INDEPENDENT COMMUNICATIONS AUTHORITY OF SOUTH AFRICA

SIEM BRIEFING SESSION

14 AUGUST 2019

Network and Server environment

- Head Office with centralized data centre
- 8 regional offices with 2 servers each
- Regions connect via 4Mbps MPLS network
- CISCO core and edge switches (approx. 40 in total)
- FortiGate Firewall owned and managed at ISP
- CISCO firewalls at all ICASA sites

- Approx. 100 virtual servers
- 3 AD servers at head office and read only domain controllers in each region
- 80% Window OS and remaining are Linux
- 1 ORACLE DB and approx. 10 MS SQL DBs
- Centralised storage on Tintri

Primary Systems in use

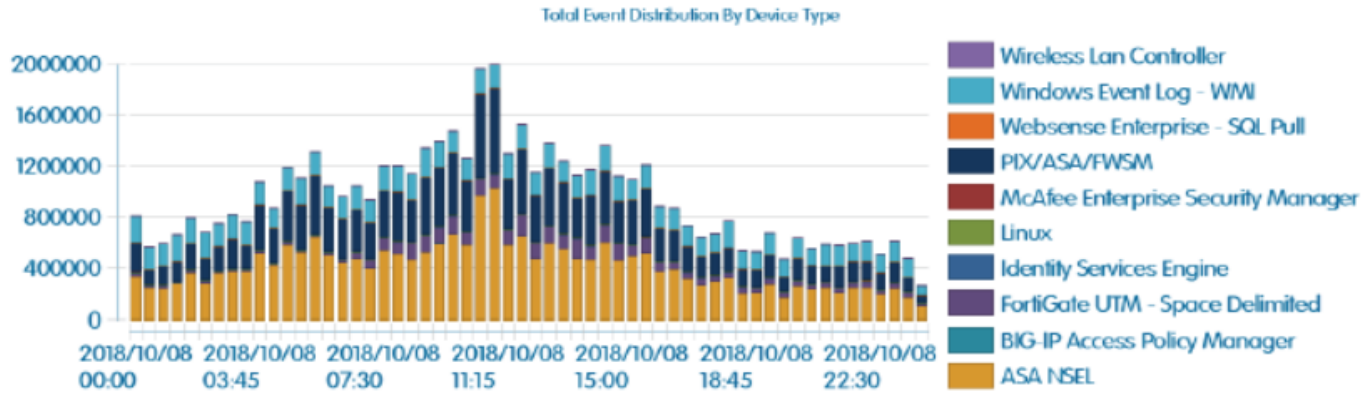
- Financial – JDE Enterprise 9.2 (Linux OS and ORACLE DB)
- HR – VIP and CBARS (SQL DB)
- CRM – Microsoft Dynamics 2013 (SQL DB)
- Licensing – Sky Manager And WRAP (Linux OS and SQL DB)
- Document Management – Alfresco (PostgreSQL DB)
- Email – Microsoft Exchange 2016
- Telephony – Skype for Business and Audiocode gateways

Other software in use

- CISCO ISE
- McAfee EPO
- Nexpose vulnerability scanner (to be replaced with Nessus within 3 months)
- Websense (Forcepoint Security Manager)
- F5 Big IP (Application Server Manager)

Minimum SIEM Requirements

- Average daily event rate of 50 000 000 events per day (>70% WMI,ISP and Internal Firewall)
- CSOC managed 24/7
- Provide a CERT support in case of computer security emergencies
- Provide ad hoc reports when needed for purpose of compliance with both Internal and External Auditors
- Regular meetings to address any concerns with reporting or SLA



