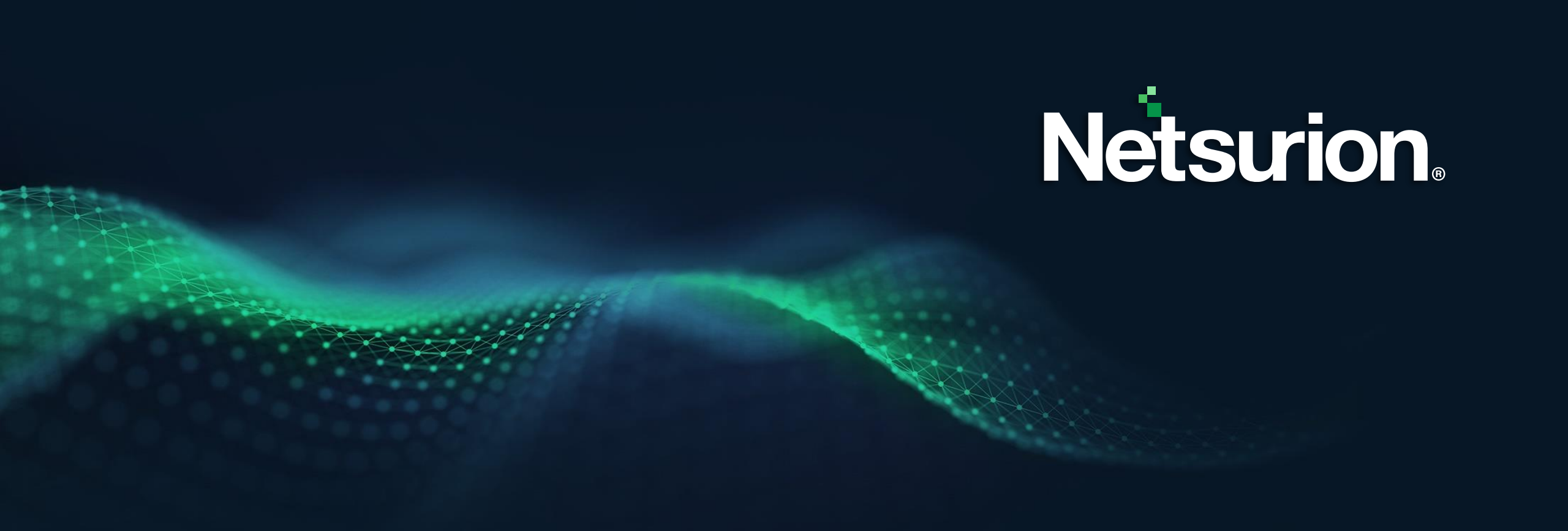


Managed XDR Service Review

Contoso | January 2023

Agenda & Introduction

- Power BI Trends
- Updates and Improvements
- Risk Management
- Integrations
- Critical Observations

Emerging and Evolving Threats

Variants

- Borat
- Azovstal Cobalt Strike
- Wiper Malware
- Nerbian RAT
- Bumblebee malware
- JokerMalware
- KurayStealer
- PowerShell RAT
- SYK Crypter
- Eternity Malware
- Fileless Malware
- Tanki X Ransomware
- MSDT Follina
- VmwareExploit APT
- Karakurt group
- Atlassian RCE
- Confluence webshell
- Maui ransomware
- Mimikatz
- OwlProxy
- Gelsemium
- Chromeloader
- Chinese Statesponsor
- Mimikatz
- OwlProxy
- Gelsemium
- Chromeloader
- Chinese Statesponsor
- CVE-2017-0199-exploit
- MSIL TrojanDownloader
- SolidBit Ransomware
- WoodyRAT
- Yanluowang ransomware
- Raccoon Ransomware
- CodeRAT
- Neshta Vice Society
- Fargo Ransomware
- Exchange0day
- Log4j
- Emotet
- BlackBasta
- Formbook
- Magniber
- Ransom.Royal
- Iranian APT
- SSH attack
- CubaRansomware
- POLONIUM
- OWASSRF

Indicators of compromises (IoC) and hash values of all these malicious file variants and other emerging threats are collected and updated in Netsurion's Active Watch list on a regular basis by your dedicated Threat Hunting team.

