tyler detect™
a total tyler solution

Daily Tyler Detect Report

Prepared for:

NCWSA

Activity For: Tuesday, 2021-02-09

tyler technologies
One Tyler Drive, Yarmouth, ME 04096
800.772.2260 | www.tylertech.com

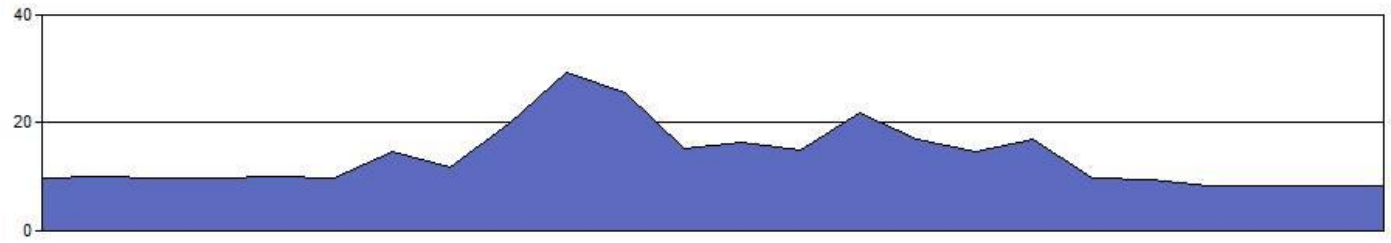
CONFIDENTIAL

Daily Metrics

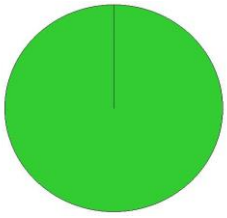
Tyler Detect Score[1]	Unanswered Questions	Unanswered Findings	Client Real-Time Alerts
100%	0	0	0
Average Client: 53%	**Average Client:** 2.47	**Average Client:** 12.22	

Firewall Events	Windows Events	Other Events	SOC Investigations[2]
120K	17.4K	193K	1
Average Client: 11.0M	**Average Client:** 1.08M	**Average Client:** 6.14M	

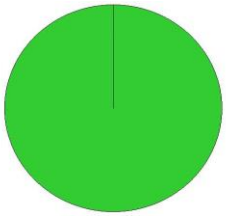
Events Received (in 000s)



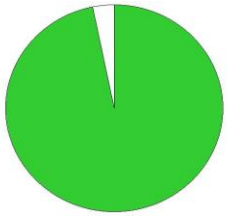
Reports 90-Day Status



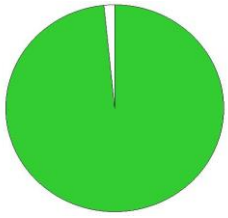
Windows Servers Status



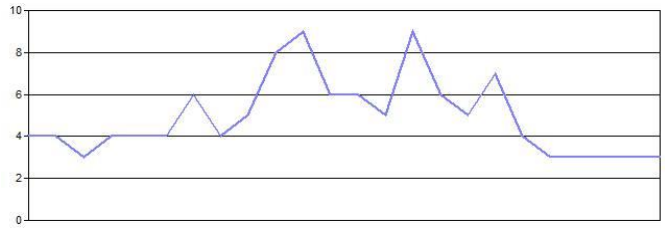
Endpoint Collection Status[3]



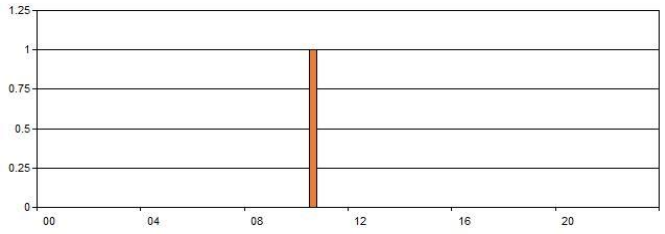
Sysmon Installs Status[3]



Firewall Events Received (in 000s)



Clients Alerts and SOC Investigations By Hour[4]



1 – "Tyler Detect Score" is an indicator of overall client interaction with the Tyler Detect service.
2 – "SOC Investigations" are events investigated in real-time that only go to clients if found to be malicious.
3 – Responded or confirmed in the past 7 days.
4 – Client Alerts are in blue and SOC Investigations are in orange.

Analyst: Multiple
Report Published By: Alan Roberge
Tyler Detect Specialist: Tynan Nida (800.772.2260 x 2335)
Data Received From NCWSA On: 2021-02-10
Date of Tyler Detect Report: 2021-02-10

Questions for Follow Up

Nothing to report.

Tyler Detect Findings

NCWSA-N-2021020901: One or more firewall administrative sessions were noted. More details about these appear in the 'Configuration Changes' field of the 'Firewall Logs' section of the report.

Recommendation: Research and document the cause of the firewall administrative session(s).

The following previously reported Tyler Detect Findings continue to occur:

Nothing to report.

Tyler Detect Findings not requiring portal posting:

Nothing to report.

Portal Activity:

User: tmc@ncwsa us
[Event]: Login [Time]: 15:30:30
[Event]: Report Access [Report Type]: TylerDetect [Report Date]: 2021-02-08 [Time]: 15:31:00

Table of Contents

Firewall Logs

Administration Events

Administrative Logons

10.0.0.1
User 'root' failed logon (1) via PORT from 10.0.0.69 at 01:43 noted.
User 'admin' logons (2) via HTTPS from 10.0.0.147 between 09:56 and 10:21 noted.
User 'tmc' logon (1) via CLI from 10.0.0.69 at 01:43 noted.

Configuration Changes

10.0.0.1
09:56:09-10:21:28: Configuration mode administration session started by 'admin' by admin from 10.0.0.147 via port '-' (2 entries)
10:15:06-10:27:00: Configuration mode administration session ended by 'admin' by admin from 10.0.0.147 via port '-' (2 entries)
10:15:06-10:27:00: GUI administration session ended by 'admin' by admin from 10.0.0.147 via port '-' (2 entries)

Traffic Events

NOTE: Potential malware infections are rated as 'Questionable', 'Suspicious', 'Potentially Infected' or 'Infected with confirmed command and control'.
Infected with confirmed command and control - We have confirmed that the noted device visited a known infectious URL and have also confirmed it is communicating with a command and control server.
Potentially Infected - We have confirmed that the noted device visited a known infectious URL and should be presumed compromised.
Suspicious - We have reviewed traffic from the noted device, and while known infectious pages were hit, the device is likely not at risk.
Questionable - We have reviewed traffic from the noted device, and concluded it is reasonable to believe that this was not intended end-user traffic of a questionable nature.

Potential Malware Infections

Nothing to report.

Secure Shell Connections

Nothing to report.

VPN Connections

Nothing to report.

Notable Inbound Traffic

Nothing to report.

Notable Outbound Traffic

Nothing to report.

Notable Local Traffic

Nothing to report.

NOTE: Outbound refers to traffic initiated by an internal device (i.e. employee web browsing) that is destined for the Internet. Inbound refers to traffic initiated by an external device (i.e. customer accessing your web server). Local refers to traffic initiated by an internal device and destined for an internal device.

Miscellaneous Events

Bandwidth Details

10.0.0.1
[Inbound]: < 1mb [Outbound]: 215mb [Local]: 1mb [Unknown]: 0mb [Total]: 216mb
10.10.0.1
[Inbound]: 0mb [Outbound]: 71mb [Local]: 0mb [Unknown]: 0mb [Total]: 71mb

Notable Denied Traffic

Nothing to report.

Miscellaneous

Nothing to report.

End Point Activity

Collection Results

Persistence Mechanism Detection: [Active Directory Computers Detected]: 62 [Computers Responding]: 56
Sysmon Installations: [Active Directory Computers Detected]: 62 [Computers Attempted]: 61 [Computers Confirmed]: 60

Analysis Results

Persistence Mechanisms: [Received]: 9862 [Analyzed]: 1,146 [Reported]: 0 [Malware]: 0

Potential Malware Infections

Nothing to report.

