nuSpective
straightforward · trustworthy · responsive

PCI Bundle

Report Start Time : Jul 30 2019, 11:59:32 AM EDT

Report End Time: Jul 30 2019, 12:59:31 PM EDT

Found Records 91

Rank	Report Name	Report Description	Count
1	PCI 1.x: Top Permitted Uncommon Services By Connections, Bytes	Tracks uncommon services permitted by firewalls - common services include DNS, SMTP, Web	1
2	PCI 10.x: Unix User Lockouts	This report captures account lockouts on unix servers. Account lockouts happen on repeated login failures and may be suspicious if they are repeated or happen at odd hours of operation	1
3	PCI 1.x: Top Permitted High Port Services By Connections, Bytes	Tracks the high port services permitted by firewalls - these services may pose security risk	1
4	PCI 8.x: 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
5	PCI 10.x: Unix User Accounts Modified	This report captures user account modifications on unix servers	1
6	PCI 10.x: Local Windows Groups Created	This report captures local group creations	1
7	PCI 10.x: Unix User Accounts Created	This report captures user accounts added on unix servers	1
8	PCI 10.x: Successful Firewall Admin Logon Details (g)	Details about successful firewall logons	1
9	PCI 10.x: Successful VPN Admin Logon (g)	Provides event details for all successful VPN admin logons	1
10	PCI 8.x: 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
11	PCI 1.x: 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	PCI 10.x: Local Windows Groups Modified	This report captures local group modifications	1
13	PCI 10.x: Local Windows Groups Deleted	This report captures local group deletions	1
14	PCI 10.x: Failed Unix Server Privileged Login	This report details failed UNIX server privileged logon (su)	1
15	PCI 1.x: Router Run vs Startup Config Difference Via Login	This report captures detected differences between a routers running and startup config	1
16	PCI 1.x: Firewall NAT Translations	This report captures the NAT translations over a time window	1
17	PCI 10.x: Unix User Accounts Deleted	This report captures user accounts removed from unix servers	1