Netsurion®

Contacting the SOC

Contact Your SOC:	SOC@Netsurion.com	1 (877) 333-1433 Option 1, Option 1

Emails received are acknowledged in 15 business minutes in accordance with the SLO of purchased Analysis Frequency Option: Weekly/Daily/24x7.

Support requests are submitted via a ticket and are categorized as Urgent, High or Low by the Customer, SOC Manager or Team Leads depending on the nature of the issue being reported. The corresponding SLOs are:

Your Service Level	Severity	Response SLO	Resolution SLO
Weekly	Urgent	1 Business hour from receipt	1 Business day from receipt
	High	4 Business hours from receipt	5 Business days from receipt
	Low	8 Business hours from receipt	10 Business days from receipt

Important:

- ✓ If you have any urgent request that you need our attention or assistance with – please mention "**Urgent**" In the email subject line.
- ✓ If you need any immediate assistance during off-hours (2:30 PM EST – 5:30 AM EST) please call us and email us so that the available analyst can make sure your request is addressed on time.
- ✓ Customer environment monitoring is performed, and the top priority incidents will be reported daily.

Netsurion®

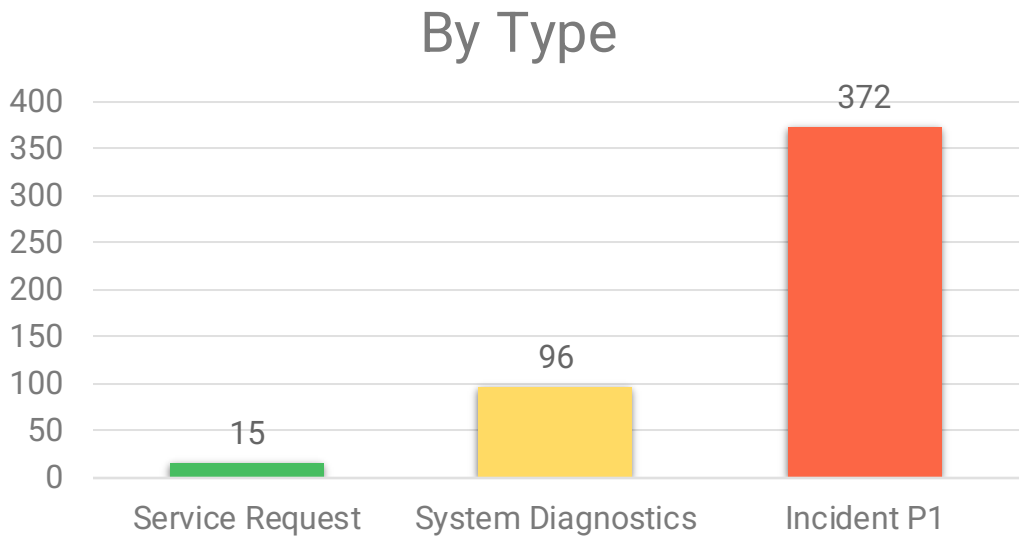
SOC Call Tree and Escalation

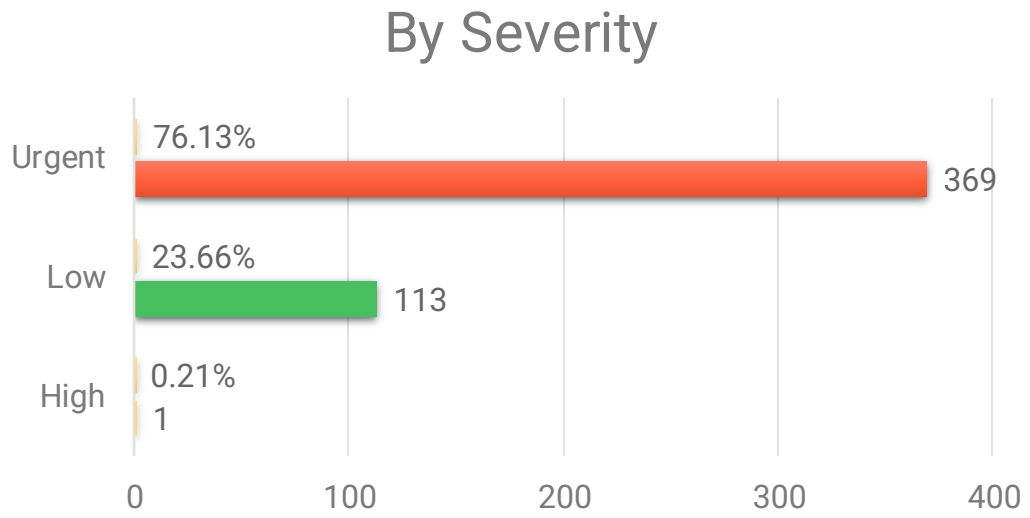
Primary Contact	**Danny Ocean** Senior Manager, Cybersecurity	d.ocean@contoso.com	555.555.5550
Additional Contact 1	**Linus Caldwell** Cybersecurity Analyst	l.caldwell@contoso.com	555.555.5555
Additional Contact 2	**Basher Tarr** IT Systems Manager	b.tarr@contoso.com	555.555.5556

