nuSpective
straightforward · trustworthy · responsive

NIST 800-53 Bundle

Report Start Time : Jul 23 2019, 10:37:55 AM EDT

Report End Time: Jul 23 2019, 11:37:54 AM EDT

Found Records 85

Rank	Report Name	Report Description	Count
1	NIST800-53 CM-11: Windows Registry Changes (Via FortiSIEM Agent)	This report captures registry changes detected via FortiSIEM Agent	1
2	NIST800-53 SI-4: Top WLAN IDS Alerts	Ranks WLAN IDS alerts	1
3	NIST800-53 AC-2: Global Groups Created	This report captures global group creations	1
4	NIST800-53 SI-4: 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
5	NIST800-53 SI-4: Top IPs with Malware Found By IPS and Firewalls	Tracks IP addresses with Malware as found by IPS - these are somewhat less reliable than Host Anti-virus and Security Gateways	1
6	NIST800-53 AC-2: Domain User Password Changes	Tracks password changes	1
7	NIST800-53 SI-4: Phishing attempt found and remediated	Captures events that indicate phishing attempt	1
8	NIST800-53 SI-4: Top Computers with Malware Found By Antivirus and Security Gateways	Tracks computers with Malware as found by Host Anti-virus and Security Gateways	1
9	NIST800-53 SI-4: Spam/Malicious Mail Attachment found and remediated	Captures events that indicate spam or maillicious mail attachments were 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, Websense Mail gateway, Ironport Mail Gateway etc.	1
10	NIST800-53 AC-2: Local Windows User Accounts Modified	This report captures local user account modifications.	1
11	NIST800-53 CM-3: Firewall 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
12	NIST800-53 SC-7: Top Permitted Uncommon Services By Connections, Bytes	Tracks uncommon services permitted by firewalls - common services include DNS, SMTP, Web	1
13	NIST800-53 AC-2: Windows domain user accounts deleted	Captures user accounts removed from a domain	1
14	NIST800-53 SI-4: Top External Source Countries By Network IPS Events	This report ranks the countries originating the most inbound IPS Events	1
15	NIST800-53 AC-2: Windows domain user accounts modified	Captures domain user account modifications.	1
16	NIST800-53 SC-7: Top Permitted High Port Services By Connections, Bytes	Tracks the high port services permitted by firewalls - these services may pose security risk	1
17	NIST800-53 AC-2: Windows domain user accounts created	Captures user accounts added to a domain	1

