nuSpective
straightforward · trustworthy · responsive

HIPAA Bundle

Report Start Time : Jul 23 2019, 09:32:27 AM EDT

Report End Time: Jul 23 2019, 10:32:26 AM EDT

Found Records 65

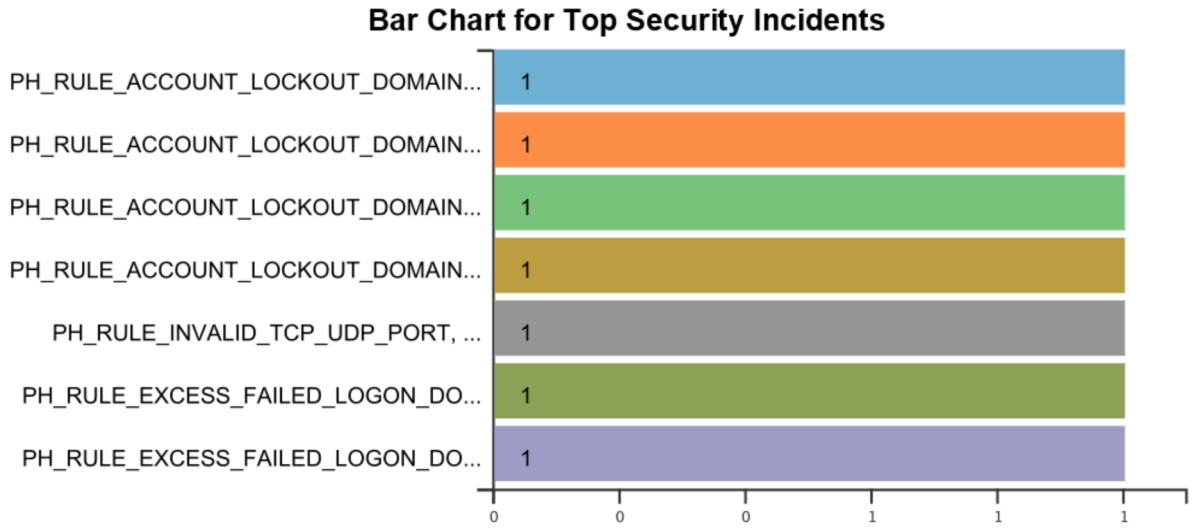
Rank	Report Name	Report Description	Count
1	HIPAA 164.308(a)(3): Local Windows Groups Modified	This report captures local group modifications	1
2	HIPAA 1.x: Top Firewalls and Permitted Uncommon Services By Connections, Bytes	Tracks uncommon services permitted by firewalls - common services include DNS, SMTP, Web	1
3	HIPAA 164.308(a)(4): Top Firewalls and 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
4	HIPAA 164.308(a)(6): Top Network Scanners By Event Count	Ranks the source IP addresses by detected network scan or reconnaissance events	1
5	HIPAA 164.312(a)(2): Failed Windows Domain Authentications	Captures failed domain authentications	1
6	HIPAA 164.308(a)(3),164.312(a)(2): Local Windows User Accounts Created	This report captures user accounts added on a server	1
7	HIPAA 164.308(a)(3): Users Added To Local Groups	This report captures users added to local groups.	1
8	HIPAA 164.308(a)(5): Server Password Changes	Tracks password changes	1
9	HIPAA 164.308(a)(6): Top Blocked Network Attacks By Count	Ranks the network attacks blocked by network IPS	1
10	HIPAA 164.308(a)(6): Top Network IPS events (affecting HIPAA devices) Ranked By Severity, Count	Ranks the network IPS events affecting HIPAA devices	1
11	HIPAA 164.308(a)(4),164.308(a)(5)(ii)(c): Unix Server Privileged Logon	This report details UNIX server privileged logon (su) details with all parsed parameters and raw logs	1
12	HIPAA 164.308(a)(6): Top hosts with Malware found by Host Antivirus	Captures hosts with malware found by host anti-virus solutions	1
13	HIPAA 164.312(a)(2): Successful VPN Logons	Captures successful VPN logons	1
14	HIPAA 164.308(a)(4),164.308(a)(5)(ii)(c),164.312(a)(2): Failed Unix Server Logons	This report details failed unix server logons with all parsed fields and raw logs	1
15	HIPAA 164.308(a)(3): Users Deleted From Local Groups	This report captures users deleted from local groups.	1
16	HIPAA 164.308(a)(4),164.308(a)(5)(ii)(c): Failed WLAN Admin Logon	Tracks failed admin logons to the WLAN Controller	1
17	HIPAA 164.312(a)(2): Failed Wireless Logons	Captures failed wireless logons	1
18	HIPAA 164.308(a)(4): Top Firewalls and 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