For any pending critical issues, please contact:			
Escalation Contact	**Saul Bloom** CIO	s.bloom@contoso.com	555.555.5551

Netsurion®

Ticket Category Trends





Netsurion®

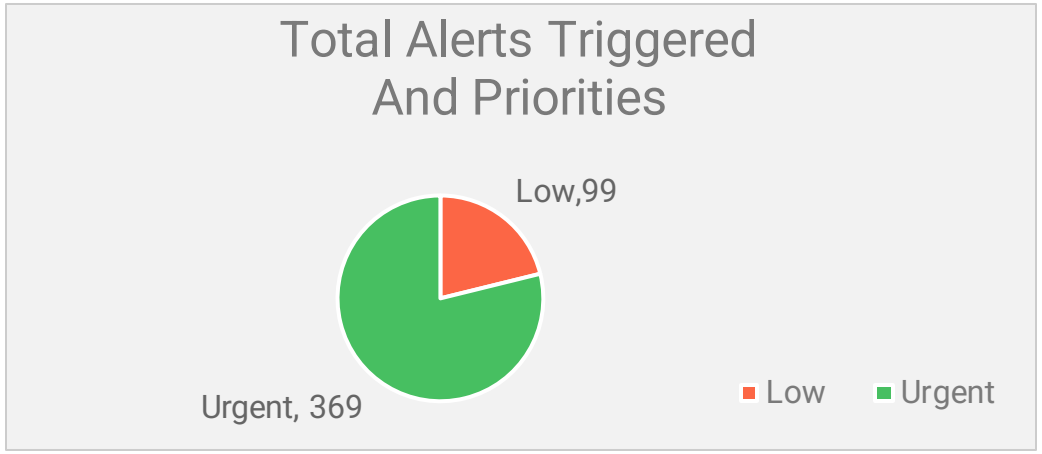
Catches – True/False Positive

Date	Ticket	Subject	Description	Priority	Status
2023-01-15 00:23:15	36654654	**Alert from OPS25.CTSO-Workstation** Alert Name: Netsurion: Suspicious exploit attempt detected - Incident No: 202210000011391	SOC has observed suspicious command on system OPS25.CTSO-Workstation in US East Region LT123 by user RRyan. Detailed logs are attached for reference.	Urgent	Closed
2023-01-18 01:19:56	36654655	**Alert from RED.CTSO-Workstation** Alert Name: PowerShell running suspicious commands - Incident No: 202301000010348	A suspicious command, powershell -NoProfile -Command was executed by PowerShell through powershell.exe.	Urgent	Closed

True Positive False Positive 

Netsurion®

Overview on Alerts

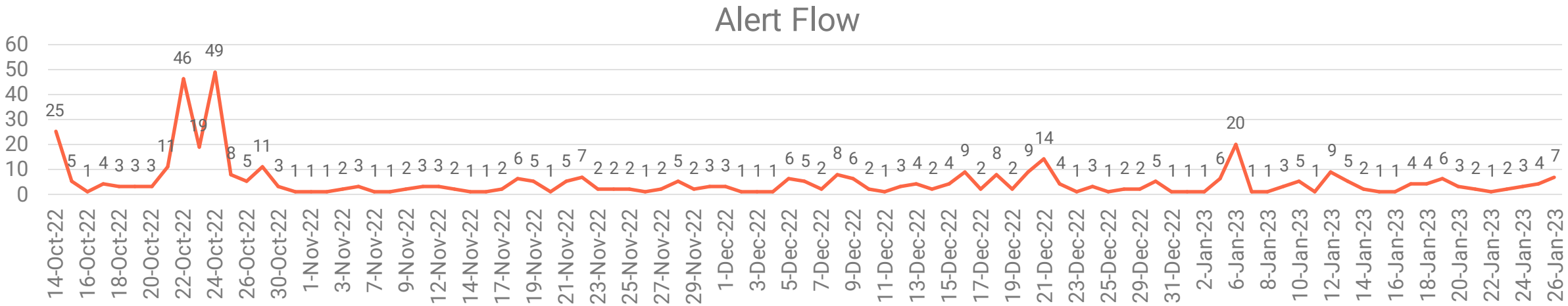


Most Triggered Alerts:

1. PowerShell running suspicious commands

Note:

1. All alerts are checked and verified by the Netsurion SOC team
2. Concerning incidents will be escalated to the Client



Netsurion®

Integrations

Currently Integrated	Suggested Integration
Cisco ASA with FirePOWER	ESET Anti-Virus
AWS	
Microsoft 365	
Deep Instinct	
Tenable	
Linux	
MacOS	

Risk Register

Risk Description	Key Risk Drivers	Consequence	Recommended Controls		
			Likelihood	Impact	Recommendation
Non-Reporting Systems	Multiple systems are not reporting to Netsurion	Will be missing events as the systems are not sending data to Netsurion XDR platform.	Serious	Serious	For Windows Machines, please follow the instructions on the guide.
Apache Web Server	Application-Level Penetration testing, Web Server Threats and attacks	We won't have visibility into events related to Web attacks or Application-level PT. Chances of missing out on important observations due to this.	High	High	Integration of Web server logs with Netsurion.

Critical Observation - Threats

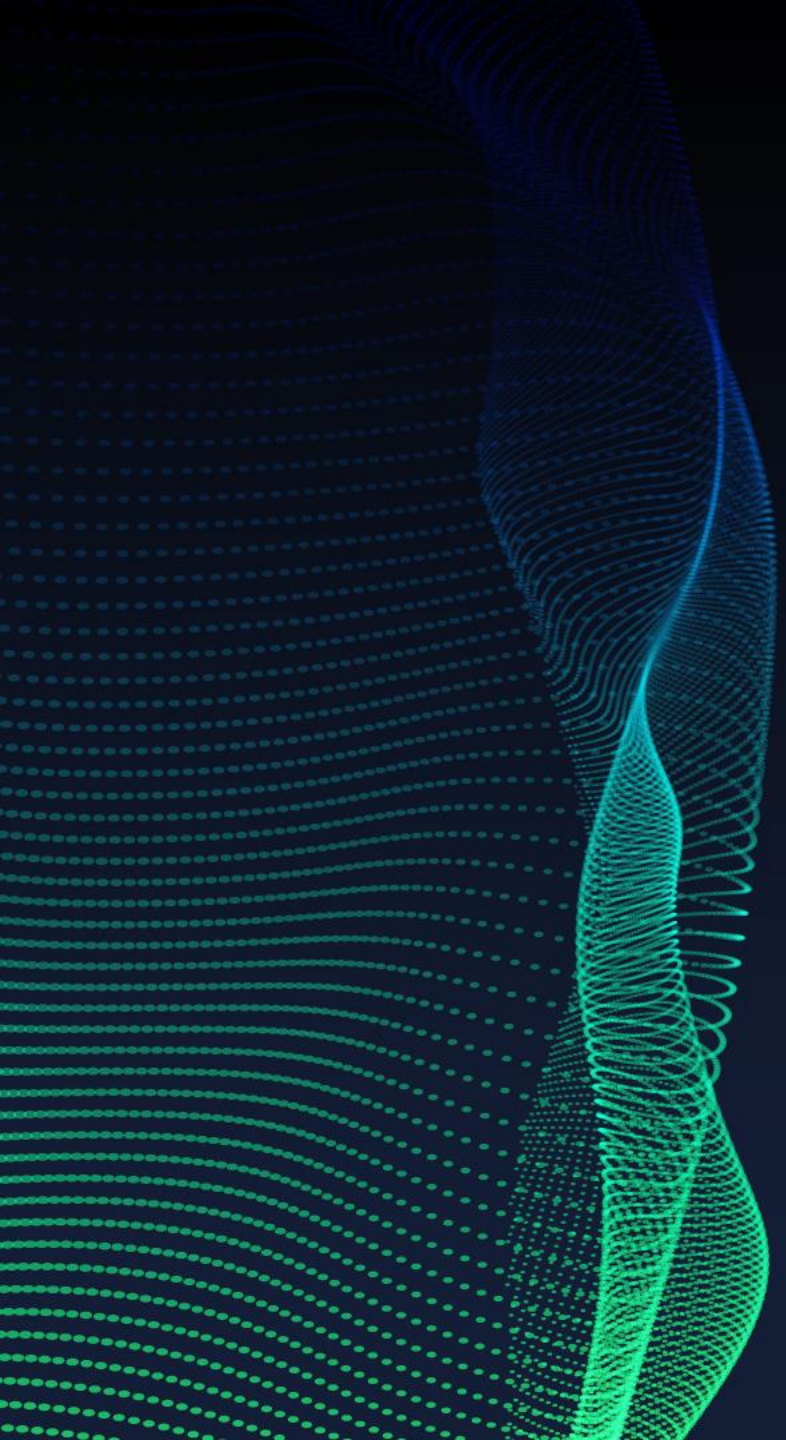
Date	Observation
Jan 15, 2023	SOC observed suspicious Network logon failures from the multiple internal source IP address on the below mentioned systems due to Unknown username from username sahhuser1.
Jan 13, 2023	Netsurion SOC has observed suspicious logon failures on multiple systems due to Bad Password, Unknown username, and An Error occurred during Logon reasons.
Jan 8, 2023	Inbound connection from multiple suspicious IP addresses were recorded while communicating with executable process nginx.exe on multiple systems
Jan 3, 2023	SOC has observed a new process TINYTAKE BY MANGOAPPS.EXE communicating to an external IP address 142.250.187.206, on system DO-LAPTOP76~CTSOHQ.
Jan 1, 2023	SOC has observed Suspicious Unknown process with bad hash value. • MD5 Hash: 3fab1bcdd7dd8b99783b9c0d2ca8dd7e • File Name: Lively.Watchdog.exe • System Name: PK-LAPTOP178~TCP-Humanity • Parent Process Name: Lively.exe • Username: hamza • Image File Path: C:\Program Files\WindowsApps\12030rocksdanister.LivelyWallpaper_1.0.130.0_x86__97hta09mmv6hy\Build\Plugins\Watchdog\Lively.Watchdog.exe