Potentially Unwanted Programs

Nothing to report.

New Medium Persistence Mechanisms

Nothing to report.

New Informational Persistence Mechanisms

--- AP1A ---
[Entry]: GoogleChromeElevationService [Category]: Services [Profile]: System-wide [Company]: Google LLC [Image]: elevation_service.exe
[Entry]: Google Chrome [Category]: Logon [Profile]: System-wide [Company]: Google LLC [Image]: chrmstp.exe
--- BILL2A ---
[Entry]: Sysmon [Category]: Services [Profile]: System-wide [Company]: Sysinternals - www.sysinternals.com [Image]: sysmon.exe
[Entry]: SysmonDrv [Category]: Drivers [Profile]: System-wide [Company]: Sysinternals - www.sysinternals.com [Image]: sysmondrv.sys
[Entry]: ScreenConnect Client (82ae8bdb9a11f68f) [Category]: Services [Profile]: System-wide [Company]: n/a [Image]: screenconnect.clientservice.exe
[Entry]: AdobeARMservice [Category]: Services [Profile]: System-wide [Company]: Adobe Inc. [Image]: armsvc.exe
[Entry]: \Adobe Acrobat Update Task [Category]: Tasks [Profile]: System-wide [Company]: Adobe Inc. [Image]: adobearm.exe
[Entry]: Adobe Reader Synchronizer [Category]: Logon [Profile]: NCWSA\sd [Company]: Adobe Systems Incorporated [Image]: adobecollabsync.exe
--- CC1 ---
[Entry]: Sysmon [Category]: Services [Profile]: System-wide [Company]: Sysinternals - www.sysinternals.com [Image]: sysmon.exe
[Entry]: SysmonDrv [Category]: Drivers [Profile]: System-wide [Company]: Sysinternals - www.sysinternals.com [Image]: sysmondrv.sys
--- CSR6A ---
[Entry]: GoogleChromeElevationService [Category]: Services [Profile]: System-wide [Company]: Google LLC [Image]: elevation_service.exe
[Entry]: Google Chrome [Category]: Logon [Profile]: System-wide [Company]: Google LLC [Image]: chrmstp.exe
[Entry]: AdobeARMservice [Category]: Services [Profile]: System-wide [Company]: Adobe Inc. [Image]: armsvc.exe
[Entry]: \Adobe Acrobat Update Task [Category]: Tasks [Profile]: System-wide [Company]: Adobe Inc. [Image]: adobearm.exe
--- CSR7A ---
[Entry]: GoogleChromeElevationService [Category]: Services [Profile]: System-wide [Company]: Google LLC [Image]: elevation_service.exe
[Entry]: Google Chrome [Category]: Logon [Profile]: System-wide [Company]: Google LLC [Image]: chrmstp.exe
--- CSR8 ---
[Entry]: GoogleChromeElevationService [Category]: Services [Profile]: System-wide [Company]: Google LLC [Image]: elevation_service.exe
[Entry]: Google Chrome [Category]: Logon [Profile]: System-wide [Company]: Google LLC [Image]: chrmstp.exe
--- CSSUP4 ---
[Entry]: GoogleChromeElevationService [Category]: Services [Profile]: System-wide [Company]: Google LLC [Image]: elevation_service.exe
[Entry]: Google Chrome [Category]: Logon [Profile]: System-wide [Company]: Google LLC [Image]: chrmstp.exe
[Entry]: GoogleChromeAutoLaunch_60742AB95EB07D411D33A5A2447399BA [Category]: Logon [Profile]: NCWSA\kw [Company]: Google LLC [Image]: chrome.exe
[Entry]: Application Restart #1 [Category]: Logon [Profile]: NCWSA\kw [Company]: Google LLC [Image]: chrome.exe
--- CSSUP5A ---
[Entry]: GoogleChromeElevationService [Category]: Services [Profile]: System-wide [Company]: Google LLC [Image]: elevation_service.exe
[Entry]: ScreenConnect Client (82ae8bdb9a11f68f) [Category]: Services [Profile]: System-wide [Company]: n/a [Image]: screenconnect.clientservice.exe
[Entry]: Google Chrome [Category]: Logon [Profile]: System-wide [Company]: Google LLC [Image]: chrmstp.exe
[Entry]: Sysmon [Category]: Services [Profile]: System-wide [Company]: Sysinternals - www.sysinternals.com [Image]: sysmon.exe

