Netsurion™ | EventTracker

Executive Summary and Monthly Report

Contoso – Nov 2018

Agenda

Netsurion | EventTracker

Review of prior month

- Trends – Log volume and incidents
- Measuring what is important
- Network security
- Operational overview
- Updates and improvements
- Critical observations
- Current configuration specifications
- Action items from last review

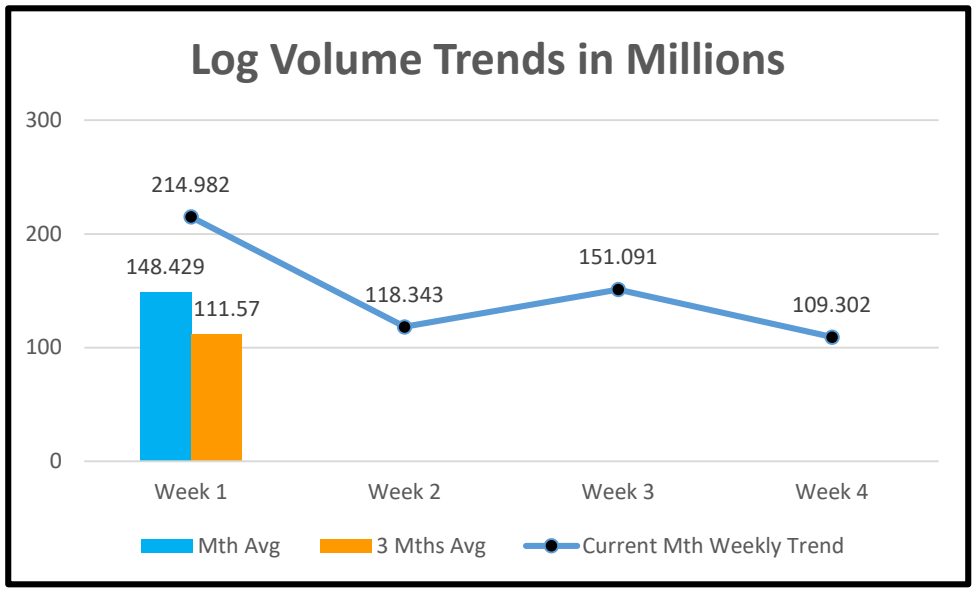
Technical Details

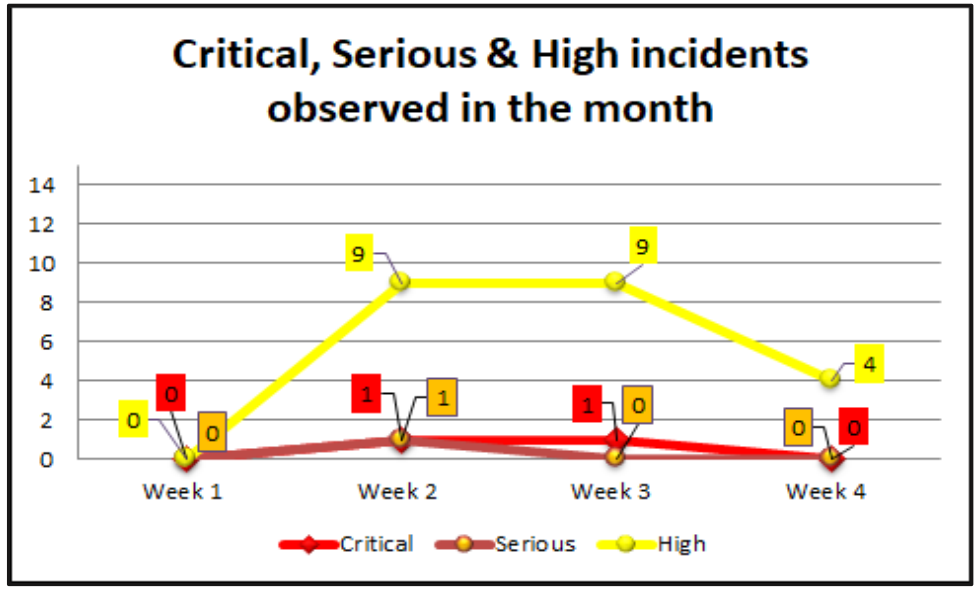
- Threats
- Changes to identity and access policies
- Application activity
- System resource