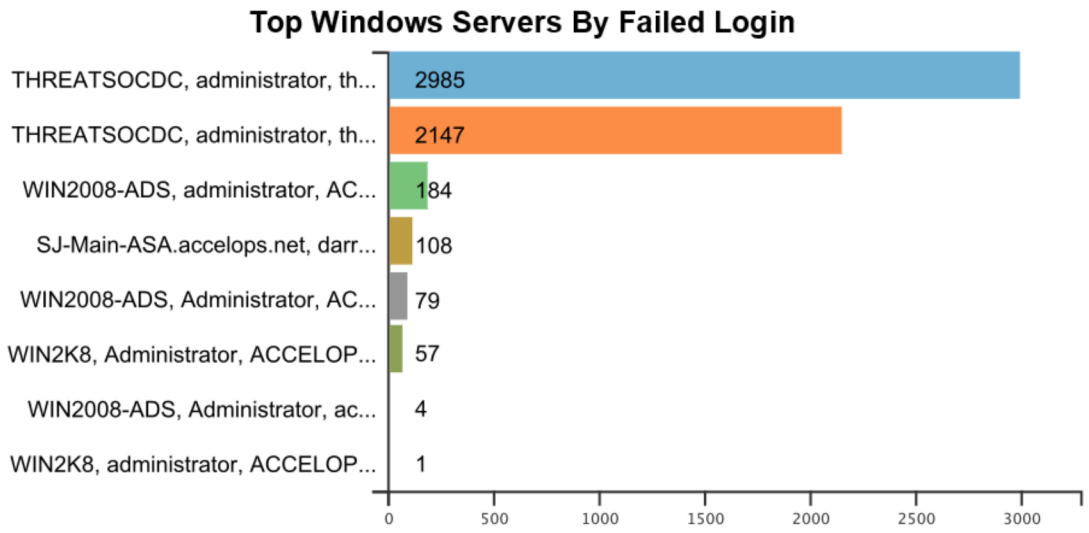
Rank	Report Name	Report Description	Count
18	PCI 8.x: Windows Server Account Lock/Unlock history (g)	Captures account lockouts and unlocks on windows servers. Account lockouts happen on repeated login failures and may be suspicious if they are repeated or happen at odd hours of operation.	1
19	PCI 1.x: Top Unauthorized Permitted Connections to Web DMZ By Connections, Bytes	Tracks the unauthorized permitted connections involving Web DMZ. This assumes that there are certain protocols allowed between Internet and Web DMZ, between Web DMZ and App DMZ and between Inside and Web DMZ. This report captures the traffic that violates these conditions.	1
20	PCI 10.x: Unix User Unlocks	This report details windows domain account lockouts	1
21	PCI 10.x: Successful Router/Switch Admin Login	Successful router/switch logons	1
22	PCI 10.x: Privileged Windows Server Logon Attempts using the Administrator Account (g)	This report details privileged logon attempts to a windows server using the Administrator account	1
23	PCI 10.x: Windows User Accounts Modified	This report captures local user account modifications.	1
24	PCI 10.x: Windows Users Deleted From Global Groups	This report captures users deleted from global or univeral groups.	1
25	PCI 10.x: Global Windows Groups Created	This report captures global group creations	1
26	PCI 5.x: Top IPs with Malware Found By Antivirus and Security Gateways	Tracks IP addresses with Malware as found by Host Anti-virus and Security Gateways	1
27	PCI 1.x: Top Firewall Originated Or Destined Permitted Connections By Count	Ranks the firewall originated or destined connections - these connections would be typically be for administrative and monitoring purposes	1
28	PCI 1.x: Top Permitted Connections Between App DMZ and DB DMZ By Connections, Bytes	Tracks the permitted connections between App DMZ and DB DMZ	1
29	PCI 10.x: Global Windows Groups Deleted	This report captures global group deletions	1
30	PCI 10.x: Successful Unix Server Privileged Command Execution	This report details privilege command executions (sudo) at a Unix server	1
31	PCI 5.x: Malware found but not remediated by Endpoint Protection	Captures events that indicate the viruses that Host Antivirus found but failed to remedy	1
32	PCI 10.x: Remote Desktop Connections to Windows Servers (g)	This report details successful and failed remote desktop connections	1
33	PCI 1.x: 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
34	PCI 10.x: Successful Remote Desktop Connections to Windows Servers	This report details successful remote desktop connections	1
35	PCI 10.x: Unix Users Added To Groups	This report captures users added to Unix groups	1
36	PCI 10.x: Windows User Accounts Deleted	This report captures user accounts removed from a server	1
37	PCI 1.x: Firewall Run vs Startup Config Difference Via Login	This report captures detected differences between a firewall's running	1

Rank	Report Name	Report Description	Count
		and startup config	
38	PCI 10.x: Windows Password Changes	Tracks password changes on Windows Servers	1
39	PCI 10.x: Failed WLAN Admin Logon (g)	Tracks failed admin logons to the WLAN Controller	1
40	PCI 10.x: Successful WLAN Admin Login	Tracks successful admin logons to the WLAN Controller	1
41	PCI 1.x: 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
42	PCI 10.x: Failed VPN Admin Login	Provides event details for all failed VPN admin logons	1
43	PCI 1.x: Router Config Changes Detected From Log	This report provides details about router config changes	1
44	PCI 1.x: Top Permitted Connections Between Internet and Web DMZ By Connections, Bytes	Tracks the permitted connections between Internet and Web DMZ	1
45	PCI 1.x: Top Unauthorized Permitted Connections to App DMZ By Connections, Bytes	Tracks the permitted connections involving Web DMZ. This assumes that there are certain protocols allowed between Web DMZ and App DMZ, between App DMZ and DB DMZ and between Inside and App DMZ. This report captures the traffic that violates these conditions.	1
46	PCI 8.x: Server Password Changes (g)	Tracks password changes	1
47	PCI 1.x: Top Reporting Firewalls By Event Count	Ranks the firewalls by the number of events sent	1
48	PCI 10.x: Successful Privileged Windows Server Logins using the Administrator Account	This report details privileged login attempts to a windows server using the Administrator account	1
49	PCI 10.x: Failed WLAN Admin Login	Tracks failed admin logons to the WLAN Controller	1
50	PCI 1.x: Top Inbound Permitted Services By Connections, Bytes	Ranks firewalls and permitted inbound services by first the total number of connections and then by bytes for that service	1
51	PCI 5.x: Spyware found but not remediated by Endpoint Protection	Captures events that indicate Spyware found on a device Host Anti-virus solutions failed to remedy	1
52	PCI 1.x: Firewall Admin Activity Details	Provides details about firewall admin activity - logons, command executions and logoff	1
53	PCI 10.x: Failed Unix Server Privileged Command Execution	This report details privilege command executions (sudo) at a Unix server	1
54	PCI 10.x: Windows User 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
55	PCI 10.x: Successful Unix Server Privileged Login	This report details successful UNIX server privileged logon (su)	1
56	All PCI Systems By Last Event Receive Time	Lists PCI Systems with last event receive time	1
57	PCI 10.x: Successful Router Admin Logon Details (g)	Details about successful router logons	1