[Entry]: SysmonDrv [Category]: Drivers [Profile]: System-wide [Company]: Sysinternals - www.sysinternals.com [Image]: sysmondrv.sys
--- **DIRECT** ---
[Entry]: Application Restart #4 [Category]: Logon [Profile]: NCWSA\mah [Company]: Google LLC [Image]: chrome.exe
[Entry]: 0D063F18FAD5A1C53CC790652040E90287C6A2EC._service_run [Category]: Logon [Profile]: NCWSA\mah [Company]: Google LLC [Image]: chrome.exe
[Entry]: GoogleChromeElevationService [Category]: Services [Profile]: System-wide [Company]: Google LLC [Image]: elevation_service.exe
[Entry]: Google Chrome [Category]: Logon [Profile]: System-wide [Company]: Google LLC [Image]: chrmstp.exe
[Entry]: AdobeARMservice [Category]: Services [Profile]: System-wide [Company]: Adobe Inc. [Image]: armsvc.exe
[Entry]: \Adobe Acrobat Update Task [Category]: Tasks [Profile]: System-wide [Company]: Adobe Inc. [Image]: adobearm.exe
--- **ENG1A** ---
[Entry]: GoogleChromeElevationService [Category]: Services [Profile]: System-wide [Company]: Google LLC [Image]: elevation_service.exe
[Entry]: Google Chrome [Category]: Logon [Profile]: System-wide [Company]: Google LLC [Image]: chrmstp.exe
--- **ENGLT** ---
[Entry]: \Agent Activation Runtime\S-1-5-21-1643497915-630510821-2581511069-3616 [Category]: Tasks [Profile]: System-wide [Company]: n/a [Image]: agentactivationruntimestarter.exe
[Entry]: GoogleChromeElevationService [Category]: Services [Profile]: System-wide [Company]: Google LLC [Image]: elevation_service.exe
[Entry]: Google Chrome [Category]: Logon [Profile]: System-wide [Company]: Google LLC [Image]: chrmstp.exe
--- **FIN1** ---
[Entry]: GoogleChromeElevationService [Category]: Services [Profile]: System-wide [Company]: Google LLC [Image]: elevation_service.exe
[Entry]: Google Chrome [Category]: Logon [Profile]: System-wide [Company]: Google LLC [Image]: chrmstp.exe
--- **GIS3** ---
[Entry]: GoogleChromeElevationService [Category]: Services [Profile]: System-wide [Company]: Google LLC [Image]: elevation_service.exe
[Entry]: Google Chrome [Category]: Logon [Profile]: System-wide [Company]: Google LLC [Image]: chrmstp.exe
--- **GIS4** ---
[Entry]: GoogleChromeElevationService [Category]: Services [Profile]: System-wide [Company]: Google LLC [Image]: elevation_service.exe
[Entry]: Google Chrome [Category]: Logon [Profile]: System-wide [Company]: Google LLC [Image]: chrmstp.exe
--- **HR1** ---
[Entry]: AdobeARMservice [Category]: Services [Profile]: System-wide [Company]: Adobe Inc. [Image]: armsvc.exe
[Entry]: \Adobe Acrobat Update Task [Category]: Tasks [Profile]: System-wide [Company]: Adobe Inc. [Image]: adobearm.exe
[Entry]: Application Restart #5 [Category]: Logon [Profile]: NCWSA\tc [Company]: Google LLC [Image]: chrome.exe
[Entry]: GoogleChromeElevationService [Category]: Services [Profile]: System-wide [Company]: Google LLC [Image]: elevation_service.exe
[Entry]: Google Chrome [Category]: Logon [Profile]: System-wide [Company]: Google LLC [Image]: chrmstp.exe
--- **IT** ---
[Entry]: AdobeARMservice [Category]: Services [Profile]: System-wide [Company]: Adobe Inc. [Image]: armsvc.exe
[Entry]: \Adobe Acrobat Update Task [Category]: Tasks [Profile]: System-wide [Company]: Adobe Inc. [Image]: adobearm.exe
[Entry]: Application Restart #0 [Category]: Logon [Profile]: NCWSA\tmc [Company]: Google LLC [Image]: chrome.exe
--- **IT123** ---
[Entry]: Acrobat PDFMaker Office COM Addin [Category]: Office Addins [Profile]: System-wide [Company]: Adobe Systems Incorporated [Image]: pdfmofficeaddin.dll
[Entry]: GoogleChromeElevationService [Category]: Services [Profile]: System-wide [Company]: Google LLC [Image]: elevation_service.exe
[Entry]: Google Chrome [Category]: Logon [Profile]: System-wide [Company]: Google LLC [Image]: chrmstp.exe
[Entry]: Acrobat PDFMaker Office COM Addin [Category]: Office Addins [Profile]: System-wide [Company]: Adobe Systems Incorporated [Image]: pdfmofficeaddin.dll
[Entry]: Acrobat PDFMaker Office COM Addin [Category]: Office Addins [Profile]: System-wide [Company]: Adobe Systems Incorporated [Image]: pdfmofficeaddin.dll
[Entry]: AdobeARMservice [Category]: Services [Profile]: System-wide [Company]: Adobe Inc. [Image]: armsvc.exe
[Entry]: \Adobe Acrobat Update Task [Category]: Tasks [Profile]: System-wide [Company]: Adobe Inc. [Image]: adobearm.exe
[Entry]: Acrobat PDFMaker Office COM Addin [Category]: Office Addins [Profile]: System-wide [Company]: Adobe Systems Incorporated [Image]: pdfmoutlookaddin.dll
[Entry]: Acrobat PDFMaker Office COM Addin [Category]: Office Addins [Profile]: System-wide [Company]: Adobe Systems Incorporated [Image]: pdfmoutlookaddin.dll
[Entry]: Acrobat PDFMaker Office COM Addin [Category]: Office Addins [Profile]: System-wide [Company]: Adobe Systems Incorporated [Image]: pdfmofficeaddin.dll
[Entry]: Acrobat PDFMaker Office COM Addin [Category]: Office Addins [Profile]: System-wide [Company]: Adobe Systems Incorporated [Image]: pdfmofficeaddin.dll
[Entry]: Acrobat PDFMaker Office COM Addin [Category]: Office Addins [Profile]: System-wide [Company]: Adobe Systems Incorporated [Image]: pdfmofficeaddin.dll
[Entry]: Acrobat PDFMaker Office COM Addin [Category]: Office Addins [Profile]: System-wide [Company]: Adobe Systems Incorporated [Image]: pdfmofficeaddin.dll
[Entry]: Acrobat PDFMaker Office COM Addin [Category]: Office Addins [Profile]: System-wide [Company]: Adobe Systems Incorporated [Image]: pdfmofficeaddin.dll
[Entry]: Acrobat PDFMaker Office COM Addin [Category]: Office Addins [Profile]: System-wide [Company]: Adobe Systems Incorporated [Image]: pdfmofficeaddin.dll
[Entry]: Acrobat Assistant 8.0 [Category]: Logon [Profile]: System-wide [Company]: Adobe Systems Inc. [Image]: acrotray.exe
[Entry]: Acrobat PDFMaker Office COM Addin [Category]: Office Addins [Profile]: NT AUTHORITY\SYSTEM [Company]: Adobe Systems Incorporated [Image]:

pdfmoutlookaddin.dll
--- IT2 ---
[Entry]: EPMVolFl [Category]: Drivers [Profile]: System-wide [Company]: Windows (R) Codename Longhorn DDK provider [Image]: epmvolfl.sys
[Entry]: Application Restart #1 [Category]: Logon [Profile]: NCWSA\tmc [Company]: Google LLC [Image]: chrome.exe
--- MAINT4 ---
[Entry]: AdobeARMservice [Category]: Services [Profile]: System-wide [Company]: Adobe Inc. [Image]: armsvc.exe
[Entry]: \Adobe Acrobat Update Task [Category]: Tasks [Profile]: System-wide [Company]: Adobe Inc. [Image]: adobearm.exe
--- MAINT6 ---
[Entry]: GoogleChromeElevationService [Category]: Services [Profile]: System-wide [Company]: Google LLC [Image]: elevation_service.exe
[Entry]: Google Chrome [Category]: Logon [Profile]: System-wide [Company]: Google LLC [Image]: chrmstp.exe
--- MAINTMAN ---
[Entry]: 3ware [Category]: Drivers [Profile]: System-wide [Company]: LSI [Image]: 3ware.sys
[Entry]: ADP80XX [Category]: Drivers [Profile]: System-wide [Company]: PMC-Sierra [Image]: adp80xx.sys
[Entry]: amdi2c [Category]: Drivers [Profile]: System-wide [Company]: Advanced Micro Devices~^~ Inc [Image]: amdi2c.sys
[Entry]: amdsata [Category]: Drivers [Profile]: System-wide [Company]: Advanced Micro Devices [Image]: amdsata.sys
[Entry]: amdsbs [Category]: Drivers [Profile]: System-wide [Company]: AMD Technologies Inc. [Image]: amdsbs.sys
[Entry]: amdxata [Category]: Drivers [Profile]: System-wide [Company]: Advanced Micro Devices [Image]: amdxata.sys
[Entry]: arcsas [Category]: Drivers [Profile]: System-wide [Company]: PMC-Sierra~^~ Inc. [Image]: arcsas.sys
[Entry]: b06bdrv [Category]: Drivers [Profile]: System-wide [Company]: QLogic Corporation [Image]: bxvbda.sys
[Entry]: cht4iscsi [Category]: Drivers [Profile]: System-wide [Company]: Chelsio Communications [Image]: cht4sx64.sys
[Entry]: cht4vbd [Category]: Drivers [Profile]: System-wide [Company]: Chelsio Communications [Image]: cht4vx64.sys
[Entry]: CimFS [Category]: Drivers [Profile]: System-wide [Company]: n/a [Image]: cimfs.sys
[Entry]: ebdrv [Category]: Drivers [Profile]: System-wide [Company]: QLogic Corporation [Image]: evbda.sys
[Entry]: HpSAMD [Category]: Drivers [Profile]: System-wide [Company]: Hewlett-Packard Company [Image]: hpsamd.sys
[Entry]: iaLPSS2i_I2C_CNL [Category]: Drivers [Profile]: System-wide [Company]: Intel Corporation [Image]: ialpss2i_i2c_cnl.sys
[Entry]: iaStorAVC [Category]: Drivers [Profile]: System-wide [Company]: Intel Corporation [Image]: iastoravc.sys
[Entry]: iaStorV [Category]: Drivers [Profile]: System-wide [Company]: Intel Corporation [Image]: iastorv.sys
[Entry]: ibbus [Category]: Drivers [Profile]: System-wide [Company]: Mellanox [Image]: ibbus.sys
[Entry]: ItSas35i [Category]: Drivers [Profile]: System-wide [Company]: Avago Technologies [Image]: itsas35i.sys
[Entry]: LSI_SAS [Category]: Drivers [Profile]: System-wide [Company]: LSI Corporation [Image]: lsi_sas.sys
[Entry]: LSI_SAS2i [Category]: Drivers [Profile]: System-wide [Company]: LSI Corporation [Image]: lsi_sas2i.sys
[Entry]: LSI_SAS3i [Category]: Drivers [Profile]: System-wide [Company]: Avago Technologies [Image]: lsi_sas3i.sys
[Entry]: LSI_SSS [Category]: Drivers [Profile]: System-wide [Company]: LSI Corporation [Image]: lsi_sss.sys
[Entry]: megasas [Category]: Drivers [Profile]: System-wide [Company]: Avago Technologies [Image]: megasas.sys
[Entry]: megasas2i [Category]: Drivers [Profile]: System-wide [Company]: Avago Technologies [Image]: megasas2i.sys
[Entry]: megasas35i [Category]: Drivers [Profile]: System-wide [Company]: Avago Technologies [Image]: megasas35i.sys
[Entry]: megasr [Category]: Drivers [Profile]: System-wide [Company]: LSI Corporation~^~ Inc. [Image]: megasr.sys
[Entry]: mlx4_bus [Category]: Drivers [Profile]: System-wide [Company]: Mellanox [Image]: mlx4_bus.sys
[Entry]: mvumis [Category]: Drivers [Profile]: System-wide [Company]: Marvell Semiconductor~^~ Inc. [Image]: mvumis.sys
[Entry]: ndfltr [Category]: Drivers [Profile]: System-wide [Company]: Mellanox [Image]: ndfltr.sys
[Entry]: nvraid [Category]: Drivers [Profile]: System-wide [Company]: NVIDIA Corporation [Image]: nvraid.sys
[Entry]: nvstor [Category]: Drivers [Profile]: System-wide [Company]: NVIDIA Corporation [Image]: nvstor.sys
[Entry]: percsas2i [Category]: Drivers [Profile]: System-wide [Company]: Avago Technologies [Image]: percsas2i.sys
[Entry]: percsas3i [Category]: Drivers [Profile]: System-wide [Company]: Avago Technologies [Image]: percsas3i.sys
[Entry]: SiSRaid2 [Category]: Drivers [Profile]: System-wide [Company]: Silicon Integrated Systems Corp. [Image]: sisraid2.sys
[Entry]: SiSRaid4 [Category]: Drivers [Profile]: System-wide [Company]: Silicon Integrated Systems [Image]: sisraid4.sys
[Entry]: SmartSAMD [Category]: Drivers [Profile]: System-wide [Company]: Microsemi Corportation [Image]: smartsamd.sys
[Entry]: stexstor [Category]: Drivers [Profile]: System-wide [Company]: Promise Technology~^~ Inc. [Image]: stexstor.sys
[Entry]: vsmraid [Category]: Drivers [Profile]: System-wide [Company]: VIA Technologies Inc.~^~Ltd [Image]: vsmraid.sys
[Entry]: VSTXRAID [Category]: Drivers [Profile]: System-wide [Company]: VIA Corporation [Image]: vstxraid.sys
[Entry]: WinMad [Category]: Drivers [Profile]: System-wide [Company]: Mellanox [Image]: winmad.sys
[Entry]: WinVerbs [Category]: Drivers [Profile]: System-wide [Company]: Mellanox [Image]: winverbs.sys
[Entry]: \Microsoft\Windows\HelloFace\FODCleanupTask [Category]: Tasks [Profile]: System-wide [Company]: n/a [Image]: facefoduninstaller.exe
[Entry]: \Microsoft\Windows\NetTrace\GatherNetworkInfo [Category]: Tasks [Profile]: System-wide [Company]: n/a [Image]: gathernetworkinfo.vbs
[Entry]: msacm.l3acm [Category]: Codecs [Profile]: System-wide [Company]: Fraunhofer Institut Integrierte Schaltungen IIS [Image]: l3codeca.acm
[Entry]: vidc.cvid [Category]: Codecs [Profile]: System-wide [Company]: Radius Inc. [Image]: iccvid.dll
[Entry]: msacm.l3acm [Category]: Codecs [Profile]: System-wide [Company]: Fraunhofer Institut Integrierte Schaltungen IIS [Image]: l3codeca.acm
[Entry]: Application Restart #2 [Category]: Logon [Profile]: NCWSA\mw [Company]: Google LLC [Image]: chrome.exe
--- TEMPUS2 ---
[Entry]: GoogleChromeElevationService [Category]: Services [Profile]: System-wide [Company]: Google LLC [Image]: elevation_service.exe
[Entry]: Google Chrome [Category]: Logon [Profile]: System-wide [Company]: Google LLC [Image]: chrmstp.exe
--- TYLERDETECT ---
[Entry]: GoogleChromeElevationService [Category]: Services [Profile]: System-wide [Company]: Google LLC [Image]: elevation_service.exe
[Entry]: Google Chrome [Category]: Logon [Profile]: System-wide [Company]: Google LLC [Image]: chrmstp.exe

--- WH1 ---
[Entry]: AdobeARMservice [Category]: Services [Profile]: System-wide [Company]: Adobe Inc. [Image]: armsvc.exe
[Entry]: \Adobe Acrobat Update Task [Category]: Tasks [Profile]: System-wide [Company]: Adobe Inc. [Image]: adobearm.exe
--- WH2 ---
[Entry]: AdobeARMservice [Category]: Services [Profile]: System-wide [Company]: Adobe Inc. [Image]: armsvc.exe
[Entry]: \Adobe Acrobat Update Task [Category]: Tasks [Profile]: System-wide [Company]: Adobe Inc. [Image]: adobearm.exe
--- YRWRD1A ---
[Entry]: GoogleChromeElevationService [Category]: Services [Profile]: System-wide [Company]: Google LLC [Image]: elevation_service.exe
[Entry]: Google Chrome [Category]: Logon [Profile]: System-wide [Company]: Google LLC [Image]: chrmstp.exe
[Entry]: GoogleChromeAutoLaunch_C622CFBF497C394974C0996CD3A6F4F9 [Category]: Logon [Profile]: NCWSA\km [Company]: Google LLC [Image]: chrome.exe
[Entry]: Application Restart #2 [Category]: Logon [Profile]: NCWSA\km [Company]: Google LLC [Image]: chrome.exe
--- YRWRD2A ---
[Entry]: AdobeARMservice [Category]: Services [Profile]: System-wide [Company]: Adobe Inc. [Image]: armsvc.exe
[Entry]: \Adobe Acrobat Update Task [Category]: Tasks [Profile]: System-wide [Company]: Adobe Inc. [Image]: adobearm.exe
--- YRWRD5A ---
[Entry]: AdobeARMservice [Category]: Services [Profile]: System-wide [Company]: Adobe Inc. [Image]: armsvc.exe
[Entry]: \Adobe Acrobat Update Task [Category]: Tasks [Profile]: System-wide [Company]: Adobe Inc. [Image]: adobearm.exe
--- YRWRD6A ---
[Entry]: GoogleChromeElevationService [Category]: Services [Profile]: System-wide [Company]: Google LLC [Image]: elevation_service.exe
[Entry]: Google Chrome [Category]: Logon [Profile]: System-wide [Company]: Google LLC [Image]: chrmstp.exe
[Entry]: Application Restart #0 [Category]: Logon [Profile]: NCWSA\pm [Company]: Google LLC [Image]: chrome.exe
--- YRWRD8 ---
[Entry]: GoogleChromeElevationService [Category]: Services [Profile]: System-wide [Company]: Google LLC [Image]: elevation_service.exe
[Entry]: Google Chrome [Category]: Logon [Profile]: System-wide [Company]: Google LLC [Image]: chrmstp.exe

*Note: Generally, the items above will only be the **first** devices seen with a specific persistence mechanism in your environment.*

End Point Workstation Logs

Workstation RDP Sessions

Device: WORKSTATIONS
-- Event ID: 4624 - Successful Logon (8) --
[Device]: BILL2A [Acct]: NCWSA\tmc [Src]: 10.0.0.147 [First]: 07:49:45 [Last]: 07:54:54 [Qty]: 4

Workstation User Management

Nothing to report.

Workstation Group Management

Nothing to report.

Workstation Account Lockouts

Nothing to report.

Workstation Password Changes

Nothing to report.

End Point Workstation Logs

'Routine' Events

Workstation RDP Sessions

Nothing to report.