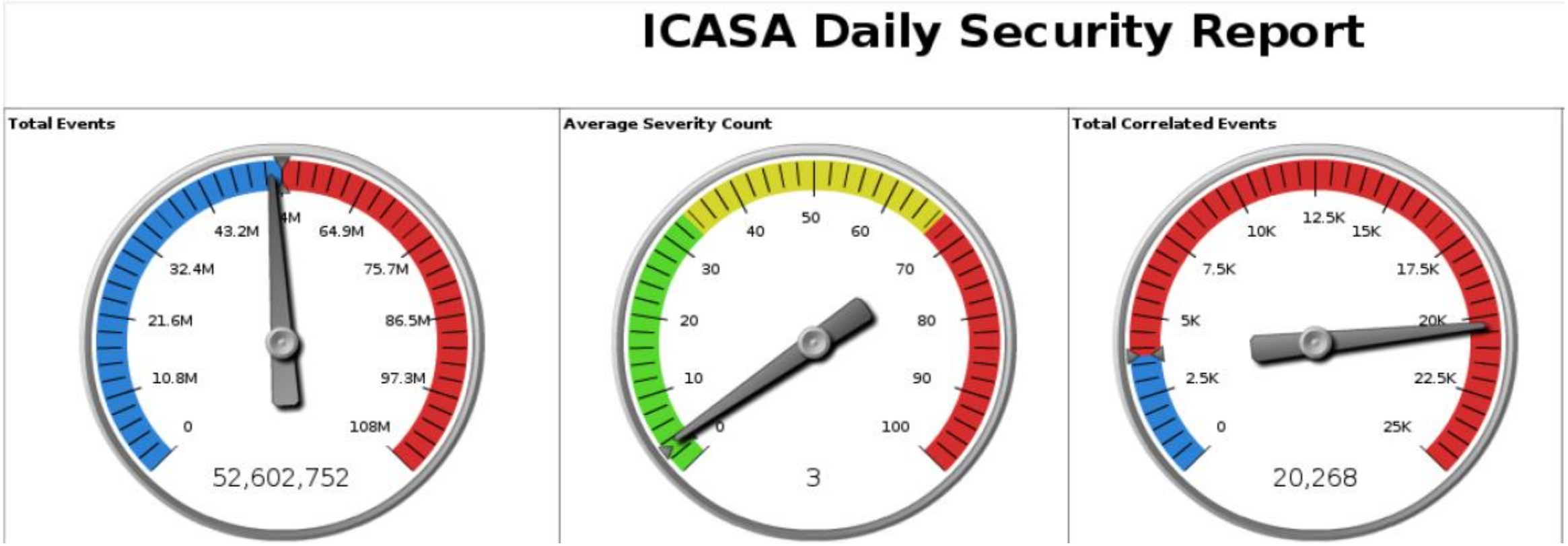
Minimum reporting requirements

Daily report - Analysis of security events for the past 24-hours with recommendations

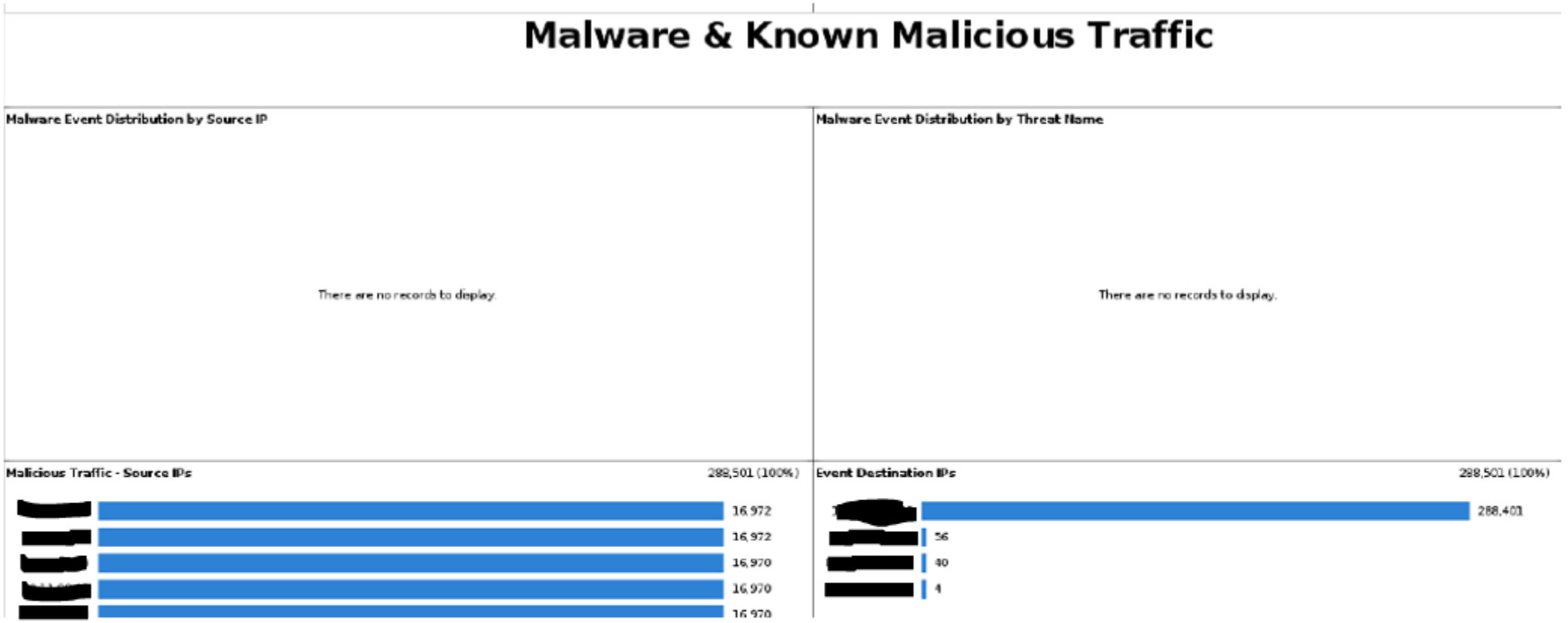
- Active Directory activities: failed login accounts, multiple logon from same accounts, AD configuration and changes
- Traffic to known malicious sites
- Suspicious traffic using backdoor ports
- Perimeter Security- external IPs communicating with internal IPs, External perimeter scans,
- Correlated internal recon events: internal IP scanning
- Malware events
- Database activity Monitoring (SQL X 3 and Oracle X 1)
  - Report of all SQL activities showing who, when, source, destination, command

