Hosts and Security Software License Expirations	System	Tracks non-compliant hosts and license expiry events from Security Management Gateways and Firewalls. Non-compliant hosts m...
(s) HIPAA 164.308(a)(6): Spyware found but not remediated by Host Antivirus	System	Captures events that indicate Spyware found on a device Host Anti-virus solutions failed to remedy
(s) HIPAA 164.308(a)(6): Top Blocked Network Attacks By Count	System	Ranks the network attacks attacks blocked by network IPS
(s) HIPAA 164.308(a)(6): Top IPs with Malware Found By Antivirus and Security Gateways	System	Tracks IP addresses with Malware as found by Host Anti-virus and Security Gateways
(s) HIPAA 164.308(a)(6): Top IPs with Malware Found By IPS and Firewalls	System	Tracks IP addresses with Malware as found by IPS
(s) HIPAA 164.308(a)(6): Top Network IPS events (affecting HIPAA devices) Ranked By Severity,	System	Ranks the network IPS events affecting HIPAA devices
(s) HIPAA 164.308(a)(6): Top Network Scanners By Event Count	System	Ranks the source IP addresses by detected network scan or reconnaissance events
(s) HIPAA 164.308(a)(6): Top System detected Security Incidents (affecting HIPAA devices)	System	Ranks the security related incidents by first their severity and then by their count - restricted to HIPAA devices
(s) HIPAA 164.308(a)(6): Top hosts with Malware found by Host Antivirus	System	Captures hosts with malware found by host anti-virus solutions
(s) HIPAA 164.308(a)(6): Virus found but not remediated by Host Antivirus	System	Captures events that indicate the viruses that Host Antivirus found but failed to remedy
(s) HIPAA 164.312(a)(2): Failed Database Server Logons	System	Captures failed database server logons
(s) HIPAA 164.312(a)(2): Failed VPN Logons	System	Captures failed VPN logons
(s) HIPAA 164.312(a)(2): Failed Windows Domain Authentications	System	Captures failed domain authentications
(s) HIPAA 164.312(a)(2): Failed Wireless Logons	System	Captures failed wireless logons
(s) HIPAA 164.312(a)(2): Successful Database Server Logons	System	Captures successful database server logons
(s) HIPAA 164.312(a)(2): Successful VPN Logons	System	Captures successful VPN logons

StratoZen HIPAA Reports 3 of 3



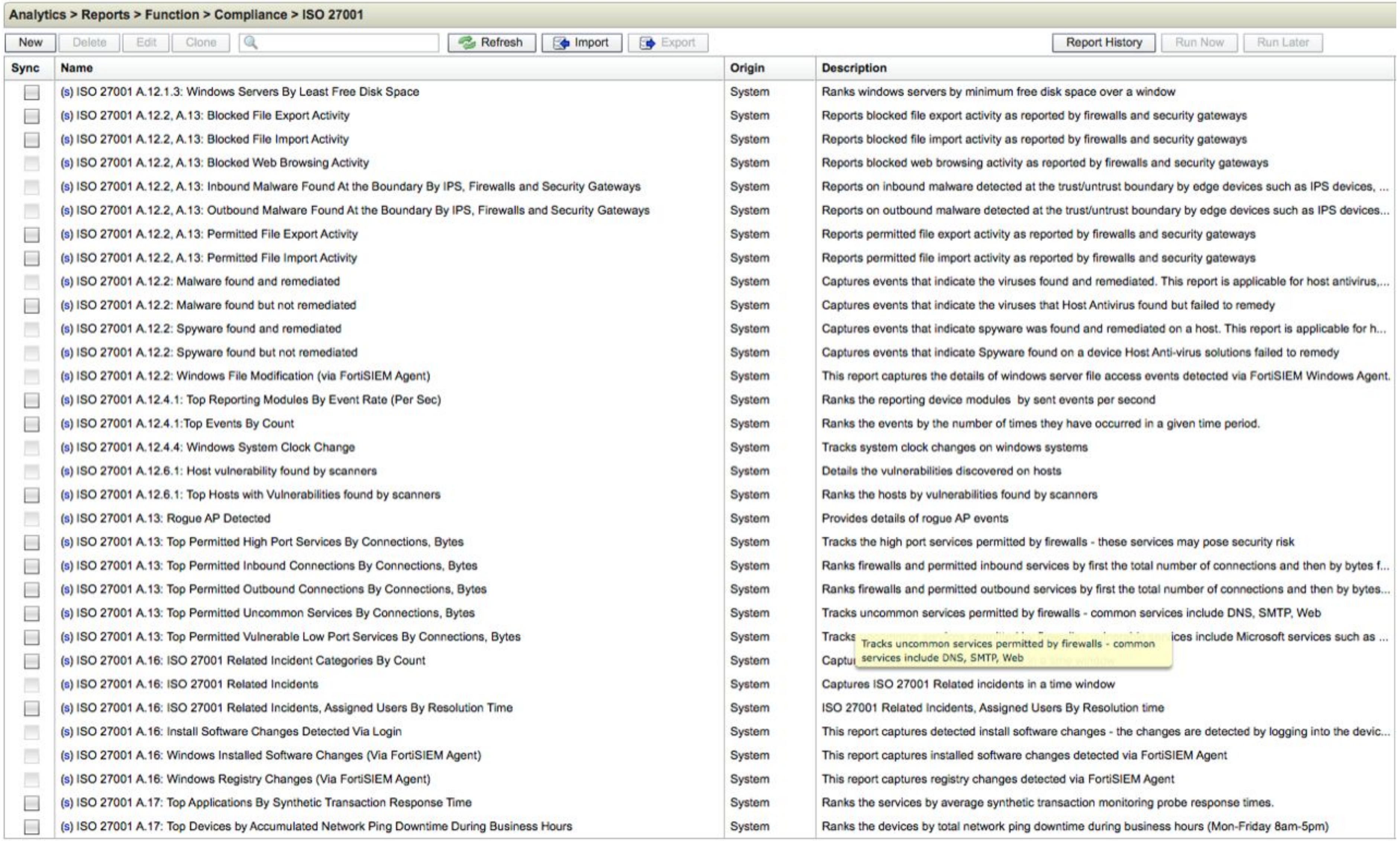
(s) HIPAA 164.312(a)(2): Successful Windows Domain Authentications	System	Captures successful domain authentications
(s) HIPAA 164.312(a)(2): Successful Wireless Logons	System	Captures successful wireless logons
(s) HIPAA 164.312(b): All System Admin User Logon Attempts	System	Details all System Admin User Logon Attempts
(s) HIPAA 164.312(b): System Operational Warnings	System	Detects System operational errors including license limits, down collector
(s) HIPAA 164.312(b): Windows Audit Policy Changed	System	This report captures audit policy changes

StratoZen ISO 27001 Reports 1 of 3



Sync	Name	Origin	Description
☐	(s) ISO 27001 A.12.1.2: Global Windows Groups Created	System	This report captures global group creations
☐	(s) ISO 27001 A.12.1.2: Global Windows Groups Deleted	System	This report captures global group deletions
☐	(s) ISO 27001 A.12.1.2: Global Windows Groups Modified	System	This report captures global group modifications
☐	(s) ISO 27001 A.12.1.2: Local Windows Groups Created	System	This report captures local group creations
☐	(s) ISO 27001 A.12.1.2: Local Windows Groups Deleted	System	This report captures local group deletions
☐	(s) ISO 27001 A.12.1.2: Local Windows Groups Modified	System	This report captures local group modifications
☐	(s) ISO 27001 A.12.1.2: Local Windows User Accounts Created	System	This report captures user accounts added on a server
☐	(s) ISO 27001 A.12.1.2: Local Windows User Accounts Deleted	System	This report captures user accounts removed from a server
☐	(s) ISO 27001 A.12.1.2: Local Windows User Accounts Modified	System	This report captures local user account modifications.
☐	(s) ISO 27001 A.12.1.2: Network Config Changes Detected From Log	System	This report provides details about router config changes
☐	(s) ISO 27001 A.12.1.2: Network Config Changes Detected Via Login	System	This report captures detected startup or running config changes - the changes are detected by logging into...
☐	(s) ISO 27001 A.12.1.2: Network Device Run vs Startup Config Difference Via Login	System	This report captures detected differences between a routers running and startup config
☐	(s) ISO 27001 A.12.1.2: Server Password Changes	System	Tracks password changes
☐	(s) ISO 27001 A.12.1.2: Unix Users Added To Group	System	Tracks user additions to groups
☐	(s) ISO 27001 A.12.1.2: User added to Privileged Windows Groups	System	Tracks users added to Windows priviledged groups such as Domain Admins, Remote Desktop Users, Bac...
☐	(s) ISO 27001 A.12.1.2: User removed from Privileged Windows Groups	System	Tracks users removed from Windows priviledged groups such as Domain Admins, Remote Desktop Users,...
☐	(s) ISO 27001 A.12.1.2: Users Added To Global Groups	System	This report captures users added to global or univeral groups.
☐	(s) ISO 27001 A.12.1.2: Users Added To Local Groups	System	This report captures users added to local groups.
☐	(s) ISO 27001 A.12.1.2: Users Deleted From Global Groups	System	This report captures users deleted from global or univeral groups.
☐	(s) ISO 27001 A.12.1.2: Users Deleted From Local Groups	System	This report captures users deleted from local groups.
☐	(s) ISO 27001 A.12.1.2: Windows System Configuration and Policy Modifications	System	This report server configuration change and policy modification events
☐	(s) ISO 27001 A.12.1.3: Top Datastores By Least Free Space	System	This report ranks ESX datastore with lowest free space
☐	(s) ISO 27001 A.12.1.3: Top ESX By CPU Utilization	System	This report ranks ESX hosts by aggregate cpu utilization. Other CPU usage metrics are included.
☐	(s) ISO 27001 A.12.1.3: Top ESX By Device Disk Read Latency	System	This report ranks ESX hosts by device disk I/O read latency
☐	(s) ISO 27001 A.12.1.3: Top ESX By Device Disk Write Latency	System	This report ranks ESX hosts by device disk I/O write latency.
☐	(s) ISO 27001 A.12.1.3: Top ESX By Memory Utilization With Details	System	This report ranks ESX hosts by memory utilization. Other memory usage metrics are included.
☐	(s) ISO 27001 A.12.1.3: Top Routers/Firewalls By Memory Utilization	System	Ranks the routers by average memory utilization over a window
☐	(s) ISO 27001 A.12.1.3: Top Routers/Firewalls Ranked By CPU Utilization	System	Ranks the routers by average cpu utilization over a window
☐	(s) ISO 27001 A.12.1.3: Top VMs By PCPU Ready Pct	System	This report ranks VMware virtual machines by per-cpu ready percent. A high number indicates the VM is st...
☐	(s) ISO 27001 A.12.1.3: Unix Servers By Least Free Disk Space	System	Ranks windows servers by minimum free disk space over a window
☐	(s) ISO 27001 A.12.1.3: VMware Cluster Utilization Report	System	This report provides a cluster level resource utilization report; ranked by CPU util
☐	(s) ISO 27001 A.12.1.3: Windows Servers By Least Free Disk Space	System	Ranks windows servers by minimum free disk space over a window

