nuSpective
straightforward · trustworthy · responsive

ISO 27001 Bundle

Report Start Time : Jul 23 2019, 09:47:46 AM EDT

Report End Time: Jul 23 2019, 10:47:45 AM EDT

Found Records 82

Rank	Report Name	Report Description	Count
1	ISO 27001 A.12.1.2: Users Added To Local Groups	This report captures users added to local groups.	1
2	ISO 27001 A.13: Rogue AP Detected	Provides details of rogue AP events	1
3	ISO 27001 A.12.2, A.13: Permitted File Export Activity	Reports permitted file export activity as reported by firewalls and security gateways	1
4	ISO 27001 A.12.6.1: Top Hosts with Vulnerabilities found by scanners	Ranks the hosts by vulnerabilities found by scanners	1
5	ISO 27001 A.12.1.2: Local Windows Groups Modified	This report captures local group modifications	1
6	ISO 27001 A.13: Top Permitted Vulnerable Low Port Services By Connections, Bytes	Tracks uncommon services permitted by firewalls - vulnerable services include Microsoft services such as MS-RPC (135), NETBIOS-SSN (139), MICROSOFT-DS (445), MS-SQL (1433,1434), FTP (23), TELNET (21)	1
7	ISO 27001 A.9.4: Failed VPN Admin Logon	Provides event details for all failed VPN admin logons	1
8	ISO 27001 A.12.2: Malware found but not remediated	Captures events that indicate the viruses that Host Antivirus found but failed to remedy	1
9	ISO 27001 A.12.1.3: Top ESX By Memory Utilization With Details	This report ranks ESX hosts by memory utilization. Other memory usage metrics are included.	1
10	ISO 27001 A.12.2, A.13: Permitted File Import Activity	Reports permitted file import activity as reported by firewalls and security gateways	1
11	ISO 27001 A.8.1.1: CMDB Device Modification History	Details the history of device attribute changed in CMDB	1
12	ISO 27001 A.17: Top Applications By Synthetic Transaction Response Time	Ranks the services by average synthetic transaction monitoring probe response times.	1
13	ISO 27001 A.12.2, A.13: Inbound Malware Found At the Boundary By IPS, Firewalls and Security Gateways	Reports on inbound malware detected at the trust/untrust boundary by edge devices such as IPS devices, Firewalls and Security Gateways.	1
14	ISO 27001 A.12.4.1: Top Reporting Modules By Event Rate (Per Sec)	Ranks the reporting device modules by sent events per second	1
15	ISO 27001 A.9.4: Unix Server Privileged Logon	This report details UNIX server privileged logon (su) details with all parsed parameters and raw logs	1
16	ISO 27001 A.12.1.3: Top ESX By CPU Utilization	This report ranks ESX hosts by aggregate cpu utilization. Other CPU usage metrics are included.	1
17	ISO 27001 A.12.1.3: Top Datastores By Least Free Space	This report ranks ESX datastore with lowest free space	1