Workstation User Management

Device: WORKSTATIONS
-- Event ID: 4648 - A Logon Was Attempted Using Explicit Credentials (8) --
[Device]: SPICEWORKS [Acct]: NCWSA\tmc (Tim McCart) [Credentials Used]: NCWSA\administrator [Target Device]: FC300 [Process Name]:
C:\Windows\System32\svchost.exe [First]: 01:16:08 [Last]: 01:16:21 [Qty]: 6
[Device]: SPICEWORKS [Acct]: NCWSA\tmc (Tim McCart) [Credentials Used]: NCWSA\administrator [Target Device]: HH1 [Process Name]:
C:\Windows\System32\svchost.exe [First]: 01:10:41 [Last]: 01:10:44 [Qty]: 3
[Device]: SPICEWORKS [Acct]: NCWSA\tmc (Tim McCart) [Credentials Used]: NCWSA\administrator [Target Device]: HH2 [Process Name]:
C:\Windows\System32\svchost.exe [First]: 01:08:12 [Last]: 01:08:15 [Qty]: 3
[Device]: SPICEWORKS [Acct]: NCWSA\tmc (Tim McCart) [Credentials Used]: NCWSA\administrator [Target Device]: HH3 [Process Name]:
C:\Windows\System32\svchost.exe [First]: 01:05:11 [Last]: 01:05:14 [Qty]: 3
[Device]: SPICEWORKS [Acct]: NCWSA\tmc (Tim McCart) [Credentials Used]: NCWSA\administrator [Target Device]: NCWSASRV.NCWSA.COM [Process Name]:
C:\Windows\System32\svchost.exe [Time]: 00:44:23
[Device]: SPICEWORKS [Acct]: NCWSA\tmc (Tim McCart) [Credentials Used]: NCWSA\administrator [Target Device]: YRWWTP-WS-1 [Process Name]:
C:\Windows\System32\svchost.exe [First]: 00:14:54 [Last]: 00:14:55 [Qty]: 2

Workstation Group Management

Nothing to report.

Workstation Account Lockouts

Nothing to report.

Workstation Password Changes

Nothing to report.

Windows Security Event Logs

Administration Events

Administrative Interactive Logons

Nothing to report.

User Management

Nothing to report.

Group Management

Nothing to report.

Computer Management

Active Directory Domain: NCWSA

-- Event ID: 4742 - Computer Account Changed --

[Acct]: NCWSA\SCHEDULER$ [Service Principal Names]: HOST/scheduler.ncwsa.local RestrictedKrbHost/scheduler.ncwsa.local HOST/SCHEDULER RestrictedKrbHost/SCHEDULER TERMSRV/scheduler.ncwsa.local TERMSRV/SCHEDULER [Admin]: NCWSA\SCHEDULER$ [Time]: 17:34:24

[Acct]: NCWSA\SCHEDULER$ [Service Principal Names]: HOST/scheduler.ncwsa.local RestrictedKrbHost/scheduler.ncwsa.local HOST/SCHEDULER RestrictedKrbHost/SCHEDULER TERMSRV/scheduler.ncwsa.local TERMSRV/SCHEDULER AcronisAgent/scheduler.ncwsa.local [Admin]: NCWSA\SCHEDULER$ [Time]: 17:35:04

[Acct]: NCWSA\SPICEWORKS$ [Service Principal Names]: HOST/SPICEWORKS RestrictedKrbHost/SPICEWORKS TERMSRV/SPICEWORKS HOST/spiceworks.ncwsa.local RestrictedKrbHost/spiceworks.ncwsa.local TERMSRV/spiceworks.ncwsa.local [Admin]: NCWSA\SPICEWORKS$ [Time]: 18:37:23

[Acct]: NCWSA\SPICEWORKS$ [Service Principal Names]: HOST/SPICEWORKS RestrictedKrbHost/SPICEWORKS TERMSRV/SPICEWORKS HOST/spiceworks.ncwsa.local RestrictedKrbHost/spiceworks.ncwsa.local TERMSRV/spiceworks.ncwsa.local AcronisAgent/spiceworks.ncwsa.local [Admin]: NCWSA\SPICEWORKS$ [Time]: 18:37:55

Device: CMS2

-- Event ID: 4697 - Service Install Attempt --

[Admin]: NCWSA\CMS2$ [Service]: MpKsl12973b3b (C:\ProgramData\Microsoft\Windows Defender\Definition Updates\{C7C61738-E992-4AC8-A540-4CECA7C65B6D}\MpKslDrv.sys) [Type]: Kernel Driver [Startup]: Demand [Acct]: LocalSystem [Time]: 09:55:17

Device: DOS

-- Event ID: 4697 - Service Install Attempt --

[Admin]: NCWSA\DOS$ [Service]: MpKsld31ebd76 (C:\ProgramData\Microsoft\Windows Defender\Definition Updates\{BFB1A046-5826-4983-8488-7AED77E09A00}\MpKslDrv.sys) [Type]: Kernel Driver [Startup]: Demand [Acct]: LocalSystem [Time]: 12:46:47

Device: SW-HCA-VM1

-- Event ID: 4697 - Service Install Attempt --

[Admin]: NCWSA\SW-HCA-VM1$ [Service]: MpKsl29d36ee5 (C:\ProgramData\Microsoft\Windows Defender\Definition Updates\{41912FCD-5396-4FB0-99AA-51927C2B19BA}\MpKslDrv.sys) [Type]: Kernel Driver [Startup]: Demand [Acct]: LocalSystem [Time]: 12:21:18

Device: SW-HCA-VM2

-- Event ID: 4697 - Service Install Attempt --

[Admin]: NCWSA\SW-HCA-VM2$ [Service]: MpKsl052e3c1c (C:\ProgramData\Microsoft\Windows Defender\Definition Updates\{081CDFFC-2CA0-4167-AD3B-C2ADEC1DD7AE}\MpKslDrv.sys) [Type]: Kernel Driver [Startup]: Demand [Acct]: LocalSystem [Time]: 12:45:39

Device: TRES

-- Event ID: 4697 - Service Install Attempt --

[Admin]: NCWSA\TRES$ [Service]: MpKslc4ae398f (C:\ProgramData\Microsoft\Windows Defender\Definition Updates\{1B709D74-E87F-4FF4-AB37-CCD3CF65A4BD}\MpKslDrv.sys) [Type]: Kernel Driver [Startup]: Demand [Acct]: LocalSystem [Time]: 03:12:19

Device: TYLERDETECT

-- Event ID: 4697 - Service Install Attempt --

[Admin]: NCWSA\TYLERDETECT$ [Service]: MpKsl8d40e839 (C:\ProgramData\Microsoft\Windows Defender\Definition Updates\{5219BEF5-14CD-4A96-9C3B-30DF2B096CF8}\MpKslDrv.sys) [Type]: Kernel Driver [Startup]: Demand [Acct]: LocalSystem [Time]: 14:57:41

Group Policy Object Management

Nothing to report.

Organizational Unit Management

Nothing to report.

Share Management

Nothing to report.

File/Folder Management

Nothing to report.

User Events

Account Lockouts

Nothing to report.

Invalid Passwords

Nothing to report.

Password Changes

Nothing to report.

Logon Restrictions

Nothing to report.

Invalid Logon Type

Nothing to report.

Invalid Account Logons

Nothing to report.

Miscellaneous Events

Server Reboots

Nothing to report.

Miscellaneous

Nothing to report.

Windows Logs Additional Reporting

Service Management

Nothing to report.

Windows Update Service

Nothing to report.

Software Management

Nothing to report.

Server Reboot Comments

Nothing to report.

Windows Security Event Logs

'Routine' Events

Administration Events

Administrative Interactive Logons

Nothing to report.

User Management

Nothing to report.

Group Management

Nothing to report.

Computer Management

Nothing to report.

Group Policy Object Management

Nothing to report.

Organizational Unit Management

Nothing to report.

Share Management

Nothing to report.