StratoZen ISO 27001 Reports 2 of 3

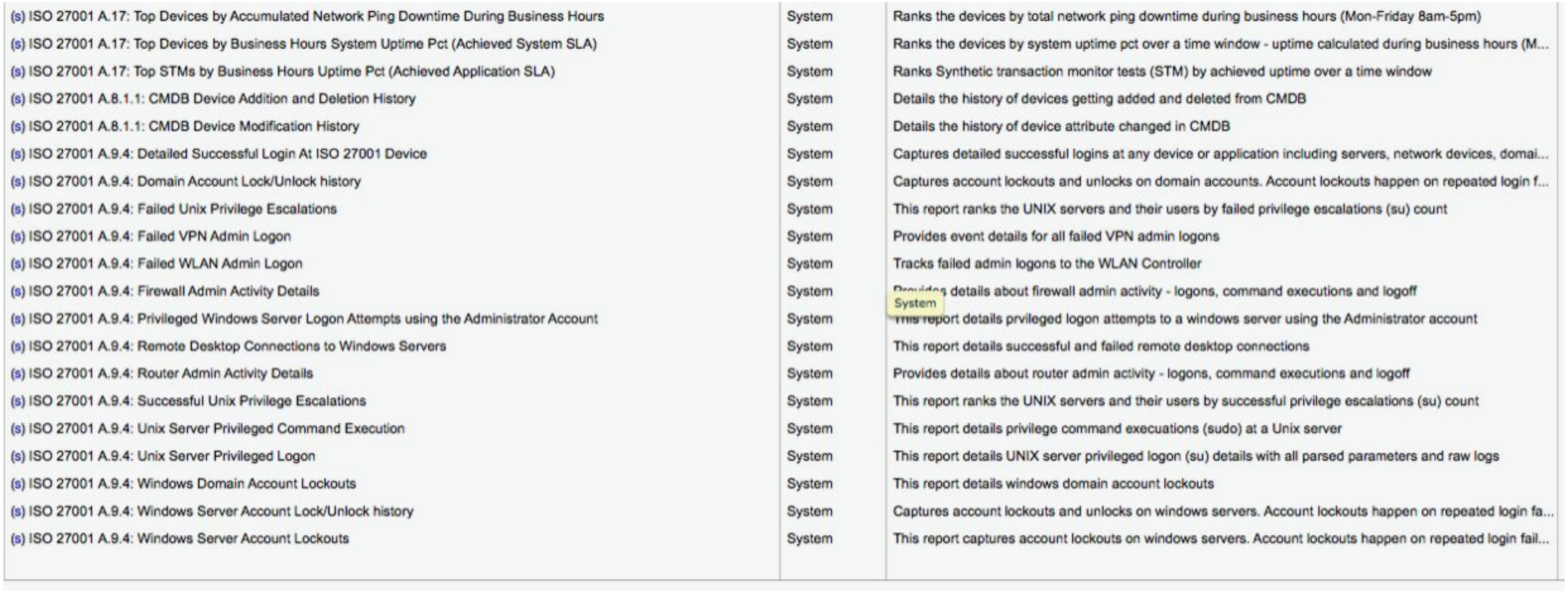


Analytics > Reports > Function > Compliance > ISO 27001

Sync	Name	Origin	Description
☐	(s) ISO 27001 A.12.1.3: Windows Servers By Least Free Disk Space	System	Ranks windows servers by minimum free disk space over a window
☐	(s) ISO 27001 A.12.2, A.13: Blocked File Export Activity	System	Reports blocked file export activity as reported by firewalls and security gateways
☐	(s) ISO 27001 A.12.2, A.13: Blocked File Import Activity	System	Reports blocked file import activity as reported by firewalls and security gateways
☐	(s) ISO 27001 A.12.2, A.13: Blocked Web Browsing Activity	System	Reports blocked web browsing activity as reported by firewalls and security gateways
☐	(s) ISO 27001 A.12.2, A.13: Inbound Malware Found At the Boundary By IPS, Firewalls and Security Gateways	System	Reports on inbound malware detected at the trust/untrust boundary by edge devices such as IPS devices, ...
☐	(s) ISO 27001 A.12.2, A.13: Outbound Malware Found At the Boundary By IPS, Firewalls and Security Gateways	System	Reports on outbound malware detected at the trust/untrust boundary by edge devices such as IPS devices...
☐	(s) ISO 27001 A.12.2, A.13: Permitted File Export Activity	System	Reports permitted file export activity as reported by firewalls and security gateways
☐	(s) ISO 27001 A.12.2, A.13: Permitted File Import Activity	System	Reports permitted file import activity as reported by firewalls and security gateways
☐	(s) ISO 27001 A.12.2: Malware found and remediated	System	Captures events that indicate the viruses found and remediated. This report is applicable for host antivirus,...
☐	(s) ISO 27001 A.12.2: Malware found but not remediated	System	Captures events that indicate the viruses that Host Antivirus found but failed to remedy
☐	(s) ISO 27001 A.12.2: Spyware found and remediated	System	Captures events that indicate spyware was found and remediated on a host. This report is applicable for h...
☐	(s) ISO 27001 A.12.2: Spyware found but not remediated	System	Captures events that indicate Spyware found on a device Host Anti-virus solutions failed to remedy
☐	(s) ISO 27001 A.12.2: Windows File Modification (via FortiSIEM Agent)	System	This report captures the details of windows server file access events detected via FortiSIEM Windows Agent.
☐	(s) ISO 27001 A.12.4.1: Top Reporting Modules By Event Rate (Per Sec)	System	Ranks the reporting device modules by sent events per second
☐	(s) ISO 27001 A.12.4.1:Top Events By Count	System	Ranks the events by the number of times they have occurred in a given time period.
☐	(s) ISO 27001 A.12.4.4: Windows System Clock Change	System	Tracks system clock changes on windows systems
☐	(s) ISO 27001 A.12.6.1: Host vulnerability found by scanners	System	Details the vulnerabilities discovered on hosts
☐	(s) ISO 27001 A.12.6.1: Top Hosts with Vulnerabilities found by scanners	System	Ranks the hosts by vulnerabilities found by scanners
☐	(s) ISO 27001 A.13: Rogue AP Detected	System	Provides details of rogue AP events
☐	(s) ISO 27001 A.13: Top Permitted High Port Services By Connections, Bytes	System	Tracks the high port services permitted by firewalls - these services may pose security risk
☐	(s) ISO 27001 A.13: Top Permitted Inbound Connections By Connections, Bytes	System	Ranks firewalls and permitted inbound services by first the total number of connections and then by bytes f...
☐	(s) ISO 27001 A.13: Top Permitted Outbound Connections By Connections, Bytes	System	Ranks firewalls and permitted outbound services by first the total number of connections and then by bytes...
☐	(s) ISO 27001 A.13: Top Permitted Uncommon Services By Connections, Bytes	System	Tracks uncommon services permitted by firewalls - common services include DNS, SMTP, Web
☐	(s) ISO 27001 A.13: Top Permitted Vulnerable Low Port Services By Connections, Bytes	System	Tracks ices include Microsoft services such as ...
☐	(s) ISO 27001 A.16: ISO 27001 Related Incident Categories By Count	System	Captu
☐	(s) ISO 27001 A.16: ISO 27001 Related Incidents	System	Captures ISO 27001 Related incidents in a time window
☐	(s) ISO 27001 A.16: ISO 27001 Related Incidents, Assigned Users By Resolution Time	System	ISO 27001 Related Incidents, Assigned Users By Resolution time
☐	(s) ISO 27001 A.16: Install Software Changes Detected Via Login	System	This report captures detected install software changes - the changes are detected by logging into the devic...
☐	(s) ISO 27001 A.16: Windows Installed Software Changes (Via FortiSIEM Agent)	System	This report captures installed software changes detected via FortiSIEM Agent
☐	(s) ISO 27001 A.16: Windows Registry Changes (Via FortiSIEM Agent)	System	This report captures registry changes detected via FortiSIEM Agent
☐	(s) ISO 27001 A.17: Top Applications By Synthetic Transaction Response Time	System	Ranks the services by average synthetic transaction monitoring probe response times.
☐	(s) ISO 27001 A.17: Top Devices by Accumulated Network Ping Downtime During Business Hours	System	Ranks the devices by total network ping downtime during business hours (Mon-Friday 8am-5pm)

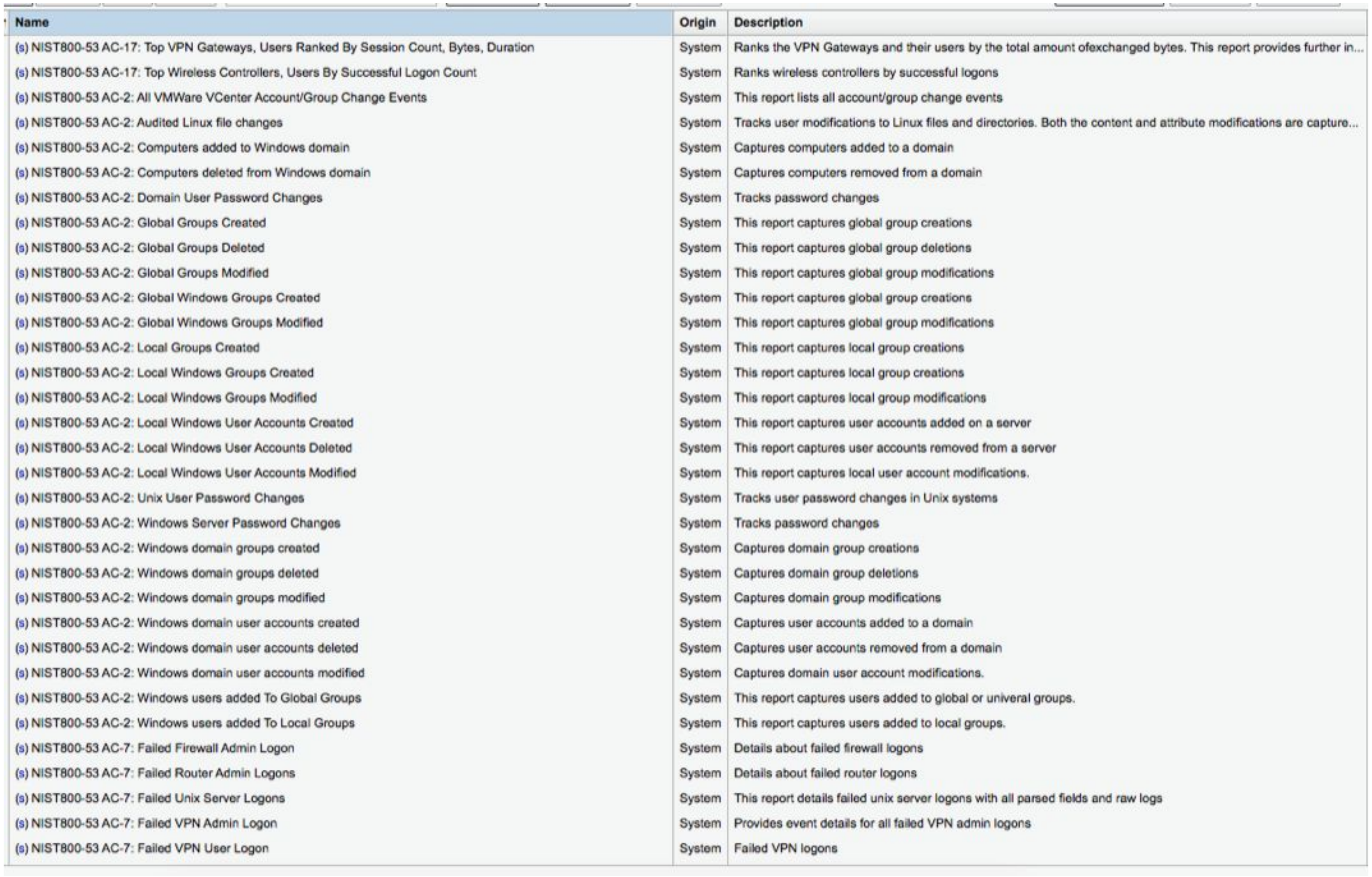
Tracks uncommon services permitted by firewalls - common services include DNS, SMTP, Web

