nuSpective
straightforward · trustworthy · responsive

GLBA Bundle

Report Start Time : Jul 22 2019, 09:22:31 AM EDT

Report End Time: Jul 22 2019, 10:22:30 AM EDT

Found Records 69

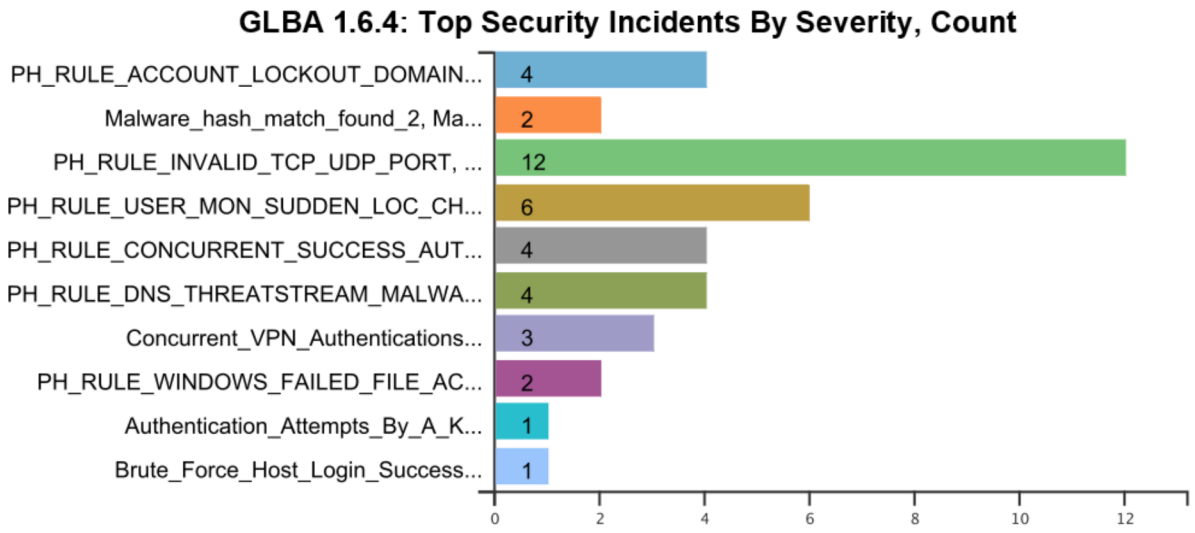
Rank	Report Name	Report Description	Count
1	GLBA 2.B.12,2.M.9: Top Inbound Blacklisted Mail Gateways By Connections	Ranks denied mail gateways by the number of attempted SMTP connections. The most common reason of denial is often the gateway being included in blacklists.	1
2	GLBA 2.C.8: Top hosts with Malware found by Host Antivirus	Captures hosts with malware found by host anti-virus solutions	1
3	GLBA 2.M.9: 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
4	GLBA 2.M.9: 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
5	GLBA 1.7.7: Windows Server Config Modification Details	This report captures the details of windows server configuration or policy modification events. Details include the administrative user, file/directory, the operation performed and the raw log	1
6	GLBA 2.A.2: Global Windows Groups Created	This report captures global group creations	1
7	GLBA 2.C.8: 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
8	GLBA 2.B.12,2.M.9: Filtered Outbound Spam Count	Counts total outbound spam denied by policy	1
9	GLBA 2.M.9: Phishing attempt found and remediated	Captures events that indicate phishing attempt	1
10	GLBA 2.A.4: Remote Desktop Connections to Windows Servers	This report details successful and failed remote desktop connections	1
11	GLBA 2.A.2: Local Windows Groups Modified	This report captures local group modifications	1
12	GLBA 2.B.12,2.M.9: Top Network Scanners By Event Count	Ranks the source IP addresses by detected network scan or reconnaissance events	1
13	GLBA 2.C.8: Top IPs with Malware Found By IPS and Firewalls	Tracks IP addresses with Malware as found by IPS	1
14	GLBA 2.C.8: 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