Appendix

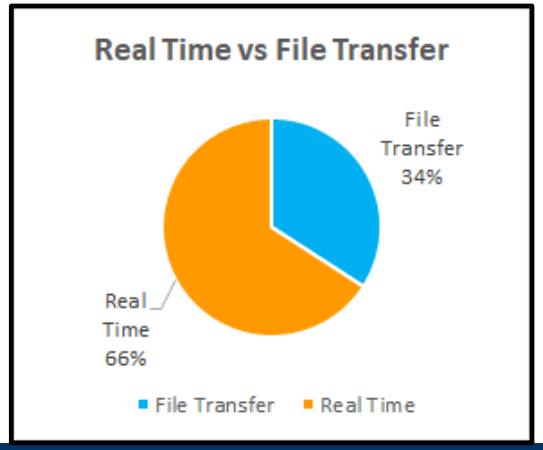
- Threat alerts
- Application activity
- Change management

Trends – Log Volume and Incidents





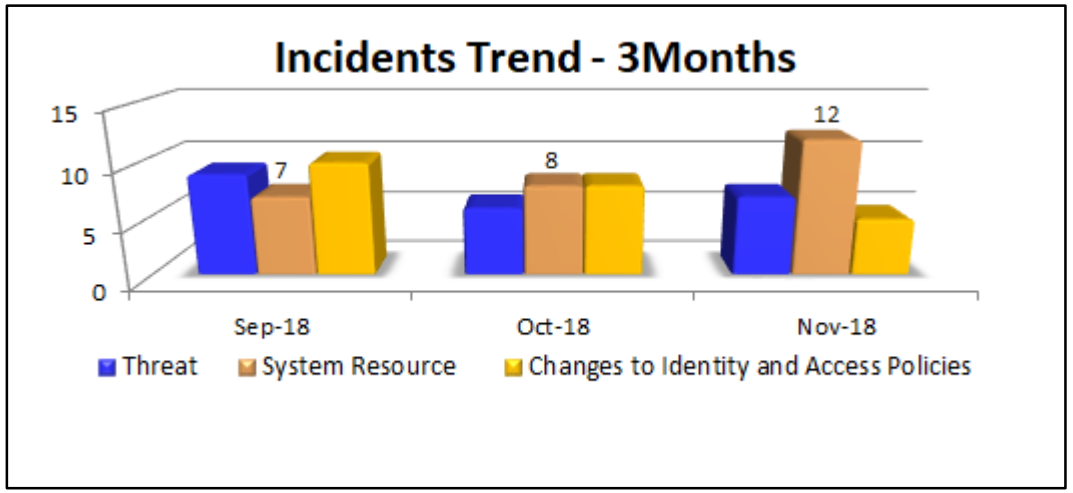
Log Volume increase in week 1 is due to event ID 8 (User logoff detected) from multiple systems