StratoZen ISO 27001 Reports 3 of 3



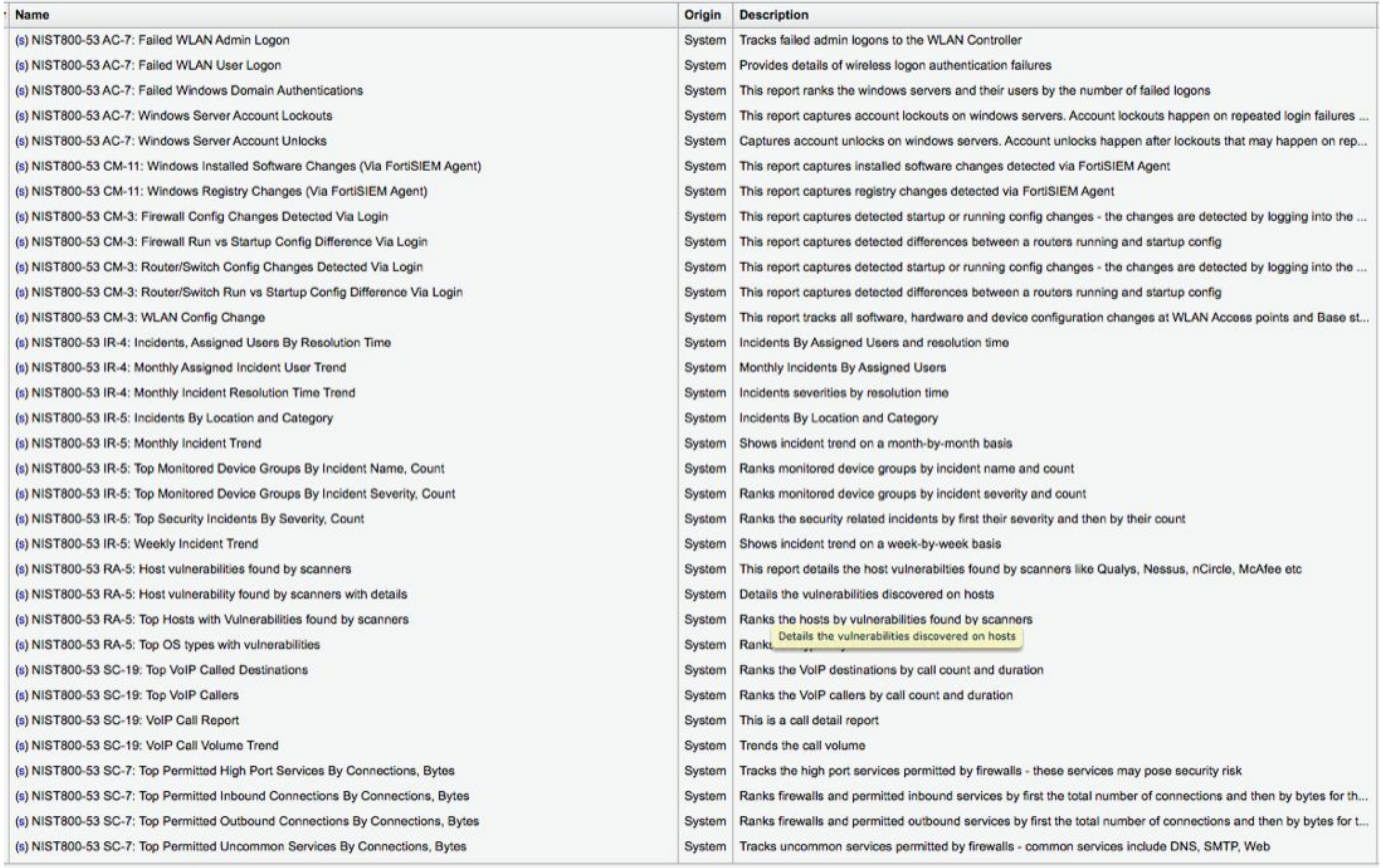
(s) ISO 27001 A.17: Top Devices by Accumulated Network Ping Downtime During Business Hours	System	Ranks the devices by total network ping downtime during business hours (Mon-Friday 8am-5pm)
(s) ISO 27001 A.17: Top Devices by Business Hours System Uptime Pct (Achieved System SLA)	System	Ranks the devices by system uptime pct over a time window - uptime calculated during business hours (M...
(s) ISO 27001 A.17: Top STMs by Business Hours Uptime Pct (Achieved Application SLA)	System	Ranks Synthetic transaction monitor tests (STM) by achieved uptime over a time window
(s) ISO 27001 A.8.1.1: CMDB Device Addition and Deletion History	System	Details the history of devices getting added and deleted from CMDB
(s) ISO 27001 A.8.1.1: CMDB Device Modification History	System	Details the history of device attribute changed in CMDB
(s) ISO 27001 A.9.4: Detailed Successful Login At ISO 27001 Device	System	Captures detailed successful logins at any device or application including servers, network devices, domai...
(s) ISO 27001 A.9.4: Domain Account Lock/Unlock history	System	Captures account lockouts and unlocks on domain accounts. Account lockouts happen on repeated login f...
(s) ISO 27001 A.9.4: Failed Unix Privilege Escalations	System	This report ranks the UNIX servers and their users by failed privilege escalations (su) count
(s) ISO 27001 A.9.4: Failed VPN Admin Logon	System	Provides event details for all failed VPN admin logons
(s) ISO 27001 A.9.4: Failed WLAN Admin Logon	System	Tracks failed admin logons to the WLAN Controller
(s) ISO 27001 A.9.4: Firewall Admin Activity Details	System	Provides details about firewall admin activity - logons, command executions and logoff
(s) ISO 27001 A.9.4: Privileged Windows Server Logon Attempts using the Administrator Account	System	This report details prvileged logon attempts to a windows server using the Administrator account
(s) ISO 27001 A.9.4: Remote Desktop Connections to Windows Servers	System	This report details successful and failed remote desktop connections
(s) ISO 27001 A.9.4: Router Admin Activity Details	System	Provides details about router admin activity - logons, command executions and logoff
(s) ISO 27001 A.9.4: Successful Unix Privilege Escalations	System	This report ranks the UNIX servers and their users by successful privilege escalations (su) count
(s) ISO 27001 A.9.4: Unix Server Privileged Command Execution	System	This report details privilege command execuations (sudo) at a Unix server
(s) ISO 27001 A.9.4: Unix Server Privileged Logon	System	This report details UNIX server privileged logon (su) details with all parsed parameters and raw logs
(s) ISO 27001 A.9.4: Windows Domain Account Lockouts	System	This report details windows domain account lockouts
(s) ISO 27001 A.9.4: Windows Server Account Lock/Unlock history	System	Captures account lockouts and unlocks on windows servers. Account lockouts happen on repeated login fa...
(s) ISO 27001 A.9.4: Windows Server Account Lockouts	System	This report captures account lockouts on windows servers. Account lockouts happen on repeated login fail...

StratoZen NIST 800-53 Reports 1 of 3



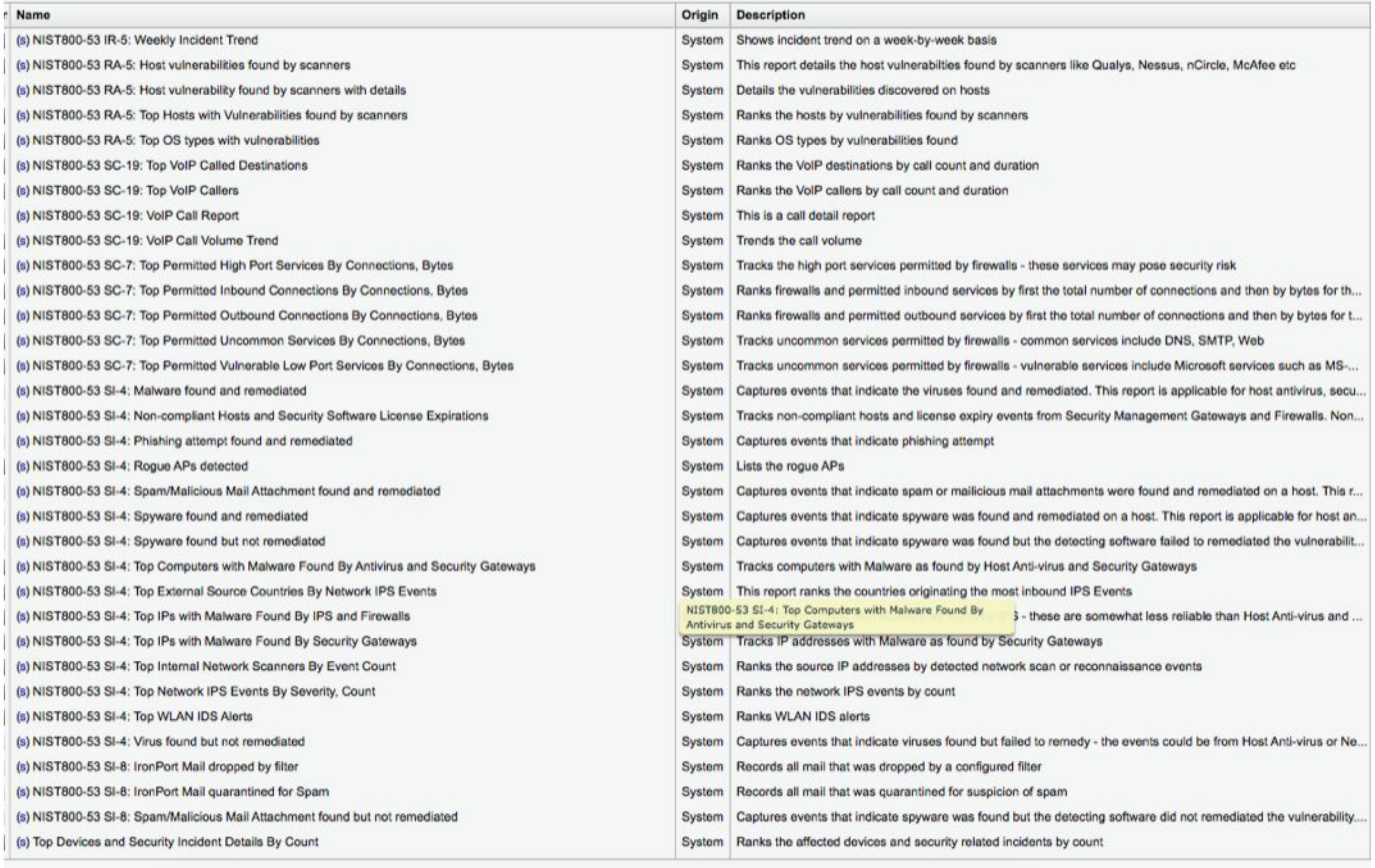
Name	Origin	Description
(s) NIST800-53 AC-17: Top VPN Gateways, Users Ranked By Session Count, Bytes, Duration	System	Ranks the VPN Gateways and their users by the total amount ofexchanged bytes. This report provides further in...
(s) NIST800-53 AC-17: Top Wireless Controllers, Users By Successful Logon Count	System	Ranks wireless controllers by successful logons
(s) NIST800-53 AC-2: All VMWare VCenter Account/Group Change Events	System	This report lists all account/group change events
(s) NIST800-53 AC-2: Audited Linux file changes	System	Tracks user modifications to Linux files and directories. Both the content and attribute modifications are capture...
(s) NIST800-53 AC-2: Computers added to Windows domain	System	Captures computers added to a domain
(s) NIST800-53 AC-2: Computers deleted from Windows domain	System	Captures computers removed from a domain
(s) NIST800-53 AC-2: Domain User Password Changes	System	Tracks password changes
(s) NIST800-53 AC-2: Global Groups Created	System	This report captures global group creations
(s) NIST800-53 AC-2: Global Groups Deleted	System	This report captures global group deletions
(s) NIST800-53 AC-2: Global Groups Modified	System	This report captures global group modifications
(s) NIST800-53 AC-2: Global Windows Groups Created	System	This report captures global group creations
(s) NIST800-53 AC-2: Global Windows Groups Modified	System	This report captures global group modifications
(s) NIST800-53 AC-2: Local Groups Created	System	This report captures local group creations
(s) NIST800-53 AC-2: Local Windows Groups Created	System	This report captures local group creations
(s) NIST800-53 AC-2: Local Windows Groups Modified	System	This report captures local group modifications
(s) NIST800-53 AC-2: Local Windows User Accounts Created	System	This report captures user accounts added on a server
(s) NIST800-53 AC-2: Local Windows User Accounts Deleted	System	This report captures user accounts removed from a server
(s) NIST800-53 AC-2: Local Windows User Accounts Modified	System	This report captures local user account modifications.
(s) NIST800-53 AC-2: Unix User Password Changes	System	Tracks user password changes in Unix systems
(s) NIST800-53 AC-2: Windows Server Password Changes	System	Tracks password changes
(s) NIST800-53 AC-2: Windows domain groups created	System	Captures domain group creations
(s) NIST800-53 AC-2: Windows domain groups deleted	System	Captures domain group deletions
(s) NIST800-53 AC-2: Windows domain groups modified	System	Captures domain group modifications
(s) NIST800-53 AC-2: Windows domain user accounts created	System	Captures user accounts added to a domain
(s) NIST800-53 AC-2: Windows domain user accounts deleted	System	Captures user accounts removed from a domain
(s) NIST800-53 AC-2: Windows domain user accounts modified	System	Captures domain user account modifications.
(s) NIST800-53 AC-2: Windows users added To Global Groups	System	This report captures users added to global or univeral groups.
(s) NIST800-53 AC-2: Windows users added To Local Groups	System	This report captures users added to local groups.
(s) NIST800-53 AC-7: Failed Firewall Admin Logon	System	Details about failed firewall logons
(s) NIST800-53 AC-7: Failed Router Admin Logons	System	Details about failed router logons
(s) NIST800-53 AC-7: Failed Unix Server Logons	System	This report details failed unix server logons with all parsed fields and raw logs
(s) NIST800-53 AC-7: Failed VPN Admin Logon	System	Provides event details for all failed VPN admin logons
(s) NIST800-53 AC-7: Failed VPN User Logon	System	Failed VPN logons