Reporting

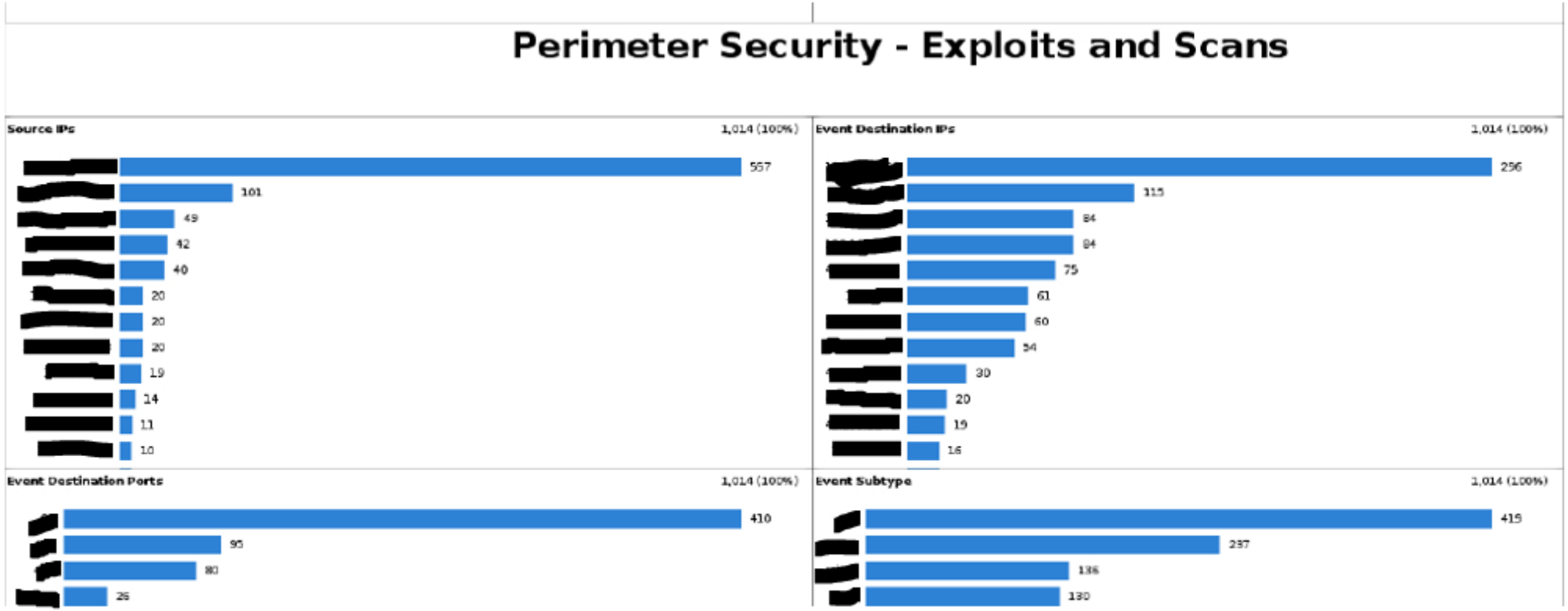
- Average daily events rate of 50M events