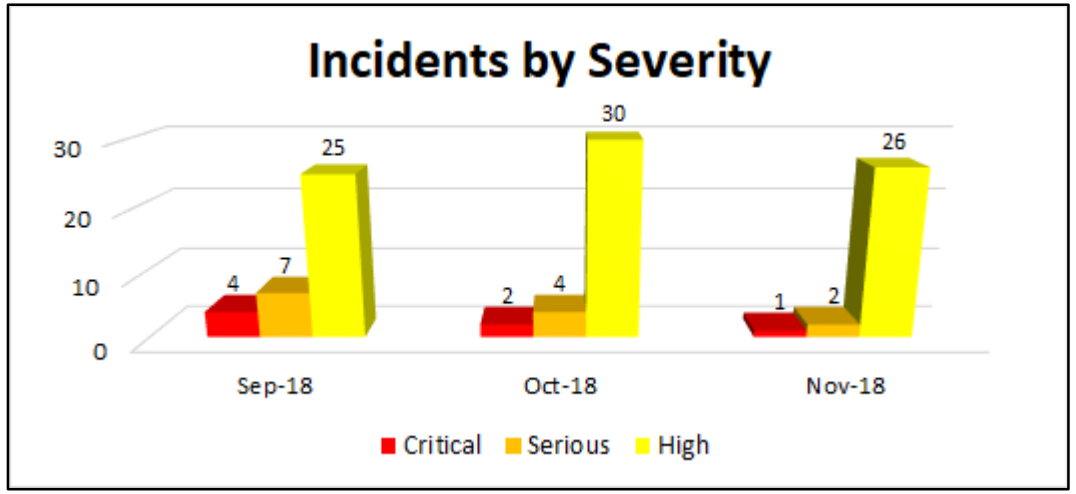


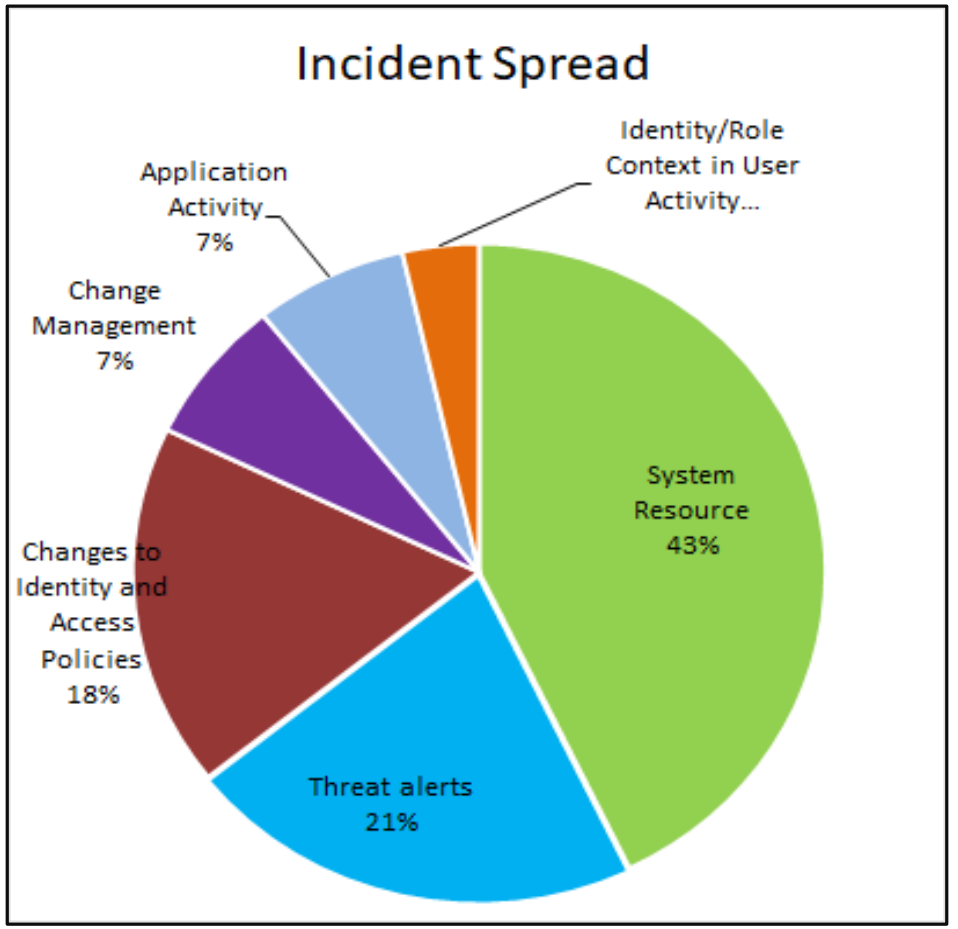
Top 3 Incidents (by count)		Top 3 Incidents (by criticality)
System Resource	12	System Resource
Threat Alert	06	Threat Alert
Changes to Identitiy and Access Policies	05	Changes to Identitiy and Access Policies