File/Folder Management

Nothing to report.

User Events

Account Lockouts

Nothing to report.

Invalid Passwords

Active Directory Domain: NCWSA
-- Administrative/Service Accounts --
-- Event ID: 4771 - Pre-authentication Failed (Failure) --
[Acct]: NCWSA\administrator [Src]: 10.0.0.3 [First]: 01:13:57 [Last]: 02:07:40 [Qty]: 48
[Acct]: NCWSA\administrator [Src]: 10.0.0.69 [First]: 01:13:57 [Last]: 02:07:40 [Qty]: 48
[Acct]: NCWSA\mah (Mike Hopkins) [Src]: 10.0.0.72 [Time]: 05:35:04
-- Other Accounts --
Nothing to report.

Password Changes

Nothing to report.

Logon Restrictions

Nothing to report.

Invalid Logon Type

Nothing to report.

Invalid Account Logons

Nothing to report.

Miscellaneous Events

Server Reboots

Nothing to report.

Miscellaneous

Nothing to report.

'Routine' events are those events which have happened at least 3 times in the past 7 days, or happened on the same day of the week the previous two weeks. Events can also be moved to the 'Routine' section at your request based on event syntax.

Windows Logs Additional Reporting

'Routine' Events

Service Management

Nothing to report.

Windows Update Service

Nothing to report.

Software Management

Nothing to report.

Server Reboot Comments

Nothing to report.

'Routine' events are those events which have happened at least 3 times in the past 7 days, or happened on the same day of the week the previous two weeks. Events can also be moved to the 'Routine' section at your request based on event syntax.

Linux Logs

Linux Administration Events

Nothing to report.

Linux Configuration Events

Nothing to report.

Linux Authentication Events

Nothing to report.

Linux Miscellaneous Events

Nothing to report.

Linux Logs

'Routine' Events

Linux Administration Events

Nothing to report.

Linux Configuration Events

Nothing to report.

Linux Authentication Events

Nothing to report.

Linux Miscellaneous Events

Nothing to report.

'Routine' events are those events which have happened at least 3 times in the past 7 days, or happened on the same day of the week the previous two weeks. Events can also be moved to the 'Routine' section at your request based on event syntax.

Office 365 Events

Azure Active Directory

Nothing to report.

Azure Active Directory Account Logon

Nothing to report.

Azure Active Directory Sts Logon

Nothing to report.

Compliance DLP Exchange

Nothing to report.

Compliance DLP Share Point

Nothing to report.

CRM

Nothing to report.

Data Center Security Cmdlet

Nothing to report.

Discovery

Nothing to report.

Exchange Admin

Nothing to report.

Exchange Aggregated Operation

Nothing to report.

Exchange Item

Nothing to report.

Exchange Item Group

Nothing to report.

Microsoft Teams

Nothing to report.

Microsoft Teams Add Ons

Nothing to report.

Microsoft Teams Settings Operation

Nothing to report.

One Drive

Nothing to report.

Power BI Audit

Nothing to report.

Security Compliance Center EOP Cmdlet

Nothing to report.

Share Point

Nothing to report.

Share Point File Operation

Nothing to report.

Share Point Sharing Operation

Nothing to report.

Skype For Business Cmdlets

Nothing to report.

Skype For Business PSTN Usage

Nothing to report.

Skype For Business Users Blocked

Nothing to report.

Sway

Nothing to report.

Threat Intelligence

Nothing to report.

Yammer

Nothing to report.

Office 365 Events

'Routine Events'

Azure Active Directory

Nothing to report.

Azure Active Directory Account Logon

Nothing to report.

Azure Active Directory Sts Logon

Nothing to report.

Compliance DLP Exchange

Nothing to report.

Compliance DLP Share Point

Nothing to report.

CRM

Nothing to report.

Data Center Security Cmdlet

Nothing to report.

Discovery

Nothing to report.

Exchange Admin

Nothing to report.

Exchange Aggregated Operation

Nothing to report.

Exchange Item

Nothing to report.

Exchange Item Group

Nothing to report.

Microsoft Teams

Nothing to report.

Microsoft Teams Add Ons

Nothing to report.

Microsoft Teams Settings Operation

Nothing to report.

One Drive

Nothing to report.

Power BI Audit

Nothing to report.

Security Compliance Center EOP Cmdlet

Nothing to report.

Share Point

Nothing to report.

Share Point File Operation

Nothing to report.

Share Point Sharing Operation

Nothing to report.

Skype For Business Cmdlets

Nothing to report.

Skype For Business PSTN Usage

Nothing to report.

Skype For Business Users Blocked

Nothing to report.

Sway

Nothing to report.

Threat Intelligence

Nothing to report.

Yammer

Nothing to report.

Web Server Logs

Notable General Errors

Nothing to report.

Notable Exploit Attempts

Nothing to report.

Potential SQL Injection

Nothing to report.

Probable Hacking Tools

Nothing to report.

Probable Site Mirrors

Nothing to report.

Miscellaneous

Nothing to report.

IDS/IPS Logs

IDS/IPS Administration Events

Nothing to report.

IDS/IPS Configuration Events

Nothing to report.

IDS/IPS Authentication Events

Nothing to report.

IDS/IPS Miscellaneous Events

Nothing to report.

IDS/IPS Logs

'Routine' Events

IDS/IPS Administration Events

Nothing to report.

IDS/IPS Configuration Events

Nothing to report.

IDS/IPS Authentication Events

Nothing to report.

IDS/IPS Miscellaneous Events

Nothing to report.

'Routine' events are those events which have happened at least 3 times in the past 7 days, or happened on the same day of the week the previous two weeks. Events can also be moved to the 'Routine' section at your request based on event syntax.

SQL Server Logs

SQL Server Authentication Events

Nothing to report.

SQL Server Database Events

Nothing to report.

SQL Server Server Events

Nothing to report.

SQL Server User Events

Nothing to report.

SQL Server Object Events

Nothing to report.

SQL Server Recompile Events

Nothing to report.

SQL Server Miscellaneous Events

Nothing to report.

SQL Server Logs

'Routine' Events

SQL Server Authentication Events

Nothing to report.

SQL Server Database Events

Nothing to report.

SQL Server Server Events

Nothing to report.

SQL Server User Events

Nothing to report.

SQL Server Object Events

Nothing to report.

SQL Server Recompile Events

Nothing to report.

SQL Server Miscellaneous Events

Nothing to report.

'Routine' events are those events which have happened at least 3 times in the past 7 days, or happened on the same day of the week the previous two weeks. Events can also be moved to the 'Routine' section at your request based on event syntax.

Oracle Application Logs

Oracle Authentication

Nothing to report.

Oracle User Management

Nothing to report.

Oracle Table Management

Nothing to report.

Oracle Miscellaneous

Nothing to report.

Oracle Application Logs

'Routine' Events

Oracle Authentication

Nothing to report.

Oracle Routine User Management

Nothing to report.

Oracle Routine Table Management

Nothing to report.

Oracle Routine Miscellaneous

Nothing to report.

'Routine' events are those events which have happened at least 3 times in the past 7 days, or happened on the same day of the week the previous two weeks. Events can also be moved to the 'Routine' section at your request based on event syntax.

Router Logs

Router Administrative Logons

Nothing to report.

Router Configuration Changes

Nothing to report.

Router Miscellaneous Events

Nothing to report.

NOTE: Tyler Technologies recommends some sort of automated authenticated event be setup to attempt authentication (it need not be successful) to each Tyler Detect-reviewed router to ensure that the router is generating log events for each day as some log extremely minimal events.

Router Logs

'Routine' Events

Router Administrative Logons

Nothing to report.

Router Configuration Changes

Nothing to report.

Router Miscellaneous Events

Nothing to report.

'Routine' events are those events which have happened at least 3 times in the past 7 days, or happened on the same day of the week the previous two weeks. Events can also be moved to the 'Routine' section at your request based on event syntax.