Rank	Report Name	Report Description	Count
15	GLBA 2.A.4: Successful Router Admin Logons	Details about successful router logons	1
16	GLBA 2.M.9: Virus 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
17	GLBA 2.A.4: Successful Firewall Admin Logons	Details about successful firewall logons	1
18	GLBA 2.B.12: Total Denied Web Connections By Policy	Counts denied web site connections because of policy violations	1
19	GLBA 2.A.2: Local Windows User Accounts Deleted	This report captures user accounts removed from a server	1
20	GLBA 2.B.12,2.M.9: 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
21	GLBA 2.C.17: Windows File Access Successes	This report captures the details of windows server file access successes. Details include the administrative user, file/directory, the operation performed.	1
22	GLBA 2.A.4: Privileged Domain Controller Logon Attempts using the Administrator Account	Ranks the windows servers and their users by the number of failed logons using the administrator account	1
23	GLBA 2.M.9: Host vulnerabilities found by scanners	This report details the host vulnerabilities found by scanners like Qyalys, Nessus, nCircle etc	1
24	GLBA 2.A.4,2.B.17: Successful WLAN Admin Logon	Tracks successful admin logons to the WLAN Controller	1
25	GLBA 2.B.12,2.M.9: 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
26	GLBA 2.B.12,2.M.9: Filtered Inbound Spam Count	Counts total inbound spam denied by spam filtering policy	1
27	GLBA 2.B.12: Top Mail Security Gateway Actions By Count	Ranks the actions taken by the mail security gateway - actions include blocking an inbound/outbound mail gateway because of RBL or other SMTP violations, blocking a mail because of spam or other policy violations and delivering a mail	1
28	GLBA 2.M.9: 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
29	GLBA 2.C.17: Windows Audit Policy Changes	This report captures audit policy changes	1
30	GLBA 1.7.7,2.C.9: 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
31	GLBA 2.B.12,2.M.9: Top Permitted High Port Services By Connections, Bytes	Tracks the high port services permitted by firewalls - these services may pose security risk	1

Rank	Report Name	Report Description	Count
32	GLBA 1.6.4: Top Security Incidents By Severity, Count	Ranks the security related incidents by first their severity and then by their count	1
33	GLBA 2.B.12,2.M.9: Top Outbound Blacklisted Mail Gateways By Connections	Ranks denied mail gateways by the number of attempted SMTP connections. The most common reason of denial is often the gateway being included in blacklists.	1
34	GLBA 2.A.2: Users Added To Local Groups	This report captures users added to local groups.	1
35	GLBA 2.B.12,2.M.9: Top Permitted Uncommon Services By Connections, Bytes	Tracks uncommon services permitted by firewalls - common services include DNS, SMTP, Web	1
36	GLBA 2.B.12,2.M.9: Top Blocked Outbound Connections By Count	Top Blocked Outbound Connections Ranked By Count	1
37	GLBA 2.A.2: Local Windows User Accounts Modified	This report captures local user account modifications.	1
38	GLBA 1.7.7: Firewall Configuration Changes	This report captures detected firewall configuration changes	1
39	GLBA 2.A.4,2.B.17: Failed WLAN Admin Logon	Tracks failed admin logons to the WLAN Controller	1
40	GLBA 2.M.9: 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
41	GLBA 1.7.7: Windows Domain Controller Config Changes	Provides detailed windows domain controller config changes	1
42	GLBA 1.7.7: Router Run vs Startup Configuration Difference	This report captures detected differences between a routers running and startup config	1
43	GLBA 2.A.4: Remote Desktop Connections to Domain Controller	Details successful remote desktop connections	1
44	GLBA 2.A.4,2.B.17: Failed VPN Admin Logon	Provides event details for all failed VPN admin logons	1
45	GLBA 2.B.12,2.M.9: 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
46	GLBA 2.A.2: Global Windows Groups Modified	This report captures global group modifications	1
47	GLBA 2.B.12: Top Network IPS events By Severity, Count	Ranks the network IPS events by count	1
48	GLBA 1.7.7,2.C.9: Windows File Access Failures	This report captures the details of windows server file access failures. Details include the administrative user, file/directory, the operation performed and the raw log	1
49	GLBA 2.A.4: Unix Server Privileged Command Execution	This report details privilege command executions (sudo) at a Unix server	1
50	GLBA 2.A.4,2.B.17: Successful VPN Admin Logon	Provides event details for all successful VPN admin logons	1
51	GLBA 2.B.12,2.M.9: Top Blocked Inbound Connections By Count	Top Inbound Denied Connections Ranked By Count	1