StratoZen NIST 800-53 Reports 2 of 3



Name	Origin	Description
(s) NIST800-53 AC-7: Failed WLAN Admin Logon	System	Tracks failed admin logons to the WLAN Controller
(s) NIST800-53 AC-7: Failed WLAN User Logon	System	Provides details of wireless logon authentication failures
(s) NIST800-53 AC-7: Failed Windows Domain Authentications	System	This report ranks the windows servers and their users by the number of failed logons
(s) NIST800-53 AC-7: Windows Server Account Lockouts	System	This report captures account lockouts on windows servers. Account lockouts happen on repeated login failures ...
(s) NIST800-53 AC-7: Windows Server Account Unlocks	System	Captures account unlocks on windows servers. Account unlocks happen after lockouts that may happen on rep...
(s) NIST800-53 CM-11: Windows Installed Software Changes (Via FortiSIEM Agent)	System	This report captures installed software changes detected via FortiSIEM Agent
(s) NIST800-53 CM-11: Windows Registry Changes (Via FortiSIEM Agent)	System	This report captures registry changes detected via FortiSIEM Agent
(s) NIST800-53 CM-3: Firewall Config Changes Detected Via Login	System	This report captures detected startup or running config changes - the changes are detected by logging into the ...
(s) NIST800-53 CM-3: Firewall Run vs Startup Config Difference Via Login	System	This report captures detected differences between a routers running and startup config
(s) NIST800-53 CM-3: Router/Switch Config Changes Detected Via Login	System	This report captures detected startup or running config changes - the changes are detected by logging into the ...
(s) NIST800-53 CM-3: Router/Switch Run vs Startup Config Difference Via Login	System	This report captures detected differences between a routers running and startup config
(s) NIST800-53 CM-3: WLAN Config Change	System	This report tracks all software, hardware and device configuration changes at WLAN Access points and Base st...
(s) NIST800-53 IR-4: Incidents, Assigned Users By Resolution Time	System	Incidents By Assigned Users and resolution time
(s) NIST800-53 IR-4: Monthly Assigned Incident User Trend	System	Monthly Incidents By Assigned Users
(s) NIST800-53 IR-4: Monthly Incident Resolution Time Trend	System	Incidents severities by resolution time
(s) NIST800-53 IR-5: Incidents By Location and Category	System	Incidents By Location and Category
(s) NIST800-53 IR-5: Monthly Incident Trend	System	Shows incident trend on a month-by-month basis
(s) NIST800-53 IR-5: Top Monitored Device Groups By Incident Name, Count	System	Ranks monitored device groups by incident name and count
(s) NIST800-53 IR-5: Top Monitored Device Groups By Incident Severity, Count	System	Ranks monitored device groups by incident severity and count
(s) NIST800-53 IR-5: Top Security Incidents By Severity, Count	System	Ranks the security related incidents by first their severity and then by their count
(s) NIST800-53 IR-5: Weekly Incident Trend	System	Shows incident trend on a week-by-week basis
(s) NIST800-53 RA-5: Host vulnerabilities found by scanners	System	This report details the host vulnerabilties found by scanners like Qualys, Nessus, nCircle, McAfee etc
(s) NIST800-53 RA-5: Host vulnerability found by scanners with details	System	Details the vulnerabilities discovered on hosts
(s) NIST800-53 RA-5: Top Hosts with Vulnerabilities found by scanners	System	Ranks the hosts by vulnerabilities found by scanners
(s) NIST800-53 RA-5: Top OS types with vulnerabilities	System	Ranks Details the vulnerabilities discovered on hosts
(s) NIST800-53 SC-19: Top VoIP Called Destinations	System	Ranks the VoIP destinations by call count and duration
(s) NIST800-53 SC-19: Top VoIP Callers	System	Ranks the VoIP callers by call count and duration
(s) NIST800-53 SC-19: VoIP Call Report	System	This is a call detail report
(s) NIST800-53 SC-19: VoIP Call Volume Trend	System	Trends the call volume
(s) NIST800-53 SC-7: Top Permitted High Port Services By Connections, Bytes	System	Tracks the high port services permitted by firewalls - these services may pose security risk
(s) NIST800-53 SC-7: Top Permitted Inbound Connections By Connections, Bytes	System	Ranks firewalls and permitted inbound services by first the total number of connections and then by bytes for th...
(s) NIST800-53 SC-7: Top Permitted Outbound Connections By Connections, Bytes	System	Ranks firewalls and permitted outbound services by first the total number of connections and then by bytes for t...
(s) NIST800-53 SC-7: Top Permitted Uncommon Services By Connections, Bytes	System	Tracks uncommon services permitted by firewalls - common services include DNS, SMTP, Web