Switch Logs

Switch Administrative Logons

Device: 10.0.0.122
---- Authentication (FAILURE) ----
02:21:34 - 02:21:36: Authentication failed for 'admin' from 10.0.0.69 (2 entries)
02:21:31 - 02:21:39: Login attempt for nonexistent user from 10.0.0.69 (5 entries)
Device: 10.0.0.124
---- Authentication (FAILURE) ----
02:22:07 - 02:22:08: Authentication failed for 'admin' from 10.0.0.69 (2 entries)
02:22:05 - 02:22:11: Login attempt for nonexistent user from 10.0.0.69 (5 entries)
Device: 10.0.0.125
---- Authentication (FAILURE) ----
02:22:27 - 02:22:29: Authentication failed for 'admin' from 10.0.0.69 (2 entries)
02:22:25 - 02:22:32: Login attempt for nonexistent user from 10.0.0.69 (5 entries)
Device: 10.0.0.146
---- Authentication (FAILURE) ----
02:31:41 - 02:31:42: Authentication failed for 'admin' from 10.0.0.69 (2 entries)
02:31:38 - 02:31:45: Login attempt for nonexistent user from 10.0.0.69 (5 entries)
Device: 10.0.0.68
---- Authentication (FAILURE) ----
01:59:41 - 01:59:42: Authentication failed for 'admin' from 10.0.0.69 (2 entries)
01:59:38 - 01:59:45: Login attempt for nonexistent user from 10.0.0.69 (5 entries)
Device: 10.10.0.246
---- Authentication (FAILURE) ----
01:42:21 - 01:42:22: Authentication failed for 'admin' from 10.0.0.69 (2 entries)
01:42:18 - 01:42:25: Login attempt for nonexistent user from 10.0.0.69 (5 entries)
Device: 10.10.0.248
---- Authentication (FAILURE) ----
01:42:57: Authentication failed for 'admin' from 10.0.0.69 (2 entries)
01:42:55 - 01:42:59: Login attempt for nonexistent user from 10.0.0.69 (5 entries)
Device: 10.10.0.249
---- Authentication (FAILURE) ----
01:43:14 - 01:43:15: Authentication failed for 'admin' from 10.0.0.69 (2 entries)
01:43:12 - 01:43:18: Login attempt for nonexistent user from 10.0.0.69 (5 entries)
Device: 10.10.0.74
---- Authentication (FAILURE) ----
01:19:11 - 01:19:12: Authentication failed for 'admin' from 10.0.0.69 (2 entries)
01:19:08 - 01:19:15: Login attempt for nonexistent user from 10.0.0.69 (5 entries)
Device: 10.10.0.75
---- Authentication (FAILURE) ----
01:19:25 - 01:19:27: Authentication failed for 'admin' from 10.0.0.69 (2 entries)
01:19:23 - 01:19:32: Login attempt for nonexistent user from 10.0.0.69 (5 entries)
Device: 10.20.0.11
---- Authentication (FAILURE) ----
01:05:37 - 01:05:38: Authentication failed for 'admin' from 10.0.0.69 (2 entries)
01:05:35 - 01:05:42: Login attempt for nonexistent user from 10.0.0.69 (5 entries)
Device: 10.20.0.12
---- Authentication (FAILURE) ----
01:07:36 - 01:07:37: Authentication failed for 'admin' from 10.0.0.69 (2 entries)
01:07:34 - 01:07:40: Login attempt for nonexistent user from 10.0.0.69 (5 entries)
Device: 10.20.0.13
---- Authentication (FAILURE) ----
01:09:33 - 01:09:34: Authentication failed for 'admin' from 10.0.0.69 (2 entries)
01:09:31 - 01:09:37: Login attempt for nonexistent user from 10.0.0.69 (5 entries)

Switch Configuration Changes

Device: 10.20.0.11
---- Device Configuration ----
09:49:06 - 10:25:11: APPLY-CONFIG: Using fast apply (3 entries)

09:48:56 - 10:25:01: Saving mgmt_url as hxxps://10.20.0.10:8443/manage/site/default (3 entries)
09:48:56 - 10:25:01: Saving stun_url as stun://10.20.0.10/ (3 entries)
Device: 10.20.0.12
---- Device Configuration ----
09:49:06 - 10:10:25: APPLY-CONFIG: Using fast apply (2 entries)
09:48:56 - 10:18:37: Saving mgmt_url as hxxps://10.20.0.10:8443/manage/site/default (3 entries)
09:48:56 - 10:18:37: Saving stun_url as stun://10.20.0.10/ (3 entries)
Device: 10.20.0.13
---- Device Configuration ----
10:06:03 - 10:10:02: APPLY-CONFIG: Using fast apply (4 entries)
09:48:55 - 16:05:06: Saving mgmt_url as hxxps://10.20.0.10:8443/manage/site/default (6 entries)
09:48:55 - 16:05:06: Saving stun_url as stun://10.20.0.10/ (6 entries)

Switch Miscellaneous Events

Nothing to report.

NOTE: Tyler Technologies recommends some sort of automated authenticated event be setup to attempt authentication (it need not be successful) to each Tyler Detect-reviewed router to ensure that the switch is generating log events for each day as some log extremely minimal events.

Switch Logs

'Routine' Events

Switch Administrative Logons

Nothing to report.

Switch Configuration Changes

Nothing to report.

Switch Miscellaneous Events

Nothing to report.

'Routine' events are those events which have happened at least 3 times in the past 7 days, or happened on the same day of the week the previous two weeks. Events can also be moved to the 'Routine' section at your request based on event syntax.

VPN Logs

VPN Administrative Logons

Nothing to report.

VPN Configuration Changes

Nothing to report.

VPN Authentication Events

Nothing to report.

VPN Miscellaneous Events

Nothing to report.

VPN Logs

'Routine' Events

VPN Administrative Logons

Nothing to report.

VPN Configuration Changes

Nothing to report.

VPN Authentication Events

Nothing to report.

VPN Miscellaneous Events

Nothing to report.

'Routine' events are those events which have happened at least 3 times in the past 7 days, or happened on the same day of the week the previous two weeks. Events can also be moved to the 'Routine' section at your request based on event syntax.

VCenter Logs

VCenter Administrative Logons

Nothing to report.

VCenter Configuration Changes

Nothing to report.

VCenter Miscellaneous Events

Nothing to report.

VCenter Logs

'Routine' Events

VCenter Administrative Logons

Nothing to report.

VCenter Configuration Changes

Nothing to report.

VCenter Miscellaneous Events

Nothing to report.

'Routine' events are those events which have happened at least 3 times in the past 7 days, or happened on the same day of the week the previous two weeks. Events can also be moved to the 'Routine' section at your request based on event syntax.

VMWare Logs

Authentication Events

Nothing to report.

Virtual Machine Events

Nothing to report.

Virtual Disk Events

Nothing to report.

Task Events

Nothing to report.

VMWare Events

Nothing to report.

VMWare Logs

'Routine' Events

Authentication Events

Nothing to report.

Virtual Machine Events

Nothing to report.

Virtual Disk Events

Nothing to report.

Task Events

Nothing to report.

VMWare Events

Nothing to report.

'Routine' events are those events which have happened at least 3 times in the past 7 days, or happened on the same day of the week the previous two weeks. Events can also be moved to the 'Routine' section at your request based on event syntax.

Email Gateway Logs

Email Gateway Administrative Logons

Nothing to report.

Email Gateway Configuration Changes

Nothing to report.

Email Gateway Authentication Events

Nothing to report.

Email Gateway Miscellaneous Events

Nothing to report.

Email Gateway Logs

'Routine' Events

Email Gateway Administrative Logons

Nothing to report.

Email Gateway Configuration Changes

Nothing to report.

Email Gateway Authentication Events

Nothing to report.

Email Gateway Miscellaneous Events

Nothing to report.

'Routine' events are those events which have happened at least 3 times in the past 7 days, or happened on the same day of the week the previous two weeks. Events can also be moved to the 'Routine' section at your request based on event syntax.