Rank	Report Name	Report Description	Count
52	GLBA 2.B.12.2.M.9: Top Inbound Blacklisted Mail Gateways and SMTP Error Types By Connections	Ranks denied mail gateways and the SMTP errors by the number of attempted connections. The most common SMTP error is often the gateway being included in mail blacklists.	1
53	GLBA 2.B.12.2.M.9: Top Blocked Network Attacks By Count	Ranks the network attacks blocked by network IPS	1
54	GLBA 2.B.12.2.M.9: Top Outbound Blacklisted Mail Gateways and SMTP Error Types By Connections	Ranks denied mail gateways and the SMTP errors by the number of attempted connections. The most common SMTP error is often the gateway being included in mail blacklists.	1
55	GLBA 2.M.9: 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
56	GLBA 2.A.2: Users Added To Global Groups	This report captures users added to global or univeral groups.	1
57	GLBA 1.7.7: Router/Switch Configuration Changes	This report captures detected startup or running config changes	1
58	GLBA 2.A.4: Detailed Successful Login At GLBA Device	Captures detailed successful logins at any device or application including servers, network devices, domain controllers, VPN gateways, WLAN controllers and applications	1
59	GLBA 2.A.2: Local Windows User Accounts Created	This report captures user accounts added on a server	1
60	GLBA 1.7.7: Firewall Run vs Startup Configuration Change	This report captures detected differences between a firewall's running and startup config	1
61	GLBA 2.A.2: Local Windows Groups Created	This report captures local group creations	1
62	GLBA 2.B.12.2.M.9: 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
63	GLBA 1.6.1: Top Reporting Modules Ranked By Event Rate	Ranks the reporting devices by events per second. This report shows the breadth of the devices from where security logs are collected.	1
64	GLBA 2.A.2: 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
65	GLBA 2.M.6: All Monitoring System Admin User Logon Attempts	Details all Monitoring System Admin User Logon Attempts	1
66	GLBA 2.A.4: Failed Firewall Admin Logons	Details about failed firewall logons	1
67	GLBA 2.A.4: Privileged Windows Server Logon Attempts using the Administrator Account	This report details privileged logon attempts to a windows server using the Administrator account	1
68	GLBA 2.A.4: Unix Server Privileged Logon	This report details UNIX server privileged logon (su) details with all parsed parameters and raw logs	1
69	GLBA 2.A.4: Failed Router Admin Logons	Details about failed router logons	1

1 Top Security Incidents



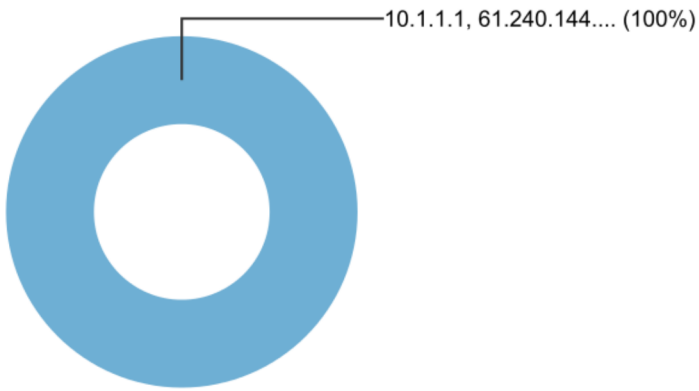
Rank	Event Name	Event Severity	COUNT(Matched Events)
1	Account Locked: Domain	10	4
2	Malware hash match found	10	2
3	Invalid TCP/UDP Port Traffic	9	12
4	Sudden User Location Change	9	6
5	Concurrent Successful Authentications To Same Account From Multiple Cities	9	4
6	DNS Traffic to Threat Stream Malware Domains	9	4
7	Concurrent VPN Authentications To Same Account From Different Countries	9	3
8	Windows failed file access	9	2
9	Authentication Attempts By A Known Host Scanner	9	1
10	Brute Force Host Login Success_Fixed	9	1