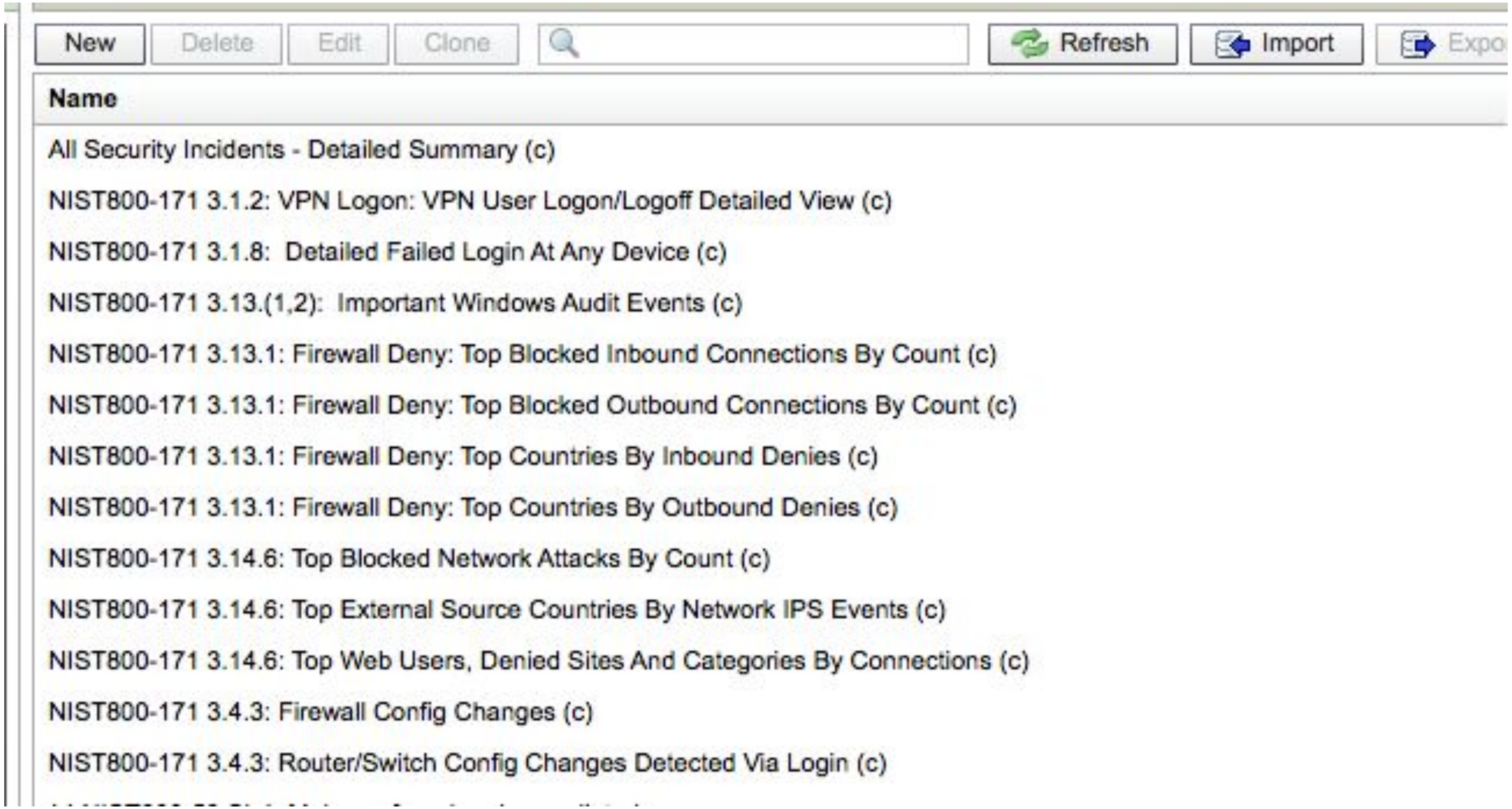
StratoZen NIST 800-53 Reports 3 of 3



Name	Origin	Description
(s) NIST800-53 IR-5: Weekly Incident Trend	System	Shows incident trend on a week-by-week basis
(s) NIST800-53 RA-5: Host vulnerabilities found by scanners	System	This report details the host vulnerabilties found by scanners like Qualys, Nessus, nCircle, McAfee etc
(s) NIST800-53 RA-5: Host vulnerability found by scanners with details	System	Details the vulnerabilities discovered on hosts
(s) NIST800-53 RA-5: Top Hosts with Vulnerabilities found by scanners	System	Ranks the hosts by vulnerabilities found by scanners
(s) NIST800-53 RA-5: Top OS types with vulnerabilities	System	Ranks OS types by vulnerabilities found
(s) NIST800-53 SC-19: Top VoIP Called Destinations	System	Ranks the VoIP destinations by call count and duration
(s) NIST800-53 SC-19: Top VoIP Callers	System	Ranks the VoIP callers by call count and duration
(s) NIST800-53 SC-19: VoIP Call Report	System	This is a call detail report
(s) NIST800-53 SC-19: VoIP Call Volume Trend	System	Trends the call volume
(s) NIST800-53 SC-7: Top Permitted High Port Services By Connections, Bytes	System	Tracks the high port services permitted by firewalls - these services may pose security risk
(s) NIST800-53 SC-7: Top Permitted Inbound Connections By Connections, Bytes	System	Ranks firewalls and permitted inbound services by first the total number of connections and then by bytes for th...
(s) NIST800-53 SC-7: Top Permitted Outbound Connections By Connections, Bytes	System	Ranks firewalls and permitted outbound services by first the total number of connections and then by bytes for t...
(s) NIST800-53 SC-7: Top Permitted Uncommon Services By Connections, Bytes	System	Tracks uncommon services permitted by firewalls - common services include DNS, SMTP, Web
(s) NIST800-53 SC-7: Top Permitted Vulnerable Low Port Services By Connections, Bytes	System	Tracks uncommon services permitted by firewalls - vulnerable services include Microsoft services such as MS-...
(s) NIST800-53 SI-4: Malware found and remediated	System	Captures events that indicate the viruses found and remediated. This report is applicable for host antivirus, secu...
(s) NIST800-53 SI-4: Non-compliant Hosts and Security Software License Expirations	System	Tracks non-compliant hosts and license expiry events from Security Management Gateways and Firewalls. Non...
(s) NIST800-53 SI-4: Phishing attempt found and remediated	System	Captures events that indicate phishing attempt
(s) NIST800-53 SI-4: Rogue APs detected	System	Lists the rogue APs
(s) NIST800-53 SI-4: Spam/Malicious Mail Attachment found and remediated	System	Captures events that indicate spam or mailicious mail attachments were found and remediated on a host. This r...
(s) NIST800-53 SI-4: Spyware found and remediated	System	Captures events that indicate spyware was found and remediated on a host. This report is applicable for host an...
(s) NIST800-53 SI-4: Spyware found but not remediated	System	Captures events that indicate spyware was found but the detecting software failed to remediated the vulnerabilit...
(s) NIST800-53 SI-4: Top Computers with Malware Found By Antivirus and Security Gateways	System	Tracks computers with Malware as found by Host Anti-virus and Security Gateways
(s) NIST800-53 SI-4: Top External Source Countries By Network IPS Events	System	This report ranks the countries originating the most inbound IPS Events
(s) NIST800-53 SI-4: Top IPs with Malware Found By IPS and Firewalls		S - these are somewhat less reliable than Host Anti-virus and ...
(s) NIST800-53 SI-4: Top IPs with Malware Found By Security Gateways	System	Tracks IP addresses with Malware as found by Security Gateways
(s) NIST800-53 SI-4: Top Internal Network Scanners By Event Count	System	Ranks the source IP addresses by detected network scan or reconnaissance events
(s) NIST800-53 SI-4: Top Network IPS Events By Severity, Count	System	Ranks the network IPS events by count
(s) NIST800-53 SI-4: Top WLAN IDS Alerts	System	Ranks WLAN IDS alerts
(s) NIST800-53 SI-4: Virus found but not remediated	System	Captures events that indicate viruses found but failed to remedy - the events could be from Host Anti-virus or Ne...
(s) NIST800-53 SI-8: IronPort Mail dropped by filter	System	Records all mail that was dropped by a configured filter
(s) NIST800-53 SI-8: IronPort Mail quarantined for Spam	System	Records all mail that was quarantined for suspicion of spam
(s) NIST800-53 SI-8: Spam/Malicious Mail Attachment found but not remediated	System	Captures events that indicate spyware was found but the detecting software did not remediated the vulnerability....
(s) Top Devices and Security Incident Details By Count	System	Ranks the affected devices and security related incidents by count

NIST800-53 SI-4: Top Computers with Malware Found By Antivirus and Security Gateways

StratoZen NIST 800-171 Reports 1 of 1



Name

All Security Incidents - Detailed Summary (c)

NIST800-171 3.1.2: VPN Logon: VPN User Logon/Logoff Detailed View (c)

NIST800-171 3.1.8: Detailed Failed Login At Any Device (c)

NIST800-171 3.13.(1,2): Important Windows Audit Events (c)

NIST800-171 3.13.1: Firewall Deny: Top Blocked Inbound Connections By Count (c)

NIST800-171 3.13.1: Firewall Deny: Top Blocked Outbound Connections By Count (c)

NIST800-171 3.13.1: Firewall Deny: Top Countries By Inbound Denies (c)

NIST800-171 3.13.1: Firewall Deny: Top Countries By Outbound Denies (c)

NIST800-171 3.14.6: Top Blocked Network Attacks By Count (c)

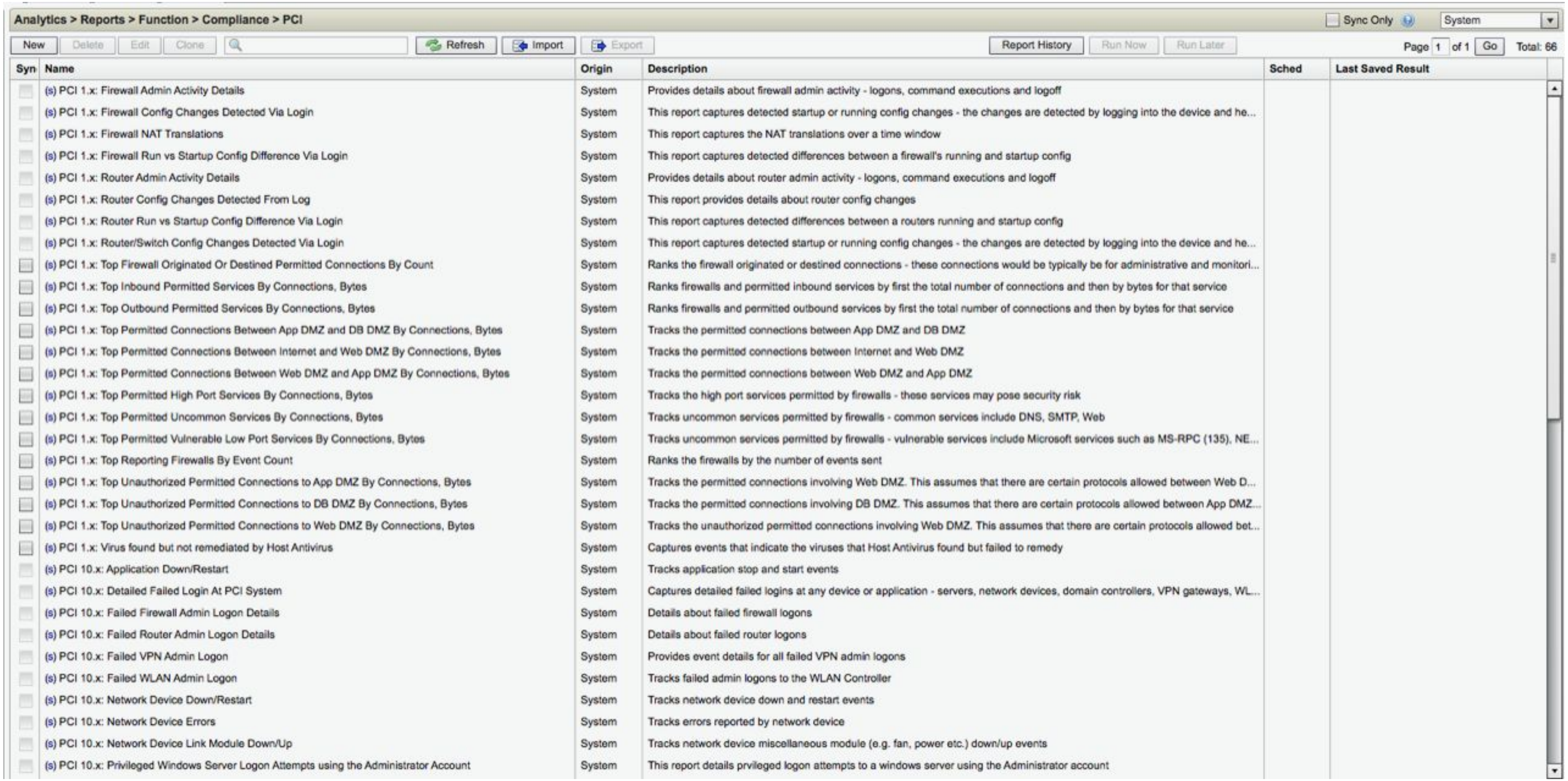
NIST800-171 3.14.6: Top External Source Countries By Network IPS Events (c)

NIST800-171 3.14.6: Top Web Users, Denied Sites And Categories By Connections (c)

NIST800-171 3.4.3: Firewall Config Changes (c)