Risk Color Coding
Critical
Serious
High
Medium
Low

Trends - Incidents







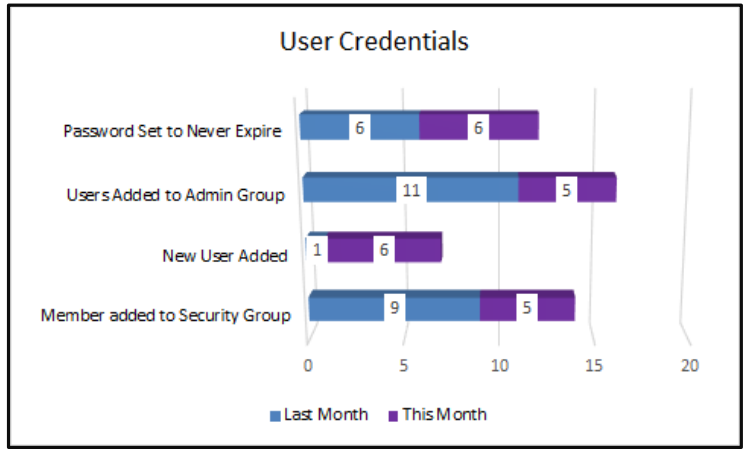
Measuring What is Important

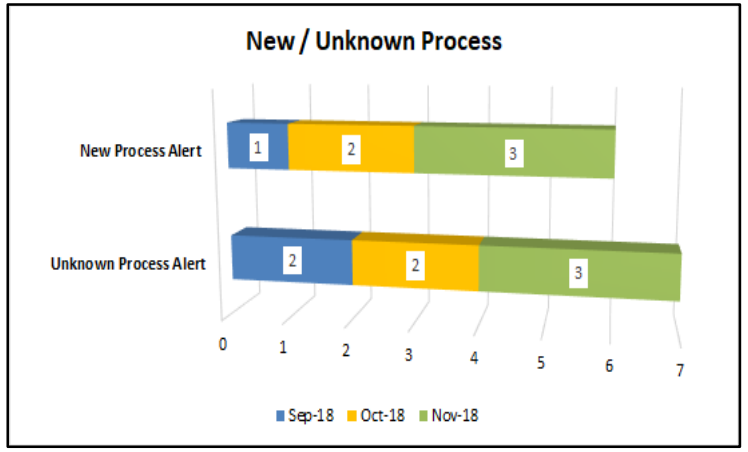
What gets measured, get managed – Peter Drucker

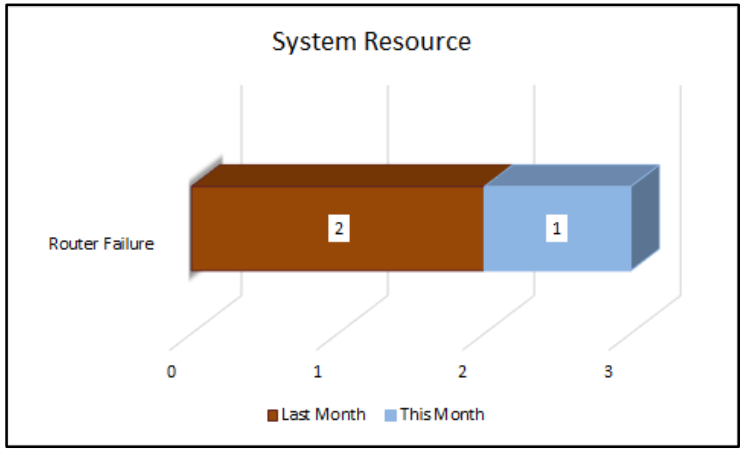
Netsurion | EventTracker

"Measuring What's Important". Based on the incidents / events of the last couple of months, we have identified 3 categories that we feel are important to track, measure and report.