Rank	Report Name	Report Description	Count
58	PCI 10.x: Unix Users Deleted From Groups	This report captures users deleted from Unix groups	1
59	PCI 10.x: Windows System Clock Change	Tracks system clock changes on windows systems	1
60	PCI 10.x: Network Device Down/Restart	Tracks network device down and restart events	1
61	PCI 10.x: Windows User Accounts Created	This report captures user accounts added on a server	1
62	PCI 1.x: Firewall Config Changes Detected Via Login (g)	This report captures detected startup or running config changes - the changes are detected by logging into the device and hence is accurate.	1
63	PCI 10.x: Detailed Successful Login At PCI Device	Captures detailed successful logins at any device or application including servers, network devices, domain controllers, VPN gateways, WLAN controllers and applications	1
64	PCI 10.x: Windows Users Added To Local Groups	This report captures users added to local groups.	1
65	PCI 10.x: Failed Router/Switch Admin Login	Failed router logons	1
66	PCI 10.x: Unix Password Changes	Tracks password changes on Unix Servers	1
67	PCI 10.x: Failed Unix Server Login	>Ranks Unix servers by the number of failed logins	1
68	PCI 1.x: Router Admin Activity Details	Provides details about router admin activity - logons, command executions and logoff	1
69	PCI 10.x: Successful VPN Admin Login	Provides event details for all successful VPN admin logons	1
70	PCI 5.x: Top IPs with Malware Found By IPS and Firewalls	Tracks IP addresses with Malware as found by IPS	1
71	PCI 10.x: Network Device Errors	Tracks errors reported by network device	1
72	PCI 10.x: Windows User Unlocks	This report details windows domain account lockouts	1
73	PCI 10.x: Top Unix Servers, Users By Successful Login	This report ranks linux servers and users by the number of successful logons	1
74	PCI 10.x: Successful Firewall Admin Login	Details about successful firewall logons	1
75	PCI 5.x: Top hosts with Malware found by Endpoint Protection	Captures hosts with malware found by host anti-virus solutions	1
76	PCI 5.x: 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
77	PCI 10.x: Windows Users Added To Global Groups	This report captures users added to global or univeral groups.	1
78	PCI 10.x: Failed Firewall Admin Login	Details about failed firewall logons	1
79	PCI 10.x: Application Down/Restart	Tracks application stop and start events	1