Rank	Report Name	Report Description	Count
19	HIPAA 164.308(a)(4),164.308(a)(5)(ii)(c),164.312(a)(2): Detailed Failed Login At HIPAA System	Captures detailed failed logins at any device or application - servers, network devices, domain controllers, VPN gateways, WLAN controllers and applications	1
20	HIPAA 164.308(a)(4),164.308(a)(5)(ii)(c): Failed Router Admin Logon Details	Details about failed router logons	1
21	HIPAA 164.308(a)(4),164.308(a)(5)(ii)(c): Failed VPN Admin Logon	Provides event details for all failed VPN admin logons	1
22	HIPAA 164.308(a)(3): Local Windows Groups Created	This report captures local group creations	1
23	HIPAA 164.308(a)(4): Router Run vs Startup Config Difference Via Login	This report captures detected differences between a routers running and startup config	1
24	HIPAA 164.308(a)(4),164.308(a)(5)(ii)(c): Privileged Windows Server Logon Attempts using the Administrator Account	This report details privileged logon attempts to a windows server using the Administrator account	1
25	HIPAA 164.308(a)(6): Spyware found but not remediated by Host Antivirus	Captures events that indicate Spyware found on a device Host Anti-virus solutions failed to remedy	1
26	HIPAA 164.312(b): All System Admin User Logon Attempts	Details all System Admin User Logon Attempts	1
27	HIPAA 164.308(a)(3): Users Added To Global Groups	This report captures users added to global or univeral groups.	1
28	HIPAA 164.308(a)(6): Virus found but not remediated by Host Antivirus	Captures events that indicate the viruses that Host Antivirus found but failed to remedy	1
29	HIPAA 164.312(a)(2): Successful Wireless Logons	Captures successful wireless logons	1
30	HIPAA 164.308(a)(6): 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
31	HIPAA 164.308(a)(4): Router 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
32	HIPAA 164.312(a)(2): Failed VPN Logons	Captures failed VPN logons	1
33	HIPAA 164.308(a)(4): Top Firewalls and Permitted High Port Services By Connections, Bytes	Tracks the high port services permitted by firewalls - these services may pose security risk	1
34	HIPAA 164.308(a)(3): Global Windows Groups Modified	This report captures global group modifications	1
35	HIPAA 164.308(a)(4),164.308(a)(5)(ii)(c),164.312(a)(2): Successful Unix Server Logons	This report details successful unix server logons with all parsed fields and raw logs	1
36	HIPAA 164.308(a)(3): Local Windows Groups Deleted	This report captures local group deletions	1
37	HIPAA 164.308(a)(3): Local Windows User Accounts Modified	This report captures local user account modifications.	1
38	HIPAA 164.308(a)(3): Users Deleted From Global Groups	This report captures users deleted from global or univeral groups.	1
39	HIPAA 164.308(a)(3): Global Windows Groups Created	This report captures global group creations	1