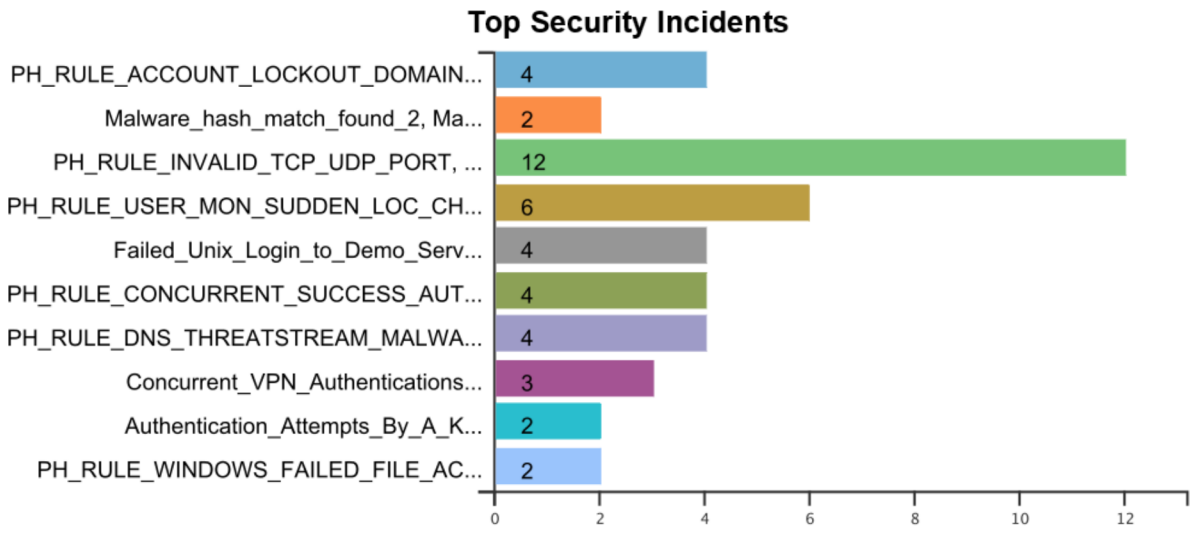
Rank	Report Name	Report Description	Count
18	NIST800-53 CM-3: WLAN Config Change	This report tracks all software, hardware and device configuration changes at WLAN Access points and Base stations. The report includes Original Reporting Controller IP, Event Type and MAC address of the AP or Controller where the event happened. If the MAC address is empty then, the event happened at the reporting Controller.	1
19	NIST800-53 SC-7: 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
20	NIST800-53 AC-2: Global Windows Groups Created	This report captures global group creations	1
21	NIST800-53 IR-5: Top Monitored Device Groups By Incident Severity, Count	Ranks monitored device groups by incident severity and count	1
22	NIST800-53 CM-3: Router/Switch Run vs Startup Config Difference Via Login	This report captures detected differences between a routers running and startup config	1
23	NIST800-53 IR-4: Monthly Assigned Incident User Trend	Monthly Incidents By Assigned Users	1
24	NIST800-53 AC-2: Windows users added To Local Groups	This report captures users added to local groups.	1
25	NIST800-53 AC-7: Windows Server Account Unlocks	Captures account unlocks on windows servers. Account unlocks happen after lockouts that may happen on repeated login failures	1
26	NIST800-53 AC-17: Top Wireless Controllers, Users By Successful Logon Count	Ranks wireless controllers by successful logons	1
27	NIST800-53 IR-4: Monthly Incident Resolution Time Trend	Incidents severities by resolution time	1
28	NIST800-53 SI-8: Spam/Malicious Mail Attachment found but not remediated	Captures events that indicate spyware was found but the detecting software did not remediated the vulnerability. This report is applicable for host antivirus, security gateways, proxies and firewalls that do content inspection e.g. Palo Alto Firewall, Untangle, Websense Mail gateway, Ironport Mail Gateway etc.	1
29	NIST800-53 AC-2: Local Windows User Accounts Created	This report captures user accounts added on a server	1
30	NIST800-53 SC-19: VoIP Call Report	This is a call detail report	1
31	NIST800-53 SI-4: Non-compliant Hosts and Security Software License Expirations	Tracks non-compliant hosts and license expiry events from Security Management Gateways and Firewalls. Non-compliant hosts may not have proper security software running and therefore may pose a security threat. License expiration of security software may expose exploitable security vulnerabilities.	1
32	NIST800-53 AC-2: Computers deleted from Windows domain	Captures computers removed from a domain	1
33	NIST800-53 IR-5: Incidents By Location and Category	Incidents By Location and Category	1
34	NIST800-53 RA-5: Top Hosts with Vulnerabilities found by scanners	Ranks the hosts by vulnerabilities found by scanners	1
35	NIST800-53 AC-2: Global Windows Groups Modified	This report captures global group modifications	1

Rank	Report Name	Report Description	Count
36	NIST800-53 SI-4: Top Internal Network Scanners By Event Count	Ranks the source IP addresses by detected network scan or reconnaissance events	1
37	NIST800-53 CM-3: Router/Switch 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
38	NIST800-53 AC-2: Windows domain groups created	Captures domain group creations	1
39	NIST800-53 SI-8: IronPort Mail dropped by filter	Records all mail that was dropped by a configured filter	1
40	NIST800-53 AC-2: Windows domain groups modified	Captures domain group modifications	1
41	NIST800-53 AC-2: Windows users added To Global Groups	This report captures users added to global or univeral groups.	1
42	NIST800-53 SI-4: Virus found but not remediated	Captures events that indicate viruses found but failed to remedy - the events could be from Host Anti-virus or Network Security Gateways. This report is applicable for host antivirus, security gateways, proxies and firewalls that do content inspection e.g. Palo Alto Firewall, Untangle etc.	1
43	NIST800-53 SI-4: 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
44	NIST800-53 SC-19: Top VoIP Called Destinations	Ranks the VoIP destinations by call count and duration	1
45	NIST800-53 AC-7: Failed VPN Admin Logon	Provides event details for all failed VPN admin logons	1
46	NIST800-53 AC-7: Failed VPN User Logon	Failed VPN logons	1
47	NIST800-53 AC-7: Failed WLAN User Logon	Provides details of wireless logon authentication failures	1
48	NIST800-53 AC-7: Failed Firewall Admin Logon	Details about failed firewall logons	1
49	NIST800-53 SC-7: 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
50	NIST800-53 RA-5: Top OS types with vulnerabilities	Ranks OS types by vulnerabilities found	1
51	NIST800-53 SC-19: Top VoIP Callers	Ranks the VoIP callers by call count and duration	1
52	NIST800-53 AC-2: Global Groups Deleted	This report captures global group deletions	1
53	NIST800-53 AC-2: Local Groups Created	This report captures local group creations	1
54	NIST800-53 AC-7: Failed Windows Domain Authentications	This report ranks the windows servers and their users by the number of failed logons	1
55	NIST800-53 IR-5: Top Security Incidents By Severity, Count	Ranks the security related incidents by first their severity and then by their count	1