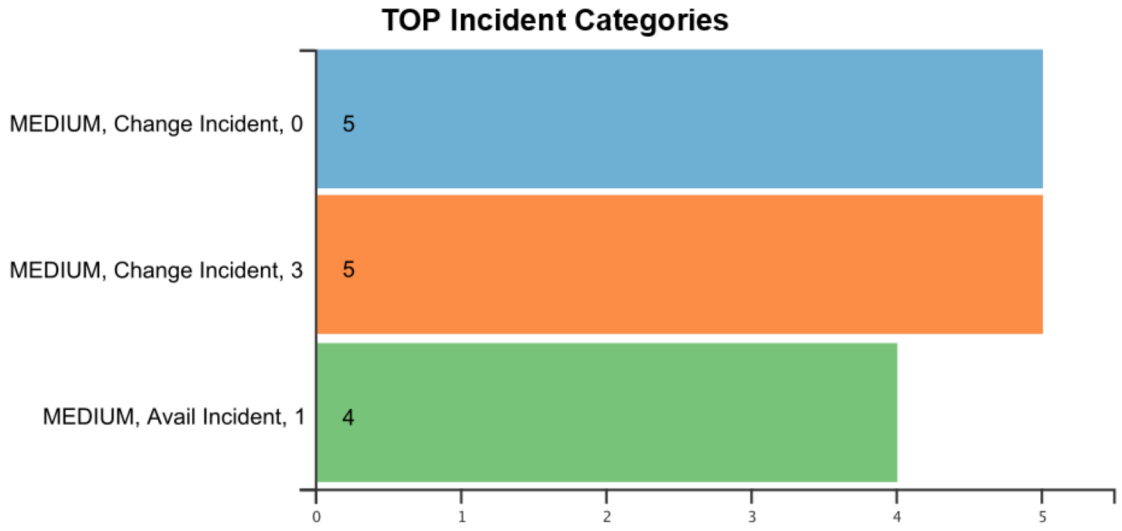
Rank	Report Name	Report Description	Count
18	ISO 27001 A.9.4: Windows Domain Account Lockouts	This report details windows domain account lockouts	1
19	ISO 27001 A.12.1.3: Windows Servers By Least Free Disk Space	Ranks windows servers by minimum free disk space over a window	1
20	ISO 27001 A.12.2, A.13: Outbound Malware Found At the Boundary By IPS, Firewalls and Security Gateways	Reports on outbound malware detected at the trust/untrust boundary by edge devices such as IPS devices, Firewalls and Security Gateways.	1
21	ISO 27001 A.12.4.4: Windows System Clock Change	Tracks system clock changes on windows systems	1
22	ISO 27001 A.12.1.2: Local Windows User Accounts Modified	This report captures local user account modifications.	1
23	ISO 27001 A.12.1.3: VMware Cluster Utilization Report	This report provides a cluster level resource utilization report; ranked by CPU util	1
24	ISO 27001 A.12.1.2: Network Config Changes Detected From Log	This report provides details about router config changes	1
25	ISO 27001 A.12.2: Spyware found but not remediated	Captures events that indicate Spyware found on a device Host Anti-virus solutions failed to remedy	1
26	ISO 27001 A.12.1.3: Top Routers/Firewalls By Memory Utilization	Ranks the routers by average memory utilization over a window	1
27	ISO 27001 A.12.4.1:Top Events By Count	Ranks the events by the number of times they have occurred in a given time period.	1
28	ISO 27001 A.9.4: Windows Server Account Lock/Unlock history	Captures account lockouts and unlocks on windows servers. Account lockouts happen on repeated login failures and may be suspicious if they are repeated or happen at odd hours of operation.	1
29	ISO 27001 A.16: ISO 27001 Related Incident Categories By Count	Captures ISO 27001 Related incidents in a time window	1
30	ISO 27001 A.9.4: Firewall Admin Activity Details	Provides details about firewall admin activity - logons, command executions and logoff	1
31	ISO 27001 A.17: Top Devices by Business Hours System Uptime Pct (Achieved System SLA)	Ranks the devices by system uptime pct over a time window - uptime calculated during business hours (Mon-Friday 8am-5pm)	1
32	ISO 27001 A.9.4: Successful Unix Privilege Escalations	This report ranks the UNIX servers and their users by successful privilege escalations (su) count	1
33	ISO 27001 A.12.1.2: Windows System Configuration and Policy Modifications	This report server configuration change and policy modification events	1
34	ISO 27001 A.9.4: Domain Account Lock/Unlock history	Captures account lockouts and unlocks on domain accounts. Account lockouts happen on repeated login failures and may be suspicious if they are repeated or happen at odd hours of operation.	1
35	ISO 27001 A.9.4: Failed Unix Privilege Escalations	This report ranks the UNIX servers and their users by failed privilege escalations (su) count	1
36	ISO 27001 A.12.1.2: Network Device Run vs Startup Config Difference Via Login	This report captures detected differences between a routers running and startup config	1
37	ISO 27001 A.12.1.2: Users Deleted From Global Groups	This report captures users deleted from global or univeral groups.	1