SAN Logs

SAN Administrative Logons

Device: 10.0.0.25
---- Authentication (FAILURE) ----
01:49:23 - 01:49:29: User 'admin' from 10.0.0.69 failed to log in via SSH (2 entries)
01:49:18: User 'pi' from 10.0.0.69 failed to log in via SSH
01:49:34 - 01:49:40: User 'root' from 10.0.0.69 failed to log in via SSH (2 entries)
01:49:45 - 01:49:51: User 'tmc' from 10.0.0.69 failed to log in via SSH (2 entries)
Device: 10.0.0.82
---- Authentication ----
20:49:46: User 'dom' from 66.188.66.174 (Charter-20115, Covington, GA) logged in successfully via DSM

SAN Configuration Changes

Nothing to report.

SAN Miscellaneous Events

Nothing to report.

SAN Logs

'Routine' Events

SAN Administrative Logons

Device: 10.0.0.25
---- Authentication ----
18:59:09 - 19:04:01: User 'admin' from 10.0.0.18 logged in successfully via FTP (38 entries)
18:59:10 - 19:04:01: User 'admin' from 10.0.0.18 logged out successfully via FTP (39 entries)

SAN Configuration Changes

Nothing to report.

SAN Miscellaneous Events

Device: 10.0.0.82
---- Device Status ----
04:46:42: System successfully registered '75.131.184.18' to 'ncwsa.synology.me' in DDNS server 'Synology'

'Routine' events are those events which have happened at least 3 times in the past 7 days, or happened on the same day of the week the previous two weeks. Events can also be moved to the 'Routine' section at your request based on event syntax.

Wireless Access Point Logs

WAP Administrative Logons

Nothing to report.

WAP Configuration Changes

Nothing to report.

WAP Authentication Events

Nothing to report.

WAP DHCP Events

Nothing to report.

WAP Miscellaneous Events

Nothing to report.

Wireless Access Point Logs

'Routine' Events

WAP Administrative Logons

Nothing to report.

WAP Configuration Changes

Nothing to report.

WAP Authentication Events

Nothing to report.

WAP DHCP Events

Nothing to report.

WAP Miscellaneous Events

Nothing to report.

'Routine' events are those events which have happened at least 3 times in the past 7 days, or happened on the same day of the week the previous two weeks. Events can also be moved to the 'Routine' section at your request based on event syntax.

RSA Authentication Manager Logs

RSA Administrative Logons

Nothing to report.

RSA Configuration Changes

Nothing to report.

RSA Authentication Events

Nothing to report.

RSA Miscellaneous Events

Nothing to report.

RSA Authentication Manager Logs

'Routine' Events

RSA Administrative Logons

Nothing to report.

RSA Configuration Changes

Nothing to report.

RSA Authentication Events

Nothing to report.

RSA Miscellaneous Events

Nothing to report.

'Routine' events are those events which have happened at least 3 times in the past 7 days, or happened on the same day of the week the previous two weeks. Events can also be moved to the 'Routine' section at your request based on event syntax.

Multi-Factor Authentication Logs

MFA Administrative Logons

Nothing to report.

MFA Configuration Changes

Nothing to report.

MFA Authentication Events

Nothing to report.

MFA Miscellaneous Events

Nothing to report.

Multi-Factor Authentication Logs

'Routine' Events

MFA Administrative Logons

Nothing to report.

MFA Configuration Changes

Nothing to report.

MFA Authentication Events

Nothing to report.

MFA Miscellaneous Events

Nothing to report.

'Routine' events are those events which have happened at least 3 times in the past 7 days, or happened on the same day of the week the previous two weeks. Events can also be moved to the 'Routine' section at your request based on event syntax.

NetScaler Logs

NetScaler Authentication Events

Nothing to report.

NetScaler Administrative Logon Events

Nothing to report.

NetScaler Configuration Changes Events

Nothing to report.

NetScaler Miscellaneous Events

Nothing to report.

NetScaler Logs

'Routine' Events

NetScaler Authentication Events

Nothing to report.

NetScaler Administrative Logon Events

Nothing to report.

NetScaler Configuration Changes Events

Nothing to report.

NetScaler Miscellaneous Events

Nothing to report.

'Routine' events are those events which have happened at least 3 times in the past 7 days, or happened on the same day of the week the previous two weeks. Events can also be moved to the 'Routine' section at your request based on event syntax.

Appendix

Monitored Windows Servers

The following Windows servers were queried by the Tyler Detect service: CMS2, DOS, SW-HCA-VM1, SW-HCA-VM2, TRES, TYLERDETECT, and UNO

Note that the Tyler Detect service relies on the provided data. For proper analysis, your windows devices should be configured to audit the following events (both success and failure) if NOT using SubCategories: Account logon events; Account management; Logon events; Policy change; System events. If using SubCategories: System: Security System Extension, Security State Change; Logon/Logoff: Logon; Object Access: Other Object Access Events; Policy Change: Audit Policy Change, Authentication Policy Change, Authorization Policy Change; Account Management: User Account Management,Computer Account Management, Security Group Management, Distribution Group Management, Other Account Management Events; Account Logon: Kerberos Authentication Service, Credential Validation.

Monitored Firewalls

The following firewalls are currently being analyzed: 10.0.0.1 (12.6mb), 10.10.0.1 (17.8mb), and 10.20.0.1 (12.7mb)

Note that the Tyler Detect service relies on the provided data. For proper analysis, your firewall should be configured to syslog all messages down to the 'Informational' level including, but not limited to: allowed traffic events; denied traffic events; administrative logons; and configuration changes. You may also be instructed to add or remove logging of specific messages by Tyler Cybersecurity.

Monitored Web Servers/Sites

The following web sites are currently being analyzed: n/a

Note that the Tyler Detect service relies on the provided data. For proper analysis, your IIS web server should be configured to log in 'W3C Extended' format, with all fields enabled for logging. For Apache servers, the same level of data (via NCSA extended format) should be collected (however, some IIS fields are unavailable in the NCSA format).

Other Monitored Devices

VMWare Hosts: 10.10.0.67 (6.5mb)
Switches: 10.0.0.68, 10.0.0.122, 10.0.0.124, 10.0.0.125, 10.0.0.146, 10.10.0.74, 10.10.0.75, 10.10.0.246, 10.10.0.248, 10.10.0.249, 10.20.0.11, 10.20.0.12, and 10.20.0.13
SAN Hosts: 10.0.0.25 (0.0mb), and 10.0.0.82 (0.1mb)

Devices in your network are not monitored by the Tyler Detect process unless specifically noted in this Appendix. If you have questions about this, please contact Tynan Nida at 800.772.2260 x 2335 or tynan.nida@tylertech.com.

Windows Server Appendix

Audit Policy Settings

For report brevity, this data only prints in reports for Sundays.

Services Running As Users

For report brevity, this data only prints in reports for Sundays.

NetScaler Logs Appendix

NetScaler SSLVPN Detailed Events

This data is available on the nData tab of the Tyler Detect portal. To opt-in to including this in your report, contact your Specialist.

NetScaler Device Access Detailed Events

This data is available on the nData tab of the Tyler Detect portal. To opt-in to including this in your report, contact your Specialist.

NetScaler Logs Appendix

'Routine Events'

NetScaler SSLVPN Detailed Events

This data is available on the nData tab of the Tyler Detect portal. To opt-in to including this in your report, contact your Specialist.

NetScaler Device Access Detailed Events

This data is available on the nData tab of the Tyler Detect portal. To opt-in to including this in your report, contact your Specialist.

'Routine' events are those events which have happened at least 3 times in the past 7 days, or happened on the same day of the week the previous two weeks. Events can also be moved to the 'Routine' section at your request based on event syntax.

End Point Appendix

Devices Not Collected within 60 Days

This information is only printed in the Sunday report.

Devices Sysmon Not Installed within 60 Days

This information is only printed in the Sunday report.