Rank	Report Name	Report Description	Count
56	NIST800-53 SI-4: Top IPs with Malware Found By Security Gateways	Tracks IP addresses with Malware as found by Security Gateways	1
57	NIST800-53 AC-2: All VMWare VCenter Account/Group Change Events	This report lists all account/group change events	1
58	NIST800-53 AC-7: Failed Unix Server Logons	This report details failed unix server logons with all parsed fields and raw logs	1
59	NIST800-53 IR-5: Top Monitored Device Groups By Incident Name, Count	Ranks monitored device groups by incident name and count	1
60	NIST800-53 IR-5: Monthly Incident Trend	Shows incident trend on a month-by-month basis	1
61	NIST800-53 SC-19: VoIP Call Volume Trend	Trends the call volume	1
62	NIST800-53 AC-2: Local Windows Groups Modified	This report captures local group modifications	1
63	NIST800-53 IR-4: Incidents, Assigned Users By Resolution Time	Incidents By Assigned Users and resolution time	1
64	NIST800-53 SI-4: Top Network IPS Events By Severity, Count	Ranks the network IPS events by count	1
65	NIST800-53 RA-5: Host vulnerability found by scanners with details	Details the vulnerabilities discovered on hosts	1
66	NIST800-53 SC-7: 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
67	NIST800-53 AC-2: Windows Server Password Changes	Tracks password changes	1
68	NIST800-53 SI-4: Rogue APs detected	Lists the rogue APs	1
69	NIST800-53 AC-7: Failed Router Admin Logons	Details about failed router logons	1
70	NIST800-53 CM-11: Windows Installed Software Changes (Via FortiSIEM Agent)	This report captures installed software changes detected via FortiSIEM Agent	1
71	NIST800-53 CM-3: Firewall Run vs Startup Config Difference Via Login	This report captures detected differences between a routers running and startup config	1
72	NIST800-53 SI-4: Spyware found but not remediated	Captures events that indicate spyware was found but the detecting software failed to remediated the vulnerability. This report is applicable for host antivirus, security gateways, proxies and firewalls that do content inspection e.g. Palo Alto Firewall, Untangle etc.	1
73	NIST800-53 AC-2: Computers added to Windows domain	Captures computers added to a domain	1
74	NIST800-53 IR-5: Weekly Incident Trend	Shows incident trend on a week-by-week basis	1
75	NIST800-53 AC-17: Top VPN Gateways, Users Ranked By Session Count, Bytes, Duration	Ranks the VPN Gateways and their users by the total amount ofexchanged bytes. This report provides further insight into the top VPN users from a bytes transferred perspective	1
76	NIST800-53 AC-2: Global Groups Modified	This report captures global group modifications	1

Rank	Report Name	Report Description	Count
77	NIST800-53 AC-2: Unix User Password Changes	Tracks user password changes in Unix systems	1
78	NIST800-53 SI-8: IronPort Mail quarantined for Spam	Records all mail that was quarantined for suspicion of spam	1
79	NIST800-53 AC-7: 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
80	NIST800-53 AC-2: Local Windows User Accounts Deleted	This report captures user accounts removed from a server	1
81	NIST800-53 AC-2: Local Windows Groups Created	This report captures local group creations	1
82	NIST800-53 RA-5: Host vulnerabilities found by scanners	This report details the host vulnerabilties found by scanners like Qualys, Nessus, nCircle, McAfee etc	1
83	NIST800-53 AC-2: Windows domain groups deleted	Captures domain group deletions	1
84	NIST800-53 AC-7: Failed WLAN Admin Logon	Tracks failed admin logons to the WLAN Controller	1
85	NIST800-53 AC-2: Audited Linux file changes	Tracks user modifications to Linux files and directories. Both the content and attribute modifications are captured. For actions on directories, the affected files in the directories are also captured.	1