Rank	Report Name	Report Description	Count
38	ISO 27001 A.12.1.2: Unix Users Added To Group	Tracks user additions to groups	1
39	ISO 27001 A.13: Top Permitted Inbound Connections By Connections, Bytes	Ranks firewalls and permitted inbound services by first the total number of connections and then by bytes for that service	1
40	ISO 27001 A.16: ISO 27001 Related Incidents, Assigned Users By Resolution Time	ISO 27001 Related Incidents, Assigned Users By Resolution time	1
41	ISO 27001 A.16: Install Software Changes Detected Via Login	This report captures detected install software changes - the changes are detected by logging into the device and hence is accurate.	1
42	ISO 27001 A.12.1.3: Top VMs By PCPU Ready Pct	This report ranks VMware virtual machines by per-cpu ready percent. A high number indicates the VM is starved of CPU	1
43	ISO 27001 A.12.1.2: Users Deleted From Local Groups	This report captures users deleted from local groups.	1
44	ISO 27001 A.12.1.2: User removed from Privileged Windows Groups	Tracks users removed from Windows priviledged groups such as Domain Admins, Remote Desktop Users, Backup Operators, DNS Admins, Administrators	1
45	ISO 27001 A.12.2, A.13: Blocked Web Browsing Activity	Reports blocked web browsing activity as reported by firewalls and security gateways	1
46	ISO 27001 A.8.1.1: CMDB Device Addition and Deletion History	Details the history of devices getting added and deleted from CMDB	1
47	ISO 27001 A.9.4: Remote Desktop Connections to Windows Servers	This report details successful and failed remote desktop connections	1
48	ISO 27001 A.13: Top Permitted High Port Services By Connections, Bytes	Tracks the high port services permitted by firewalls - these services may pose security risk	1
49	ISO 27001 A.12.1.3: Top Routers/Firewalls Ranked By CPU Utilization	Ranks the routers by average cpu utilization over a window	1
50	ISO 27001 A.12.1.2: Users Added To Global Groups	This report captures users added to global or univeral groups.	1
51	ISO 27001 A.12.1.2: User added to Privileged Windows Groups	Tracks users added to Windows priviledged groups such as Domain Admins, Remote Desktop Users, Backup Operators, DNS Admins, Administrators	1
52	ISO 27001 A.16: Windows Installed Software Changes (Via FortiSIEM Agent)	This report captures installed software changes detected via FortiSIEM Agent	1
53	ISO 27001 A.9.4: Failed WLAN Admin Logon	Tracks failed admin logons to the WLAN Controller	1
54	ISO 27001 A.17: Top Devices by Accumulated Network Ping Downtime During Business Hours	Ranks the devices by total network ping downtime during business hours (Mon-Friday 8am-5pm)	1
55	ISO 27001 A.12.1.2: Local Windows User Accounts Created	This report captures user accounts added on a server	1
56	ISO 27001 A.9.4: Privileged Windows Server Logon Attempts using the Administrator Account	This report details prvileged logon attempts to a windows server using the Administrator account	1
57	ISO 27001 A.9.4: Unix Server Privileged Command Execution	This report details privilege command execuations (sudo) at a Unix server	1

Rank	Report Name	Report Description	Count
58	ISO 27001 A.12.1.2: Global Windows Groups Deleted	This report captures global group deletions	1
59	ISO 27001 A.12.2, A.13: Blocked File Export Activity	Reports blocked file export activity as reported by firewalls and security gateways	1
60	ISO 27001 A.12.6.1: Host vulnerability found by scanners	Details the vulnerabilities discovered on hosts	1
61	ISO 27001 A.12.1.2: Local Windows User Accounts Deleted	This report captures user accounts removed from a server	1
62	ISO 27001 A.16: Windows Registry Changes (Via FortiSIEM Agent)	This report captures registry changes detected via FortiSIEM Agent	1
63	ISO 27001 A.13: Top Permitted Uncommon Services By Connections, Bytes	Tracks uncommon services permitted by firewalls - common services include DNS, SMTP, Web	1
64	ISO 27001 A.12.1.2: Local Windows Groups Created	This report captures local group creations	1
65	ISO 27001 A.9.4: Detailed Successful Login At ISO 27001 Device	Captures detailed successful logins at any device or application including servers, network devices, domain controllers, VPN gateways, WLAN controllers and applications	1
66	ISO 27001 A.17: Top STMs by Business Hours Uptime Pct (Achieved Application SLA)	Ranks Synthetic transaction monitor tests (STM) by achieved uptime over a time window	1
67	ISO 27001 A.12.1.2: Global Windows Groups Modified	This report captures global group modifications	1
68	ISO 27001 A.12.1.2: Server Password Changes	Tracks password changes	1
69	ISO 27001 A.16: ISO 27001 Related Incidents	Captures ISO 27001 Related incidents in a time window	1
70	ISO 27001 A.12.1.3: Top ESX By Device Disk Read Latency	This report ranks ESX hosts by device disk I/O read latency	1
71	ISO 27001 A.9.4: Router Admin Activity Details	Provides details about router admin activity - logons, command executions and logoff	1
72	ISO 27001 A.12.1.3: Top ESX By Device Disk Write Latency	This report ranks ESX hosts by device disk I/O write latency.	1
73	ISO 27001 A.12.1.3: Unix Servers By Least Free Disk Space	Ranks windows servers by minimum free disk space over a window	1
74	ISO 27001 A.12.2: Spyware found and remediated	Captures events that indicate spyware was found and remediated on a host. This report is applicable for host antivirus, security gateways, proxies and firewalls that do content inspection e.g. Palo Alto Firewall, Untangle etc.	1
75	ISO 27001 A.12.2: Malware found and remediated	Captures events that indicate the viruses found and remediated. This report is applicable for host antivirus, security gateways, proxies and firewalls that do content inspection e.g. Palo Alto Firewall, Untangle etc.	1
76	ISO 27001 A.12.2, A.13: Blocked File Import Activity	Reports blocked file import activity as reported by firewalls and security gateways	1
77	ISO 27001 A.9.4: Windows Server Account Lockouts	This report captures account lockouts on windows servers. Account lockouts happen on repeated login failures and may be suspicious if they are repeated or happen at odd hours of operation	1