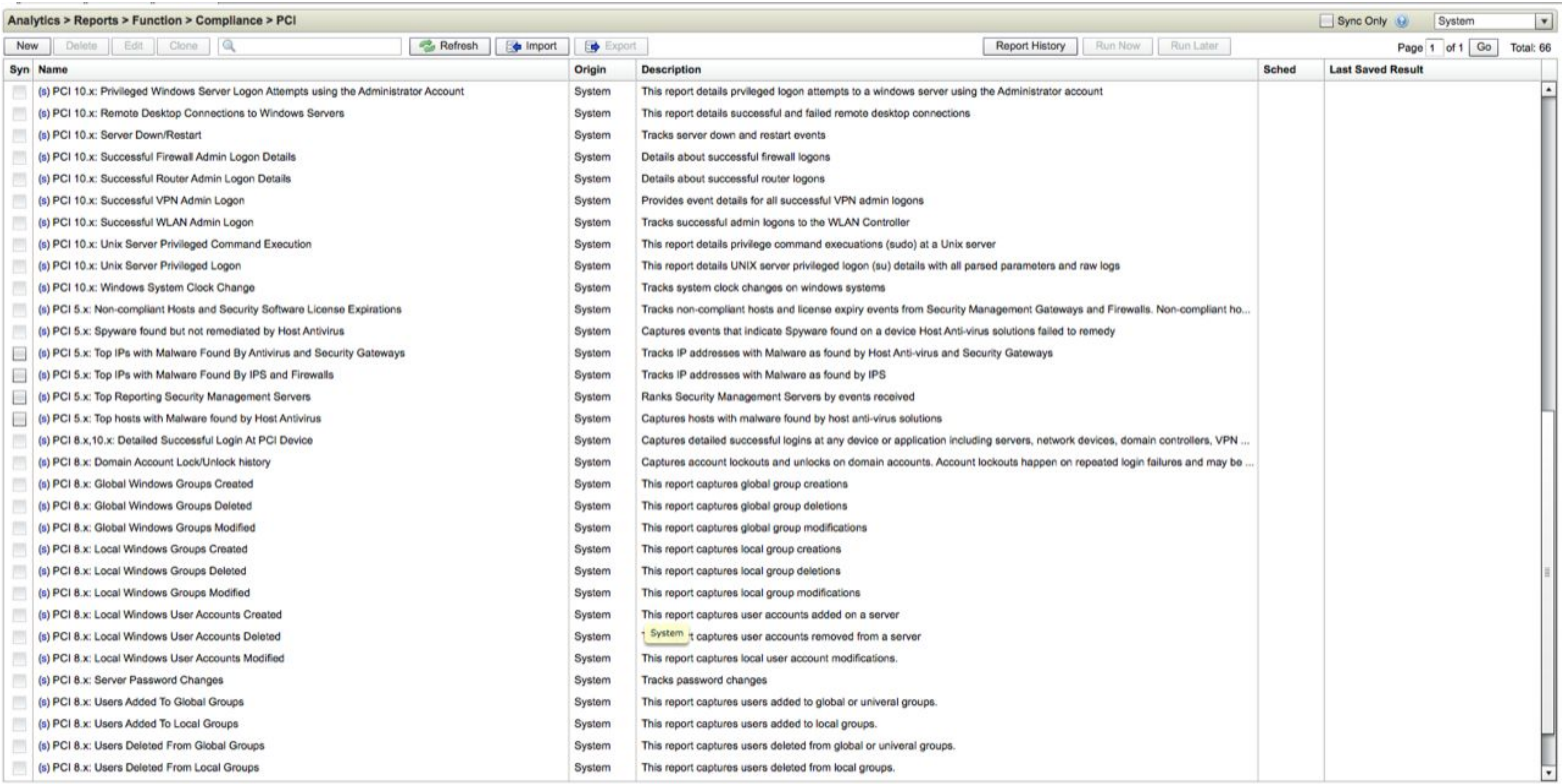
NIST800-171 3.4.3: Router/Switch Config Changes Detected Via Login (c)

StratoZen PCI Reports 1 of 2



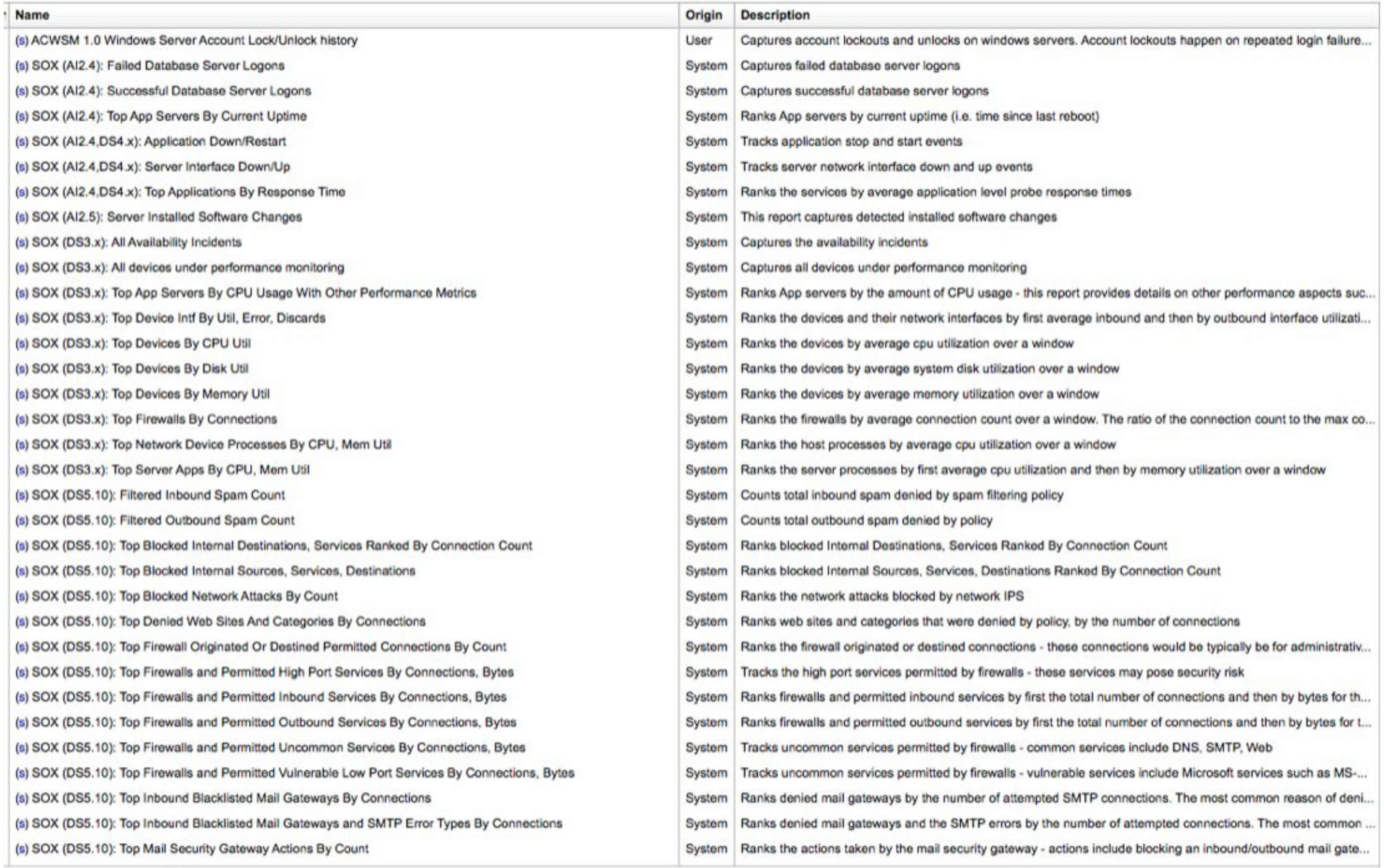
Syn	Name	Origin	Description	Sched	Last Saved Result
☐	(s) PCI 1.x: Firewall Admin Activity Details	System	Provides details about firewall admin activity - logons, command executions and logoff		
☐	(s) PCI 1.x: Firewall Config Changes Detected Via Login	System	This report captures detected startup or running config changes - the changes are detected by logging into the device and he...		
☐	(s) PCI 1.x: Firewall NAT Translations	System	This report captures the NAT translations over a time window		
☐	(s) PCI 1.x: Firewall Run vs Startup Config Difference Via Login	System	This report captures detected differences between a firewall's running and startup config		
☐	(s) PCI 1.x: Router Admin Activity Details	System	Provides details about router admin activity - logons, command executions and logoff		
☐	(s) PCI 1.x: Router Config Changes Detected From Log	System	This report provides details about router config changes		
☐	(s) PCI 1.x: Router Run vs Startup Config Difference Via Login	System	This report captures detected differences between a routers running and startup config		
☐	(s) PCI 1.x: Router/Switch Config Changes Detected Via Login	System	This report captures detected startup or running config changes - the changes are detected by logging into the device and he...		
☐	(s) PCI 1.x: Top Firewall Originated Or Destined Permitted Connections By Count	System	Ranks the firewall originated or destined connections - these connections would be typically be for administrative and monitori...		
☐	(s) PCI 1.x: Top Inbound Permitted Services By Connections, Bytes	System	Ranks firewalls and permitted inbound services by first the total number of connections and then by bytes for that service		
☐	(s) PCI 1.x: Top Outbound Permitted Services By Connections, Bytes	System	Ranks firewalls and permitted outbound services by first the total number of connections and then by bytes for that service		
☐	(s) PCI 1.x: Top Permitted Connections Between App DMZ and DB DMZ By Connections, Bytes	System	Tracks the permitted connections between App DMZ and DB DMZ		
☐	(s) PCI 1.x: Top Permitted Connections Between Internet and Web DMZ By Connections, Bytes	System	Tracks the permitted connections between Internet and Web DMZ		
☐	(s) PCI 1.x: Top Permitted Connections Between Web DMZ and App DMZ By Connections, Bytes	System	Tracks the permitted connections between Web DMZ and App DMZ		
☐	(s) PCI 1.x: Top Permitted High Port Services By Connections, Bytes	System	Tracks the high port services permitted by firewalls - these services may pose security risk		
☐	(s) PCI 1.x: Top Permitted Uncommon Services By Connections, Bytes	System	Tracks uncommon services permitted by firewalls - common services include DNS, SMTP, Web		
☐	(s) PCI 1.x: Top Permitted Vulnerable Low Port Services By Connections, Bytes	System	Tracks uncommon services permitted by firewalls - vulnerable services include Microsoft services such as MS-RPC (135), NE...		
☐	(s) PCI 1.x: Top Reporting Firewalls By Event Count	System	Ranks the firewalls by the number of events sent		
☐	(s) PCI 1.x: Top Unauthorized Permitted Connections to App DMZ By Connections, Bytes	System	Tracks the permitted connections involving Web DMZ. This assumes that there are certain protocols allowed between Web D...		
☐	(s) PCI 1.x: Top Unauthorized Permitted Connections to DB DMZ By Connections, Bytes	System	Tracks the permitted connections involving DB DMZ. This assumes that there are certain protocols allowed between App DMZ...		
☐	(s) PCI 1.x: Top Unauthorized Permitted Connections to Web DMZ By Connections, Bytes	System	Tracks the unauthorized permitted connections involving Web DMZ. This assumes that there are certain protocols allowed bet...		
☐	(s) PCI 1.x: Virus found but not remediated by Host Antivirus	System	Captures events that indicate the viruses that Host Antivirus found but failed to remedy		
☐	(s) PCI 10.x: Application Down/Restart	System	Tracks application stop and start events		
☐	(s) PCI 10.x: Detailed Failed Login At PCI System	System	Captures detailed failed logins at any device or application - servers, network devices, domain controllers, VPN gateways, WL...		
☐	(s) PCI 10.x: Failed Firewall Admin Logon Details	System	Details about failed firewall logons		
☐	(s) PCI 10.x: Failed Router Admin Logon Details	System	Details about failed router logons		
☐	(s) PCI 10.x: Failed VPN Admin Logon	System	Provides event details for all failed VPN admin logons		
☐	(s) PCI 10.x: Failed WLAN Admin Logon	System	Tracks failed admin logons to the WLAN Controller		
☐	(s) PCI 10.x: Network Device Down/Restart	System	Tracks network device down and restart events		
☐	(s) PCI 10.x: Network Device Errors	System	Tracks errors reported by network device		
☐	(s) PCI 10.x: Network Device Link Module Down/Up	System	Tracks network device miscellaneous module (e.g. fan, power etc.) down/up events		
☐	(s) PCI 10.x: Privileged Windows Server Logon Attempts using the Administrator Account	System	This report details prvileged logon attempts to a windows server using the Administrator account		