Total number of incidents in Nov 2018 has shown a 15% increase when compared to Oct 2018.







User Credentials

Count of incidents has reduced this month. Area of concern is "Password Set to Never Expire". This incident has not shown any improvement. Our recommendation has been that this is discouraged.

New / Unknown Processes

There has been a noticeable increase in the month in this area. There is a need for awareness training to be conducted to users on the risks of downloading executables off the internet.

System Resource Monitoring

Though the event count is not very high, the router failure is still being observed. We felt this was serious enough to bring to your notice

Risk Management

Netsurion | EventTracker

Risk Description	Key Risk Drivers	Operational Impact	Risk Metrics				
			Likelihood	Impact	Preventive Action	Corrective Action	Risk Status
Web Server Log Integration IIS v7 Apache 2.2.24	Application Level Penetration testing, Web Server Threats and attacks	We won't get any logs 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 EventTracker.	To Integrate 1 Internal and 1 externally facing web server	Completed
IDS Crash	ET-IDS Crashes frequently	Absence of alerts from network and application based logs. Also helps us to identify data breaches	High	Medium	Alert to be created to find the crash instantaneously	Logs to be deleted and restart Snort Service	In-Progress
Agents running on Older Version	Few agents are running on older version in Prism	Important updates will not be available for the agents running on older version	Medium	Medium	Upgrade agents	Upgrade clients to 8.2.14 and verify	Imitated agent upgrade with Domain admin credentials. Shared the list of agents which are running on older version, recommended manual installation of agents
ET-VAS Resource	Few processes are consuming very high memory leading to reports failure	Important /critical vulnerabilities could be missed	High	High	Increase system resources such as Memory, Processor	16GB of RAM, QuadCore	Completed
Firewall Integration	Firewall is not reporting to EventTracker	Leads to gaps in capturing important logs from firewall, such as port scans, CPU utilization, important configuration changes. Anomalies and malicious activities will be out of EventTracker' s reach	Critical	High	For Syslog Machines, please check the syslog forwarding and device status.	Work with IT team for swift resolution	Completed

Network Security

Netsurion | EventTracker

- Firewall and ET-IDS incidents
  - FortiGate Firewall devices FWL60D4Q63, and FWL45Y3S21 detected bad IP communications to multiple IPs over multiple ports
- Firewall Usage – Denied Network Traffic
  - Observed on Cisco appliance - Suspected port scans were detected from multiple external IP addresses which have bad reputation. Traffic was denied on multiple ports including well-known and registered ports.

Firewall Status		
Managed Devices	Description	Risk Status
189.128.107.1-syslog	Cyberhome	

ETVAS –Issues Produced during scans

SEVERITY	HIGH			MEDIUM			LOW		
Host Group	Nov	Oct	Sep	Nov	Oct	Sep	Nov	Oct	Sep
Linux Servers	1	0	0	9	12	17	14	16	17
Win2013 Servers	7	12	16	21	53	62	98	107	145
Win2008 Servers	23	41	53	19	34	41	77	85	112
Total	31	53	69	49	99	120	189	208	274

ET IDS Alerts Noted and Reported during the month

Alert Classification	Nov	Oct	Sep
Potential Bad Traffic	12,478	13,829	18,570
Unknown Traffic	11,716	12,398	16,272
Attempted Information Leak	02	09	07
Sensitive Data Transmitted across the network	-	04	82
Detection of a Non-Standard Protocols/Events	19	19	-
Executable Code was Detected	-	01	-
Detection of a Non-Standard Protocol or Event	-	421	-

Operational Overview

Netsurion | EventTracker

- EventTracker running on version 9.0 Build 18
- Count of Devices reporting to EventTracker

Class	Servers	Syslog Devices	Firewall	Workstations	Total
Collection Master (Reporting – Nov 2018)	59	13	01	36	108
Collection Master (Non-Reporting – Nov 2018)	07	05	00	04	16
Collection Point (Reporting – Nov 2018)	09	02	00	38	57
Collection Point (Non-Reporting – Nov 2018)	00	00	00	00	00

- Do you have any dependencies/roadblocks that need to be addressed?