2 Windows Account Lock/Unlock History

Rank	Reporting Device	Event Receive Time	Event Name	User	Domain	Target User	Target Domain
1	WIN2008-ADS	7/22/19 9:30:04 AM	A user account was locked out	archie.kuhn	ACCELOPS		
2	WIN2008-ADS	7/22/19 9:30:04 AM	A user account was locked out	tamera.leibtag	ACCELOPS		
3	WIN2008-ADS	7/22/19 9:30:04 AM	A user account was locked out	mike.richardson	ACCELOPS		
4	WIN2008-ADS	7/22/19 9:30:04 AM	A user account was locked out	heather.biggs	ACCELOPS		
5	WIN2008-ADS	7/22/19 9:30:04 AM	Windows user account unlocked				
6	WIN2008-ADS	7/22/19 9:30:04 AM	Windows user account unlocked				

3 Top Blocked Inbound Connections

GLBA 2.B.12,2.M.9: Top Blocked Inbound Connections By Count



Rank	Reporting IP	Source IP	Source Host Name	Destination IP	Destination Host Name	IP Protocol	Destination TCP/UDP Port	COUNT(Matched Events)
1	10.1.1.1	61.240.144.67	61.240.144.67	10.1.1.35	ip72-207-68-83.sd.sd.cox.net	6	21 (FTP)	1

4 Windows File Access

Rank	Reporting Device	Reporting IP	User	Domain	Process Name	Object Name	OS Object Type	COUNT(Matched Events)
1	THREATSOCDC	10.1.1.33	THREATSOCDC$	THREATSOC	C:\Windows\System32\svchost.exe	PlugPlaySecurityObject	Security	5,622
2	WIN2008-ADS	192.168.0.10	WIN2008-ADS$	ACCELOPS	C:\Windows\System32\svchost.exe	PlugPlaySecurityObject	Security	1,435
3	THREATSOCDC	10.1.1.33	administrator	THREATSOC	C:\Windows\System32\svchost.exe	PlugPlaySecurityObject	Security	388
4	THREATSOCDC	10.1.1.33	administrator	THREATSOC	C:\Windows\System32\Oobe.exe	\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\WSMAN\Plugin\Microsoft.ServerManager	Key	118
5	THREATSOCDC	10.1.1.33	Administrator	THREATSOC	C:\Windows\System32\svchost.exe	PlugPlaySecurityObject	Security	42
6	THREATCTR	10.1.1.41	THREATCTR$	THREATSOC	C:\WINDOWS\system32\svchost.exe	C:\WINDOWS\Tasks\User_Feed_Synchronization-{5B8A7730-47C0-4956-BE1C-98189B9D40D0}.job	File	11
7	THREATCTR	10.1.1.41	THREATCTR$	THREATSOC	C:\WINDOWS\system32\services.exe	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\Eventlog\Security	Key	4
8	THREATSOCDC	10.1.1.33	THREATSOCDC$	THREATSOC	C:\Windows\System32\mcbuilder.exe	C:\Windows\rescache	File	4
9	THREATSOCDC	10.1.1.33	THREATSOCDC$	THREATSOC	C:\Windows\System32\mcbuilder.exe	C:\Windows\rescache\ResCache.mni	File	4
10	THREATSOCDC	10.1.1.33	THREATSOCDC$	THREATSOC	C:\Windows\servicing\TrustedInstaller.exe	C:\Windows\winsxs\Temp\PendingDeletes\$$DeleteMe.sortkey.nlp.01cfc8b8bfe3cf24.003c	File	4