StratoZen PCI Reports 2 of 2



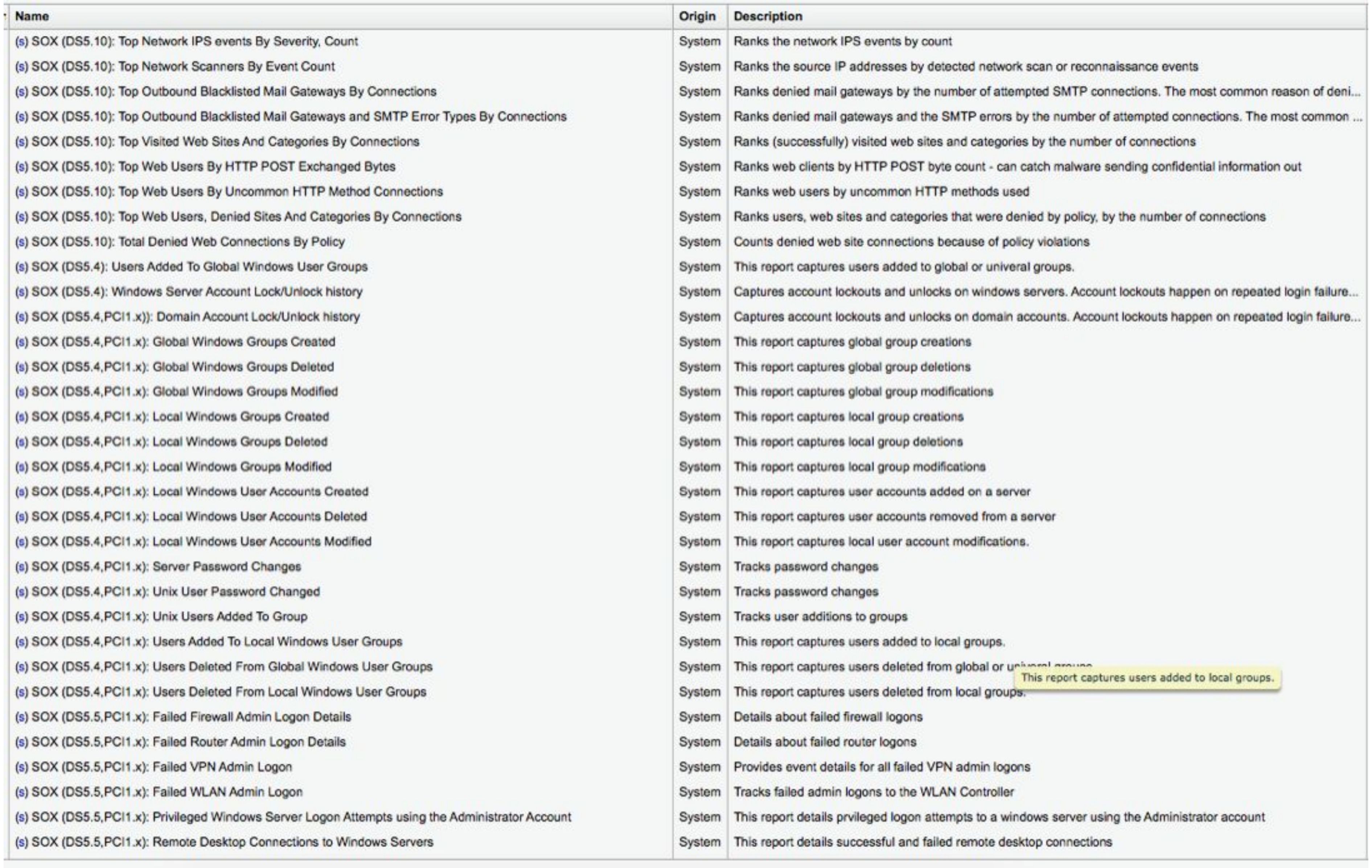
Syn	Name	Origin	Description	Sched	Last Saved Result
□	(s) PCI 10.x: Privileged Windows Server Logon Attempts using the Administrator Account	System	This report details prvileged logon attempts to a windows server using the Administrator account		
□	(s) PCI 10.x: Remote Desktop Connections to Windows Servers	System	This report details successful and failed remote desktop connections		
□	(s) PCI 10.x: Server Down/Restart	System	Tracks server down and restart events		
□	(s) PCI 10.x: Successful Firewall Admin Logon Details	System	Details about successful firewall logons		
□	(s) PCI 10.x: Successful Router Admin Logon Details	System	Details about successful router logons		
□	(s) PCI 10.x: Successful VPN Admin Logon	System	Provides event details for all successful VPN admin logons		
□	(s) PCI 10.x: Successful WLAN Admin Logon	System	Tracks successful admin logons to the WLAN Controller		
□	(s) PCI 10.x: Unix Server Privileged Command Execution	System	This report details privilege command executions (sudo) at a Unix server		
□	(s) PCI 10.x: Unix Server Privileged Logon	System	This report details UNIX server privileged logon (su) details with all parsed parameters and raw logs		
□	(s) PCI 10.x: Windows System Clock Change	System	Tracks system clock changes on windows systems		
□	(s) PCI 5.x: Non-compliant Hosts and Security Software License Expirations	System	Tracks non-compliant hosts and license expiry events from Security Management Gateways and Firewalls. Non-compliant ho...		
□	(s) PCI 5.x: Spyware found but not remediated by Host Antivirus	System	Captures events that indicate Spyware found on a device Host Anti-virus solutions failed to remedy		
□	(s) PCI 5.x: Top IPs with Malware Found By Antivirus and Security Gateways	System	Tracks IP addresses with Malware as found by Host Anti-virus and Security Gateways		
□	(s) PCI 5.x: Top IPs with Malware Found By IPS and Firewalls	System	Tracks IP addresses with Malware as found by IPS		
□	(s) PCI 5.x: Top Reporting Security Management Servers	System	Ranks Security Management Servers by events received		
□	(s) PCI 5.x: Top hosts with Malware found by Host Antivirus	System	Captures hosts with malware found by host anti-virus solutions		
□	(s) PCI 8.x,10.x: Detailed Successful Login At PCI Device	System	Captures detailed successful logins at any device or application including servers, network devices, domain controllers, VPN ...		
□	(s) PCI 8.x: Domain Account Lock/Unlock history	System	Captures account lockouts and unlocks on domain accounts. Account lockouts happen on repeated login failures and may be ...		
□	(s) PCI 8.x: Global Windows Groups Created	System	This report captures global group creations		
□	(s) PCI 8.x: Global Windows Groups Deleted	System	This report captures global group deletions		
□	(s) PCI 8.x: Global Windows Groups Modified	System	This report captures global group modifications		
□	(s) PCI 8.x: Local Windows Groups Created	System	This report captures local group creations		
□	(s) PCI 8.x: Local Windows Groups Deleted	System	This report captures local group deletions		
□	(s) PCI 8.x: Local Windows Groups Modified	System	This report captures local group modifications		
□	(s) PCI 8.x: Local Windows User Accounts Created	System	This report captures user accounts added on a server		
□	(s) PCI 8.x: Local Windows User Accounts Deleted	System	T t captures user accounts removed from a server		
□	(s) PCI 8.x: Local Windows User Accounts Modified	System	This report captures local user account modifications.		
□	(s) PCI 8.x: Server Password Changes	System	Tracks password changes		
□	(s) PCI 8.x: Users Added To Global Groups	System	This report captures users added to global or univeral groups.		
□	(s) PCI 8.x: Users Added To Local Groups	System	This report captures users added to local groups.		
□	(s) PCI 8.x: Users Deleted From Global Groups	System	This report captures users deleted from global or univeral groups.		
□	(s) PCI 8.x: Users Deleted From Local Groups	System	This report captures users deleted from local groups.		