Rank	Report Name	Report Description	Count
40	HIPAA 164.308(a)(4): 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
41	HIPAA 164.312(b): System Operational Warnings	Detects System operational errors including license limits, down collector	1
42	HIPAA 164.312(b): Windows Audit Policy Changed	This report captures audit policy changes	1
43	HIPAA 164.308(a)(4),164.308(a)(5)(ii)(c): Successful Router Admin Logon Details	Details about successful router logons	1
44	HIPAA 164.308(a)(6): Top IPs with Malware Found By IPS and Firewalls	Tracks IP addresses with Malware as found by IPS	1
45	HIPAA 164.312(a)(2): Failed Database Server Logons	Captures failed database server logons	1
46	HIPAA 164.308(a)(3): Global Windows Groups Deleted	This report captures global group deletions	1
47	HIPAA 164.308(a)(4),164.308(a)(5)(ii)(c): Failed Firewall Admin Logon Details	Details about failed firewall logons	1
48	HIPAA 164.308(a)(4),164.308(a)(5)(ii)(c): Successful VPN Admin Logon	Provides event details for all successful VPN admin logons	1
49	HIPAA 164.308(a)(5)(ii)(c): Windows Server Account Unlocks	Captures account unlocks on windows servers. Account unlocks happen after lockouts that may happen on repeated login failures	1
50	HIPAA 164.308(a)(4),164.308(a)(5)(ii)(c),164.312(a)(2): Failed Windows Server Logons	This report reports failed windows servers logons	1
51	HIPAA 164.308(a)(4): Top Firewalls and 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
52	HIPAA 164.312(a)(2): Successful Database Server Logons	Captures successful database server logons	1
53	HIPAA 164.308(a)(3): Server Password Changes	Tracks password changes	1
54	HIPAA 164.308(a)(3): Local Windows User Accounts Deleted	This report captures user accounts removed from a server	1
55	HIPAA 164.308(a)(4),164.308(a)(5)(ii)(c): Unix Server Privileged Command Execution	This report details privilege command executions (sudo) at a Unix server	1
56	HIPAA 164.308(a)(4),164.308(a)(5)(ii)(c),164.312(a)(2): Detailed Successful Login At HIPAA Device	Captures detailed successful logins at any device or application including servers, network devices, domain controllers, VPN gateways, WLAN controllers and applications	1
57	HIPAA 164.308(a)(6): Top System detected Security Incidents (affecting HIPAA devices) Ranked By Severity, Count	Ranks the security related incidents by first their severity and then by their count - restricted to HIPAA devices	1
58	HIPAA 164.308(a)(4),164.308(a)(5)(ii)(c): Remote Desktop Connections to Windows Servers	This report details successful and failed remote desktop connections	1
59	HIPAA 164.308(a)(4): 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

Rank	Report Name	Report Description	Count
60	HIPAA 164.308(a)(4),164.308(a)(5)(ii)(c): Successful Firewall Admin Logon Details	Details about successful firewall logons	1
61	HIPAA 164.308(a)(4),164.308(a)(5)(ii)(c),164.312(a)(2): Successful Windows Server Logons	This report records successful windows server logons	1
62	HIPAA 10.x: Successful WLAN Admin Logon	Tracks successful admin logons to the WLAN Controller	1
63	HIPAA 164.312(a)(2): Successful Windows Domain Authentications	Captures successful domain authentications	1
64	HIPAA 164.308(a)(5)(ii)(c): 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
65	HIPAA 164.308(a)(6): 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