Rank	Report Name	Report Description	Count
80	PCI 1.x: Top Outbound Permitted Services By Connections, Bytes	Ranks firewalls and permitted outbound services by first the total number of connections and then by bytes for that service	1
81	PCI 1.x: Top Unauthorized Permitted Connections to DB DMZ By Connections, Bytes	Tracks the permitted connections involving DB DMZ. This assumes that there are certain protocols allowed between App DMZ and DB DMZ, and between Inside and DB DMZ. This report captures the traffic that violates these conditions.	1
82	PCI 5.x: Top Reporting Security Management Servers	Ranks Security Management Servers by events received	1
83	PCI 8.x: Server Password Changes	Tracks password changes	1
84	PCI 1.x: Top Permitted Connections Between Web DMZ and App DMZ By Connections, Bytes	Tracks the permitted connections between Web DMZ and App DMZ	1
85	PCI 10.x: Global Windows Groups Modified	This report captures global group modifications	1
86	PCI 1.x: Router Config Changes Detected From Log (g)	This report provides details about router config changes	1
87	PCI 10.x: Top Windows Servers By Failed Login	Ranks Windows Servers, Users, login failure types by the number of failed logins	1
88	PCI 10.x: Network Device Link Module Down/Up	Tracks network device miscellaneous module (e.g. fan, power etc.) down/up events	1
89	PCI 10.x: Windows Users Deleted From Local Groups	This report captures users deleted from local groups.	1
90	PCI 10.x: Server Down/Restart	Tracks server down and restart events	1
91	PCI 10.x: Top Windows Servers By Successful Login	This report ranks windows server logins by users and login types	1

1 Top Windows Servers By Failed Login



Rank	Reporting Device	User	Domain	Win Logon Fail Code String	COUNT(Matched Events)
1	THREATSOCDC	administrator	threatsoc		2,985
2	THREATSOCDC	administrator	threatsoc	0xc000006a	2,147
3	WIN2008-ADS	administrator	ACCELOPS	0xc000006a	184
4	SJ-Main-ASA.accelops.net	darryl.white	ACCELOPS	0xc0000072	108
5	WIN2008-ADS	Administrator	ACCELOPS.NET	0xc000006a	79
6	WIN2K8	Administrator	ACCELOPS.NET	0xc000006a	57
7	WIN2008-ADS	Administrator	accelops.net	0xc000006a	4
8	WIN2K8	administrator	ACCELOPS	0xc000006a	1

2 Domain Account Lock/Unlock History

Rank	Reporting Device	Event Receive Time	Event Name	User	Domain	Target User	Target Domain
1	WIN2008-ADS	7/30/19 12:30:03 PM	A user account was locked out	mike.richardson	ACCELOPS		
2	WIN2008-ADS	7/30/19 12:30:03 PM	A user account was locked out	tamera.leibtag	ACCELOPS		
3	WIN2008-ADS	7/30/19 12:30:03 PM	Windows user account unlocked				
4	WIN2008-ADS	7/30/19 12:30:03 PM	A user account was locked out	heather.biggs	ACCELOPS		
5	WIN2008-ADS	7/30/19 12:30:03 PM	Windows user account unlocked				
6	WIN2008-ADS	7/30/19 12:30:03 PM	A user account was locked out	archie.kuhn	ACCELOPS		

3 Global Windows Groups Modified

Rank	Reporting Device	Event Receive Time	User	Domain	Target User Group	Win Logon Id
1	THREATSOCDC	7/30/19 12:03:30 PM	administrator	THREATSOC	Domain Admins	0x16ed07
2	THREATSOCDC	7/30/19 12:03:25 PM	administrator	THREATSOC	Domain Admins	0x16ed07
3	THREATSOCDC	7/30/19 12:00:02 PM	administrator	THREATSOC	Domain Admins	0x41bf87
4	THREATSOCDC	7/30/19 12:00:02 PM	francis.underwood	THREATSOC	Domain Admins	0x44380a
5	THREATSOCDC	7/30/19 12:00:02 PM	francis.underwood	THREATSOC	Domain Admins	0x44380a
6	WIN2008-ADS	7/30/19 12:00:05 PM	mike.long	ACCELOPS	Domain Admins	0x34d03341
7	WIN2008-ADS	7/30/19 12:00:03 PM	administrator	ACCELOPS	Domain Admins	0x34ba494
8	WIN2008-ADS	7/30/19 12:00:01 PM	administrator	ACCELOPS	Domain Admins	0x34ba4794
9	WIN2008-ADS	7/30/19 12:00:01 PM	mike.long	ACCELOPS	Domain Admins	0x34d03341

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	7/30/19 12:00:02 PM	SJ-Main-Cat6500	192.168.20.1	Running config changed	81	82	enable secret 5 $1$3T2G$AhfZnnW58ird0lmOHea0M/;	(none)