Admin Group Modification Analysis

Date	Admin	Member	System	Group Name	Operation	Group Type
Jan 23, 2023	CTSO-9099	CN=Frank Catton,OU=Accounting,OU=DMI Employees,OU=Domain Users,DC=docean,DC=com	NSPVMDFHEN19288 \DMISRV5~CTSO_SERVERS	CTSO Bellagio Application Admin	Added	Global
Jan 21, 2023	CTSO-8088	CN=Frank Catton,OU=Accounting,OU=DMI Employees,OU=Domain Users,DC=docean,DC=com	NSPVMDFHEN19288 \DMISRV5~CTSO_SERVERS	CTSO Mirage Backend Tools Admin	Added	Global
Jan 4, 2023	TBENEDICT	CN=Virgil Malloy,OU=Technical Support,OU=DMI Employees,OU=Domain Users,DC=tmalloy,DC=com	NSPVMDFHEN19288 \DMISRV5~CTSO_SERVERS	CTSO Bellagio Application Admin	Removed	Global
Jan 2, 2023	TBENEDICT	CN=Virgil Malloy,OU=Technical Support,OU=DMI Employees,OU=Domain Users,DC=tmalloy,DC=com	NSPVMDFHEN19288 \DMISRV5~CTSO_SERVERS	CTSO Mirage Backend Tools Admin	Removed	Global

Action Items

Action	Responsible	Status
Cisco WSA - Proxy Allowed Traffic: Validate and ensure that the Cryptocurrency category connections are blocked	SOC	Completed
Software Install & uninstall Activity: SOC to share software install and uninstall activity by non-system accounts.	SOC	Completed
OpenDNS Integration: SOC to share the integration guide for OpenDNS.	SOC	Completed
Informational: Validate the Top Exploited vendor list and compare it with vulnerability report and ensure that no top exploited vendors exist on the infrastructure.	SOC	Completed
Informational: Update Contoso team on Deep Instinct upgrade window	SOC	Completed
Windows Login Failure: Check reason for high login failure of following accounts and update passwords - Tmalloy - Vmalloy - Yen	CTSO	In Progress



Thank You

Netsurion®