1 Top Security Incidents

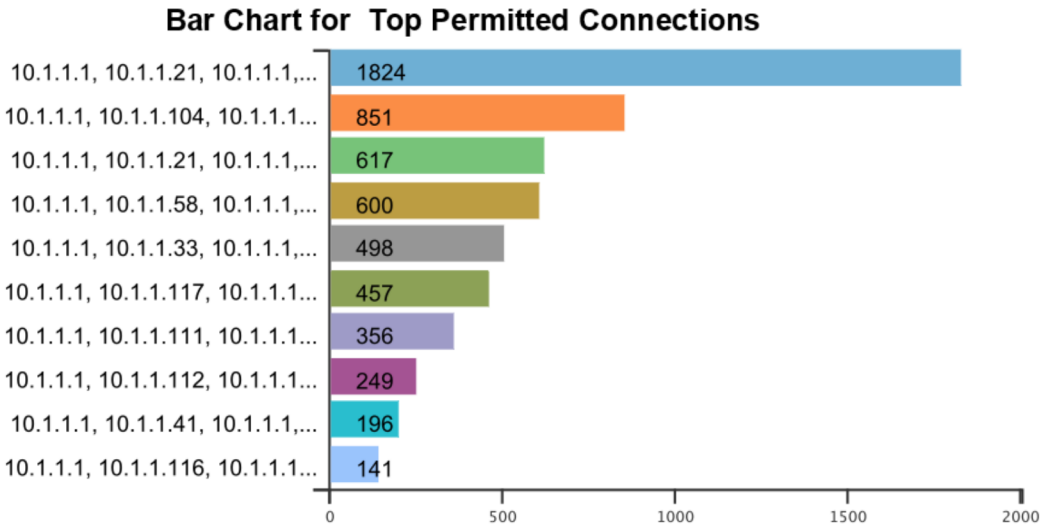


Rank	Event Name	Event Severity	Incident Source	Incident Target	COUNT(Matched Events)
1	Account Locked: Domain	10		destName:WIN2008-ADS, destIpAddr:192.168.0.10, user:archie.kuhn,	1
2	Account Locked: Domain	10		destName:WIN2008-ADS, destIpAddr:192.168.0.10, user:heather.biggs,	1
3	Account Locked: Domain	10		destName:WIN2008-ADS, destIpAddr:192.168.0.10, user:mike.richardson,	1
4	Account Locked: Domain	10		destName:WIN2008-ADS, destIpAddr:192.168.0.10, user:tamera.leibtag,	1
5	Invalid TCP/UDP Port Traffic	9	srcIpAddr:172.16.10.28,		1
6	Multiple Logon Failures: Domain	4	srcIpAddr:192.168.26.120,	destName:WIN2008-ADS, destIpAddr:192.168.0.10, domain:ACCELOPS.NET, user:sara.tanner@accelops .com,	1
7	Multiple Logon Failures: Domain	4	srcIpAddr:192.168.64.195,	destName:WIN2008-ADS, destIpAddr:192.168.0.10, domain:, user:Administrator,	1

2 Windows Account Lockout History

Rank	Event Receive Time	Event Name	Source IP	User	Domain
1	7/23/19 10:30:04 AM	A user account was locked out		tamera.leibtag	ACCELOPS
2	7/23/19 10:30:04 AM	A user account was locked out		mike.richardson	ACCELOPS
3	7/23/19 10:30:03 AM	A user account was locked out		heather.biggs	ACCELOPS
4	7/23/19 10:30:03 AM	A user account was locked out		archie.kuhn	ACCELOPS

3 Top Permitted Connections



Rank	Reporting IP	Source IP	Destination IP	IP Protocol	Destination TCP/UDP Port	COUNT(Matched Events)
1	10.1.1.1	10.1.1.21	10.1.1.1	17	161 (SNMP)	1,824
2	10.1.1.1	10.1.1.104	10.1.1.1	17	53 (DOMAIN)	851
3	10.1.1.1	10.1.1.21	10.1.1.1	17	53 (DOMAIN)	617
4	10.1.1.1	10.1.1.58	10.1.1.1	17	53 (DOMAIN)	600
5	10.1.1.1	10.1.1.33	10.1.1.1	17	53 (DOMAIN)	498
6	10.1.1.1	10.1.1.117	10.1.1.1	17	53 (DOMAIN)	457
7	10.1.1.1	10.1.1.111	10.1.1.1	17	53 (DOMAIN)	356
8	10.1.1.1	10.1.1.112	10.1.1.1	17	53 (DOMAIN)	249
9	10.1.1.1	10.1.1.41	10.1.1.1	17	53 (DOMAIN)	196
10	10.1.1.1	10.1.1.116	10.1.1.1	17	53 (DOMAIN)	141

4 Successful VPN Logons

Rank	Event Receive Time	Reporting IP	Source IP	User
1	7/23/19 9:32:25 AM	192.168.19.65	72.199.30.95	susan.davis
2	7/23/19 9:32:25 AM	192.168.19.65	71.65.237.148	ron.brown
3	7/23/19 9:32:30 AM	192.168.19.65	211.144.207.10	kevin.miller
4	7/23/19 9:32:30 AM	192.168.19.65	211.144.207.10	kevin.miller
5	7/23/19 9:32:43 AM	192.168.19.65	72.199.30.95	susan.davis
6	7/23/19 9:32:43 AM	192.168.19.65	71.65.237.148	ron.brown
7	7/23/19 9:33:02 AM	192.168.19.65	72.199.30.95	susan.davis
8	7/23/19 9:33:04 AM	192.168.19.65	218.28.58.94	jake.russell
9	7/23/19 9:33:05 AM	192.168.19.65	218.28.58.94	jake.russell
10	7/23/19 9:33:46 AM	192.168.19.65	71.65.237.148	ron.brown