1 Top Security Incidents



Rank	Event Name	Event Severity	COUNT(Matched Events)
1	Account Locked: Domain	10	4
2	Malware hash match found	10	2
3	Invalid TCP/UDP Port Traffic	9	12
4	Sudden User Location Change	9	6
5	Failed Unix Login to Demo Server	9	4
6	Concurrent Successful Authentications To Same Account From Multiple Cities	9	4
7	DNS Traffic to Threat Stream Malware Domains	9	4
8	Concurrent VPN Authentications To Same Account From Different Countries	9	3
9	Authentication Attempts By A Known Host Scanner	9	2
10	Windows failed file access	9	2
11	Brute Force Host Login Success_Fixed	9	1
12	Outbound cleartext password usage detected	9	1
13	Concurrent VPN Authentications To Same Account From Different Cities	9	1
14	Successful VPN Logon from outside my country	8	5
15	Multiple Admin Logon Failures: Net Dev: No Source IP	8	1

2 Failed Domain Authentications

Rank	Event Receive Time	Source IP	User	Domain	Win Logon Type
1	7/23/19 10:38:00 AM	192.168.1.124	Administrator	ACCELOPS.NET	3 (Network - logon)
2	7/23/19 10:38:00 AM	192.168.1.124	Administrator	ACCELOPS.NET	3 (Network - logon)
3	7/23/19 10:38:00 AM	192.168.1.124	Administrator	ACCELOPS.NET	3 (Network - logon)
4	7/23/19 10:38:02 AM	192.168.64.10	administrator	ACCELOPS	3 (Network - logon)
5	7/23/19 10:38:02 AM	192.168.64.10	administrator	ACCELOPS	3 (Network - logon)
6	7/23/19 10:38:46 AM	192.168.64.10	administrator	ACCELOPS	3 (Network - logon)
7	7/23/19 10:38:47 AM	192.168.64.10	administrator	ACCELOPS	3 (Network - logon)
8	7/23/19 10:38:47 AM	192.168.64.10	administrator	ACCELOPS	3 (Network - logon)
9	7/23/19 10:38:48 AM	192.168.1.124	Administrator	ACCELOPS.NET	3 (Network - logon)
10	7/23/19 10:38:48 AM	192.168.1.124	Administrator	ACCELOPS.NET	3 (Network - logon)
11	7/23/19 10:38:48 AM	192.168.1.124	Administrator	ACCELOPS.NET	3 (Network - logon)
12	7/23/19 10:39:46 AM	192.168.64.10	administrator	ACCELOPS	3 (Network - logon)
13	7/23/19 10:39:47 AM	192.168.64.10	administrator	ACCELOPS	3 (Network - logon)
14	7/23/19 10:39:47 AM	192.168.64.10	administrator	ACCELOPS	3 (Network - logon)
15	7/23/19 10:39:47 AM	192.168.64.10	administrator	ACCELOPS	3 (Network - logon)

3 Global Windows Groups Modified

Rank	Reporting IP	Event Receive Time	Source IP	User	Target User Group
1	192.168.0.10	7/23/19 11:00:01 AM		administrator	Domain Admins
2	192.168.0.10	7/23/19 11:00:01 AM		mike.long	Domain Admins
3	192.168.0.10	7/23/19 11:00:03 AM		administrator	Domain Admins
4	192.168.0.10	7/23/19 11:00:04 AM		mike.long	Domain Admins

4 Router/Switch Config Changes

Rank	Event Receive Time	Host Name	Host IP	Event Name	Old SVN Version	New SVN Version	Added Item	Deleted Item
1	7/23/19 11:00:01 AM	SJ-Main-Cat6500	192.168.20.1	Running config changed	81	82	enable secret 5 $1$3T2G$AhfZnnW58ird0lmOHea0M/;	(none)