Rank	Report Name	Report Description	Count
78	ISO 27001 A.12.1.2: Global Windows Groups Created	This report captures global group creations	1
79	ISO 27001 A.12.2: Windows File Modification (via FortiSIEM Agent)	This report captures the details of windows server file access events detected via FortiSIEM Windows Agent.	1
80	ISO 27001 A.12.1.2: Local Windows Groups Deleted	This report captures local group deletions	1
81	ISO 27001 A.13: Top Permitted Outbound Connections By Connections, Bytes	Ranks firewalls and permitted outbound services by first the total number of connections and then by bytes for that service	1
82	ISO 27001 A.12.1.2: Network Config Changes Detected Via Login	This report captures detected startup or running config changes - the changes are detected by logging into the device and hence is accurate.	1

1 Top Security Incidents



Rank	Event Severity Category	Event Type Group	Incident Category	COUNT(Matched Events)
1	MEDIUM	Change Incident	0	5
2	MEDIUM	Change Incident	3	5
3	MEDIUM	Avail Incident	1	4

2 Domain Account Lockout History

Rank	Reporting Device	Event Receive Time	Event Name	User	Domain
1	WIN2008-ADS	7/23/19 10:30:04 AM	A user account was locked out	tamera.leibtag	ACCELOPS
2	WIN2008-ADS	7/23/19 10:30:04 AM	Windows user account unlocked		
3	WIN2008-ADS	7/23/19 10:30:04 AM	Windows user account unlocked		
4	WIN2008-ADS	7/23/19 10:30:04 AM	A user account was locked out	mike.richardson	ACCELOPS
5	WIN2008-ADS	7/23/19 10:30:03 AM	A user account was locked out	heather.biggs	ACCELOPS
6	WIN2008-ADS	7/23/19 10:30:03 AM	A user account was locked out	archie.kuhn	ACCELOPS

3 Global Windows Groups Modified

Rank	Reporting Device	Event Receive Time	User	Computer	Target User Group
1	THREATSOCDC	7/23/19 10:03:29 AM	administrator		Domain Admins
2	THREATSOCDC	7/23/19 10:03:25 AM	administrator		Domain Admins
3	THREATSOCDC	7/23/19 10:00:02 AM	francis.underwood		Domain Admins
4	THREATSOCDC	7/23/19 10:00:02 AM	francis.underwood		Domain Admins
5	THREATSOCDC	7/23/19 10:00:01 AM	administrator		Domain Admins
6	WIN2008-ADS	7/23/19 10:00:04 AM	mike.long		Domain Admins
7	WIN2008-ADS	7/23/19 10:00:03 AM	administrator		Domain Admins
8	WIN2008-ADS	7/23/19 10:00:01 AM	administrator		Domain Admins
9	WIN2008-ADS	7/23/19 10:00:01 AM	mike.long		Domain Admins

4 Installed Software Change History

Rank	Event Receive Time	Host Name	Host IP	Event Name	Old SVN Version	New SVN Version	Added Item	Deleted Item
1	7/23/19 10:00:05 AM	THREATSOCDC	10.1.1.33	New software (un)installed	18	34	Epilog version 1.5.6.1 (1.5.6.1);Snare version 4.0.0.2 (4.0.0.2);	(none)
2	7/23/19 10:00:09 AM	threatsocdc.threatsoc.com	10.1.1.33	New software (un)installed	19	36	Epilog version 1.5.6.1 (1.5.6.1);Snare version 4.0.0.2 (4.0.0.2);	(none)