StratoZen SOX Reports - 1 of 3



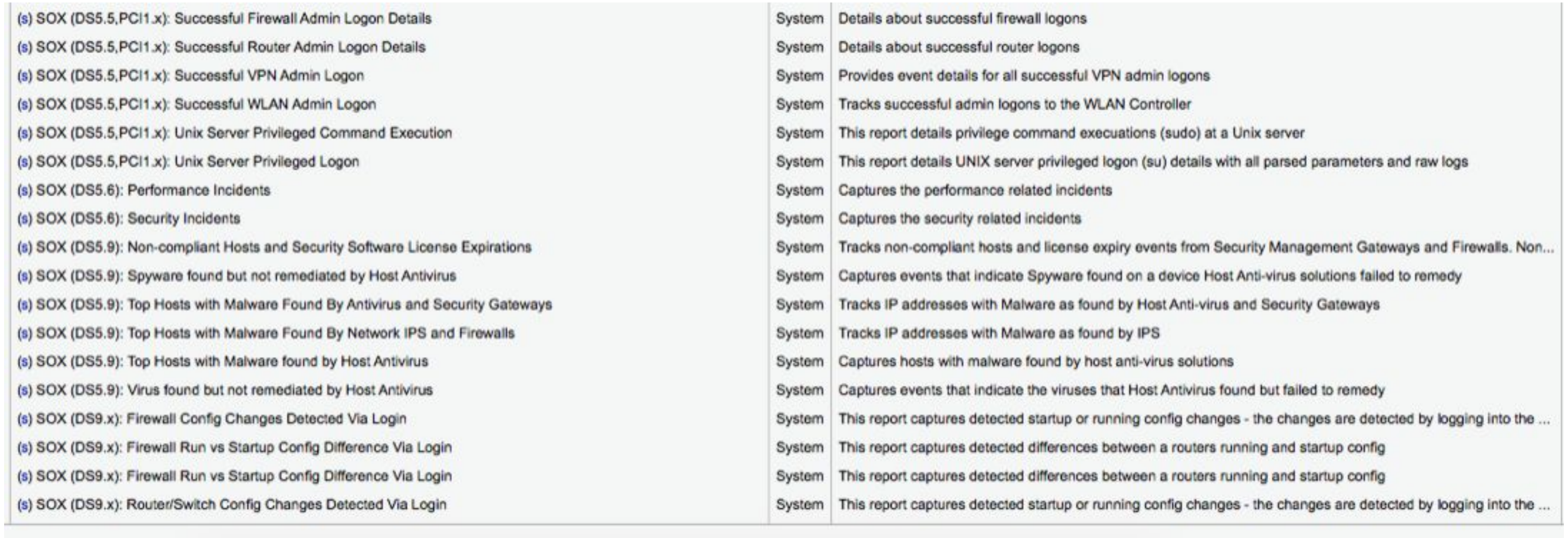
Name	Origin	Description
(s) ACWSM 1.0 Windows Server Account Lock/Unlock history	User	Captures account lockouts and unlocks on windows servers. Account lockouts happen on repeated login failure...
(s) SOX (AI2.4): Failed Database Server Logons	System	Captures failed database server logons
(s) SOX (AI2.4): Successful Database Server Logons	System	Captures successful database server logons
(s) SOX (AI2.4): Top App Servers By Current Uptime	System	Ranks App servers by current uptime (i.e. time since last reboot)
(s) SOX (AI2.4,DS4.x): Application Down/Restart	System	Tracks application stop and start events
(s) SOX (AI2.4,DS4.x): Server Interface Down/Up	System	Tracks server network interface down and up events
(s) SOX (AI2.4,DS4.x): Top Applications By Response Time	System	Ranks the services by average application level probe response times
(s) SOX (AI2.5): Server Installed Software Changes	System	This report captures detected installed software changes
(s) SOX (DS3.x): All Availability Incidents	System	Captures the availability incidents
(s) SOX (DS3.x): All devices under performance monitoring	System	Captures all devices under performance monitoring
(s) SOX (DS3.x): Top App Servers By CPU Usage With Other Performance Metrics	System	Ranks App servers by the amount of CPU usage - this report provides details on other performance aspects suc...
(s) SOX (DS3.x): Top Device Intf By Util, Error, Discards	System	Ranks the devices and their network interfaces by first average inbound and then by outbound interface utilizati...
(s) SOX (DS3.x): Top Devices By CPU Util	System	Ranks the devices by average cpu utilization over a window
(s) SOX (DS3.x): Top Devices By Disk Util	System	Ranks the devices by average system disk utilization over a window
(s) SOX (DS3.x): Top Devices By Memory Util	System	Ranks the devices by average memory utilization over a window
(s) SOX (DS3.x): Top Firewalls By Connections	System	Ranks the firewalls by average connection count over a window. The ratio of the connection count to the max co...
(s) SOX (DS3.x): Top Network Device Processes By CPU, Mem Util	System	Ranks the host processes by average cpu utilization over a window
(s) SOX (DS3.x): Top Server Apps By CPU, Mem Util	System	Ranks the server processes by first average cpu utilization and then by memory utilization over a window
(s) SOX (DS5.10): Filtered Inbound Spam Count	System	Counts total inbound spam denied by spam filtering policy
(s) SOX (DS5.10): Filtered Outbound Spam Count	System	Counts total outbound spam denied by policy
(s) SOX (DS5.10): Top Blocked Internal Destinations, Services Ranked By Connection Count	System	Ranks blocked Internal Destinations, Services Ranked By Connection Count
(s) SOX (DS5.10): Top Blocked Internal Sources, Services, Destinations	System	Ranks blocked Internal Sources, Services, Destinations Ranked By Connection Count
(s) SOX (DS5.10): Top Blocked Network Attacks By Count	System	Ranks the network attacks blocked by network IPS
(s) SOX (DS5.10): Top Denied Web Sites And Categories By Connections	System	Ranks web sites and categories that were denied by policy, by the number of connections
(s) SOX (DS5.10): Top Firewall Originated Or Destined Permitted Connections By Count	System	Ranks the firewall originated or destined connections - these connections would be typically be for administrativ...
(s) SOX (DS5.10): Top Firewalls and Permitted High Port Services By Connections, Bytes	System	Tracks the high port services permitted by firewalls - these services may pose security risk
(s) SOX (DS5.10): Top Firewalls and Permitted Inbound Services By Connections, Bytes	System	Ranks firewalls and permitted inbound services by first the total number of connections and then by bytes for th...
(s) SOX (DS5.10): Top Firewalls and Permitted Outbound Services By Connections, Bytes	System	Ranks firewalls and permitted outbound services by first the total number of connections and then by bytes for t...
(s) SOX (DS5.10): Top Firewalls and Permitted Uncommon Services By Connections, Bytes	System	Tracks uncommon services permitted by firewalls - common services include DNS, SMTP, Web
(s) SOX (DS5.10): Top Firewalls and Permitted Vulnerable Low Port Services By Connections, Bytes	System	Tracks uncommon services permitted by firewalls - vulnerable services include Microsoft services such as MS-...
(s) SOX (DS5.10): Top Inbound Blacklisted Mail Gateways By Connections	System	Ranks denied mail gateways by the number of attempted SMTP connections. The most common reason of deni...
(s) SOX (DS5.10): Top Inbound Blacklisted Mail Gateways and SMTP Error Types By Connections	System	Ranks denied mail gateways and the SMTP errors by the number of attempted connections. The most common ...
(s) SOX (DS5.10): Top Mail Security Gateway Actions By Count	System	Ranks the actions taken by the mail security gateway - actions include blocking an inbound/outbound mail gate...

StratoZen SOX Reports 2 of 3



Name	Origin	Description
(s) SOX (DS5.10): Top Network IPS events By Severity, Count	System	Ranks the network IPS events by count
(s) SOX (DS5.10): Top Network Scanners By Event Count	System	Ranks the source IP addresses by detected network scan or reconnaissance events
(s) SOX (DS5.10): Top Outbound Blacklisted Mail Gateways By Connections	System	Ranks denied mail gateways by the number of attempted SMTP connections. The most common reason of deni...
(s) SOX (DS5.10): Top Outbound Blacklisted Mail Gateways and SMTP Error Types By Connections	System	Ranks denied mail gateways and the SMTP errors by the number of attempted connections. The most common ...
(s) SOX (DS5.10): Top Visited Web Sites And Categories By Connections	System	Ranks (successfully) visited web sites and categories by the number of connections
(s) SOX (DS5.10): Top Web Users By HTTP POST Exchanged Bytes	System	Ranks web clients by HTTP POST byte count - can catch malware sending confidential information out
(s) SOX (DS5.10): Top Web Users By Uncommon HTTP Method Connections	System	Ranks web users by uncommon HTTP methods used
(s) SOX (DS5.10): Top Web Users, Denied Sites And Categories By Connections	System	Ranks users, web sites and categories that were denied by policy, by the number of connections
(s) SOX (DS5.10): Total Denied Web Connections By Policy	System	Counts denied web site connections because of policy violations
(s) SOX (DS5.4): Users Added To Global Windows User Groups	System	This report captures users added to global or univeral groups.
(s) SOX (DS5.4): Windows Server Account Lock/Unlock history	System	Captures account lockouts and unlocks on windows servers. Account lockouts happen on repeated login failure...
(s) SOX (DS5.4,PCI1.x)): Domain Account Lock/Unlock history	System	Captures account lockouts and unlocks on domain accounts. Account lockouts happen on repeated login failure...
(s) SOX (DS5.4,PCI1.x): Global Windows Groups Created	System	This report captures global group creations
(s) SOX (DS5.4,PCI1.x): Global Windows Groups Deleted	System	This report captures global group deletions
(s) SOX (DS5.4,PCI1.x): Global Windows Groups Modified	System	This report captures global group modifications
(s) SOX (DS5.4,PCI1.x): Local Windows Groups Created	System	This report captures local group creations
(s) SOX (DS5.4,PCI1.x): Local Windows Groups Deleted	System	This report captures local group deletions
(s) SOX (DS5.4,PCI1.x): Local Windows Groups Modified	System	This report captures local group modifications
(s) SOX (DS5.4,PCI1.x): Local Windows User Accounts Created	System	This report captures user accounts added on a server
(s) SOX (DS5.4,PCI1.x): Local Windows User Accounts Deleted	System	This report captures user accounts removed from a server
(s) SOX (DS5.4,PCI1.x): Local Windows User Accounts Modified	System	This report captures local user account modifications.
(s) SOX (DS5.4,PCI1.x): Server Password Changes	System	Tracks password changes
(s) SOX (DS5.4,PCI1.x): Unix User Password Changed	System	Tracks password changes
(s) SOX (DS5.4,PCI1.x): Unix Users Added To Group	System	Tracks user additions to groups
(s) SOX (DS5.4,PCI1.x): Users Added To Local Windows User Groups	System	This report captures users added to local groups.
(s) SOX (DS5.4,PCI1.x): Users Deleted From Global Windows User Groups	System	This report captures users deleted from global or univeral groups.
(s) SOX (DS5.4,PCI1.x): Users Deleted From Local Windows User Groups	System	This report captures users deleted from local groups.
(s) SOX (DS5.5,PCI1.x): Failed Firewall Admin Logon Details	System	Details about failed firewall logons
(s) SOX (DS5.5,PCI1.x): Failed Router Admin Logon Details	System	Details about failed router logons
(s) SOX (DS5.5,PCI1.x): Failed VPN Admin Logon	System	Provides event details for all failed VPN admin logons
(s) SOX (DS5.5,PCI1.x): Failed WLAN Admin Logon	System	Tracks failed admin logons to the WLAN Controller
(s) SOX (DS5.5,PCI1.x): Privileged Windows Server Logon Attempts using the Administrator Account	System	This report details prvileged logon attempts to a windows server using the Administrator account
(s) SOX (DS5.5,PCI1.x): Remote Desktop Connections to Windows Servers	System	This report details successful and failed remote desktop connections

StratoZen SOX Reports 3 of 3



(s) SOX (DS5.5,PCI1.x): Successful Firewall Admin Logon Details	System	Details about successful firewall logons
(s) SOX (DS5.5,PCI1.x): Successful Router Admin Logon Details	System	Details about successful router logons
(s) SOX (DS5.5,PCI1.x): Successful VPN Admin Logon	System	Provides event details for all successful VPN admin logons
(s) SOX (DS5.5,PCI1.x): Successful WLAN Admin Logon	System	Tracks successful admin logons to the WLAN Controller
(s) SOX (DS5.5,PCI1.x): Unix Server Privileged Command Execution	System	This report details privilege command execuations (sudo) at a Unix server
(s) SOX (DS5.5,PCI1.x): Unix Server Privileged Logon	System	This report details UNIX server privileged logon (su) details with all parsed parameters and raw logs
(s) SOX (DS5.6): Performance Incidents	System	Captures the performance related incidents
(s) SOX (DS5.6): Security Incidents	System	Captures the security related incidents
(s) SOX (DS5.9): Non-compliant Hosts and Security Software License Expirations	System	Tracks non-compliant hosts and license expiry events from Security Management Gateways and Firewalls. Non...
(s) SOX (DS5.9): Spyware found but not remediated by Host Antivirus	System	Captures events that indicate Spyware found on a device Host Anti-virus solutions failed to remedy
(s) SOX (DS5.9): Top Hosts with Malware Found By Antivirus and Security Gateways	System	Tracks IP addresses with Malware as found by Host Anti-virus and Security Gateways
(s) SOX (DS5.9): Top Hosts with Malware Found By Network IPS and Firewalls	System	Tracks IP addresses with Malware as found by IPS
(s) SOX (DS5.9): Top Hosts with Malware found by Host Antivirus	System	Captures hosts with malware found by host anti-virus solutions
(s) SOX (DS5.9): Virus found but not remediated by Host Antivirus	System	Captures events that indicate the viruses that Host Antivirus found but failed to remedy
(s) SOX (DS9.x): Firewall Config Changes Detected Via Login	System	This report captures detected startup or running config changes - the changes are detected by logging into the ...
(s) SOX (DS9.x): Firewall Run vs Startup Config Difference Via Login	System	This report captures detected differences between a routers running and startup config
(s) SOX (DS9.x): Firewall Run vs Startup Config Difference Via Login	System	This report captures detected differences between a routers running and startup config
(s) SOX (DS9.x): Router/Switch Config Changes Detected Via Login	System	This report captures detected startup or running config changes - the changes are detected by logging into the ...