Updates and Improvements

Netsurion | EventTracker

- New Reports Configured / improved:
  - VMware VM created report
  - Exchange mailbox access by non-owner
- New Alert configured / improved:
  - None
- Filters confirmed and applied
  - False positive of “Citrix Server restarts daily 12.00 midnight” observed last month was filtered
- Cases Closed
- Catch of the day
  - None

Date	Logbook ID	Details
11/08/2018 09:11	10044	SOC observed 17 systems are not reporting to the EventTracker.
11/09/2018 06:19	10045	Brute Force Attack on server "MAILS55".
10/14/2018 06:19	10046	Malware Process.
09/23/2018 09:30	10047	Dictionary Attack on MAILS55.

Critical Observations
Threats

Date	Observation
9-Nov-18	Brute Force attack on MAILS55 from external source "freerdp" by using multiple usernames. One of them is “administrator” and it is locking out due to multiple failed attempts
14-Nov-18	New unsigned processes ShowMyPC3161.exe and smpcp.exe was created on the system CTCLOUD07 by ckrygier. It has a virus total score of 5/57. Malware processes (youtube_downloader_hd_setup (1).exe, youtube_downloader_hd_setup (1).tmp, youtube_downloader_hd_setup. Tmp and youtube_downloader_hd_setup.exe) were created on system MINNIE by the user Catherine. It has a virus total score of 20/57.
23-Oct-18	TCP connection was established between MAILS55 and external IP addresses XX.145.220.201 (China) and XXX.71.213.9 (China) on port 25 (SMTP).
18-Oct-18	TCP connection was established to MAILS55 from multiple remote IP addresses.
21-Sep-18	New process uTorrent.exe was created and connected to an external IP address (XX.192.0.105 – United States) on the system CTCLOUD07 by the user Craig. It has a virus total score of 6/57.
24-Sep-18	Dictionary attack observed on system "MAILS55" from multiple external sources. 473 usernames were seen (in alphabetical order A-X) attempting to logon but failed. User accounts "admin", "db2admin"and "administrator" were used 81, 371 and 473 times respectively."
30-Sep-18	355 logon failures for the user accounts (POST1 and Administrator) from the external IP address (XX.242.255.196 (Luxembourg) and XX.252.231.222 (Hong Kong)) on the system CTCLOUD02.

Critical Observations
Changes to identity and Access Policies

Netsurion | EventTracker

Member added to/removed from security-enabled groups							
Monitoring Activity	Date	Admin	Member	System	Group Name	Operation	Group Type
Changes to Identity and Access Policies	12-Nov-18	Admin2	Britto	TGR01	Administrators	Added	Local
	17-Oct-18		BKumar	LEXICON			

Password set to never expire			
Date	User name	Admin	Computer
12-Nov-18	QBServiceDataUser24	BKumar	LEXICOM
30-Oct-18	Joshua	Admin3	CMCLOUD07
16-Sep-18	Sqlactrptsvc	Admin1	RP13SVM1
	Sqlactexec		

Critical Observations
Application Activity

Monitoring Activity	Date	Description
Application Activity	9-Nov-18	New application "BITTORRENT" has been installed on the system" Wkstn8". This could be a policy violation.
	28-Nov-18	New process ScreamingFrogSEOSpider.exe was created on the system Contoso-91-SUPP. User (Jane) was logged in during this event.
Change Management Reports to Identify Resource Access Exceptions	11-Oct-18	An Agent Configuration is modified by Admin2 on the system MELON.
		Software Birthday Reminder was installed on the system APRICOT.
	21-Sep-18	Agent Configuration was modified by Jayne on system TURTLE2.

Critical Observations
System Resources

Netsurion | EventTracker

Low Disk space				
Date	**System**	**Drive**	**Free Space**	**Disk space**
11-Nov-18	RAINFALL2	Drive: C	851 MB	12284 MB
12-Nov-18			819 MB	
13-Nov-18			822 MB	
26-Oct-18			855 MB	
17-Oct-18			860 MB	
08-Oct-18			883 MB	149 GB
04-Oct-18			856 MB	
20-Sep-18			858 MB	
13-Sep-18			854 MB	12284 MB
11-Sep-18			806 MB	
06-Sep-18			852 MB	
01-Sep-18				

Configuration Specifications

	Particulars	
Deployment Type	EventTracker SIEMphonic	EventTracker SIEMphonic
Console Type	Collection Master	Collection Point
Version	9.0 Build 18	9.0 Build 18
License Serial No.	45836087007000197d	5962950400030014O7p
Installation Date	13-Jun-16	13-Jun-16
System Configuration	Windows Server 2012 R2 Standard Processor : 2.27GHz (2 Processors) RAM : 24 GB System Type : 64-bit Hard Disk : 1397 GB, 466 GB	Windows Server 2012 R2 Datacenter Processor : 2.90GHz (1 Processor) RAM : 12 GB System Type : 64-bit Hard Disk :100 GB, 365 GB

Configuration Specifications

Netsurion | EventTracker

Collection Master

License Options/Features	Status	Available	Used
BSM Agents	Available	Unlimited	0
Change Audit Servers	Available	Unlimited	17
Change Audit Workstations	Available	Unlimited	15
Check Point	Available	Unlimited	0
Clusters	Not Available	0	0
DLA	Available	Unlimited	58
ET Servers Agent	Available	Unlimited	29
ET Servers Agent less	Available	Unlimited	0
ET Work Stations	Available	Unlimited	20
ET Work Stations Agent less	Available	Unlimited	0
NetFlow	Available	Unlimited	0
SNMP	Available	Unlimited	0
Status Tracker Resources	Available	Unlimited	97
syslog	Available	Unlimited	18
syslog VCP	Available	Unlimited	2
VMware	Available	Unlimited	2
Windows VCP	Available	Unlimited	5

Collection Point

License Options/Features	Status	Available	Used
BSM Agents	Available	Unlimited	0
Change Audit Servers	Available	Unlimited	2
Change Audit Workstations	Available	Unlimited	2
Check Point	Available	Unlimited	0
Clusters	Not Available	0	0
DLA	Available	Unlimited	59
ET Servers Agent	Available	Unlimited	8
ET Servers Agent less	Available	Unlimited	0
ET Work Stations	Available	Unlimited	47
ET Work Stations Agent less	Available	Unlimited	0
NetFlow	Not Available	0	0
SNMP	Available	Unlimited	0
Status Tracker Resources	Available	Unlimited	33
syslog	Available	Unlimited	2
syslog VCP	Available	Unlimited	2
VMware	Available	Unlimited	0
Windows VCP	Available	Unlimited	6

Action items from last review with status

Action Item	Responsibility	Status
Share report with source IP addresses for the “Administrator” account logon failures that occurred on Oct 26, 2018	SOC team	Shared on Nov 12, 2018
Details of Privileged users and systems that are to be monitored going forward	Client Contact	To be confirmed
Office 365 integration to EventTracker	SOC Team / Client Contact	Pending - To be discussed
Upgrade to 9.1.19	SOC Team	Scheduled for Jan 4, 2019
Suppress high number of logon failures from systems HAVOC02 and IRONMAN01	SOC Team	Completed on Nov 06, 2018