Reporting

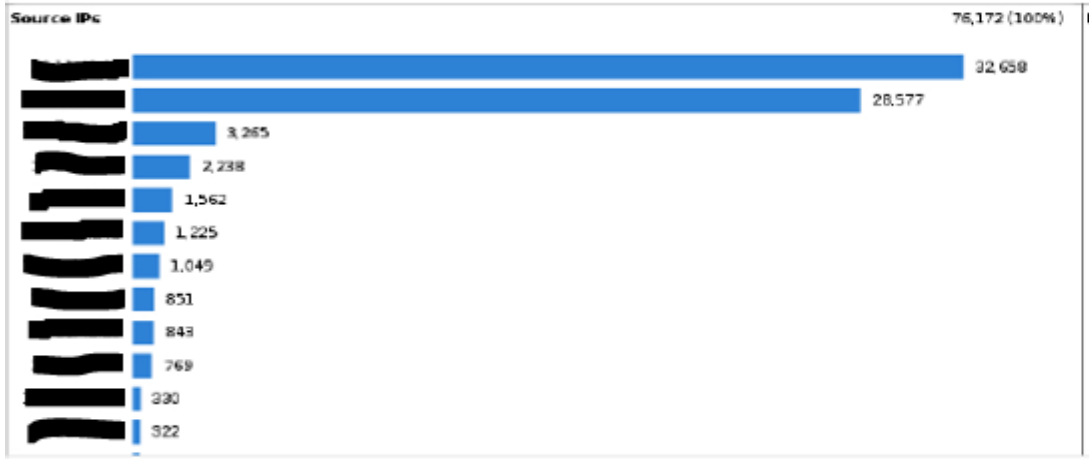

Malware & Known Malicious Traffic
Malware Event Distribution by Source IP
There are no records to display.
Malware Event Distribution by Threat Name
There are no records to display.
Malicious Traffic - Source IPs
288,501 (100%)
16,972
16,972
16,970
16,970
16,970
Event Destination IPs
288,501 (100%)
288,401
56
40
4

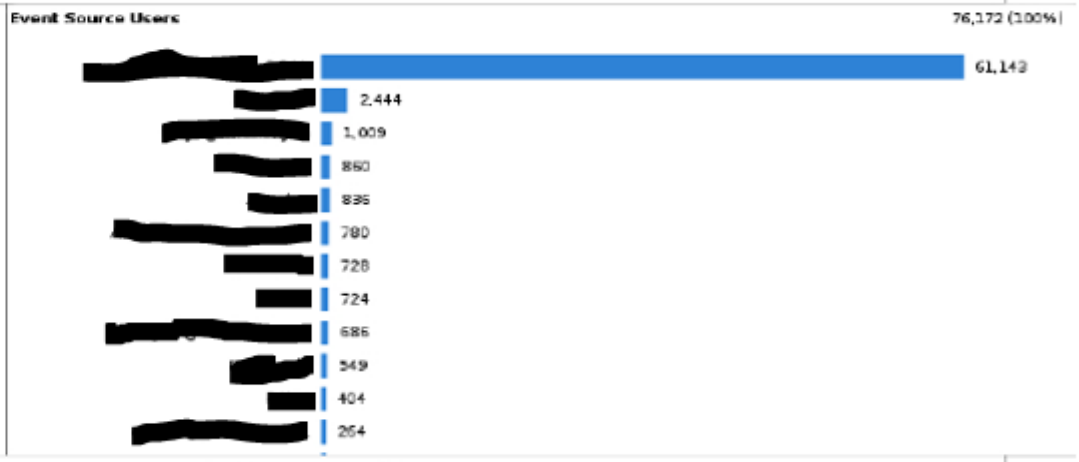
Reporting


Perimeter Security - Exploits and Scans
Source IPs
1,014 (100%)
557
101
49
42
40
20
20
20
19
14
11
10
Event Destination IPs
1,014 (100%)
256
115
84
84
75
61
60
54
30
20
19
16
Event Destination Ports
1,014 (100%)
410
95
80
26
Event Subtype
1,014 (100%)
415
237
136
130

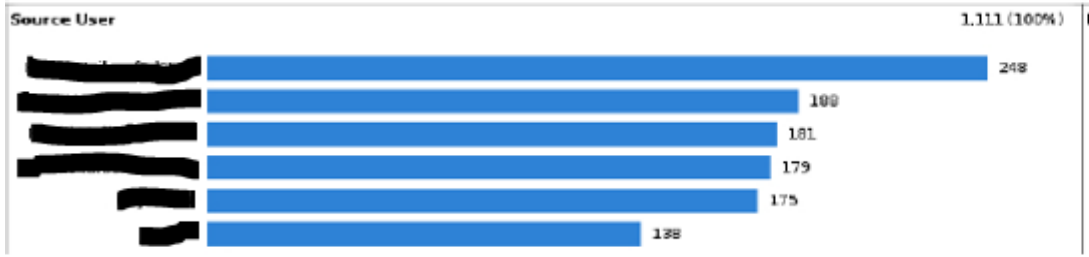
Reporting

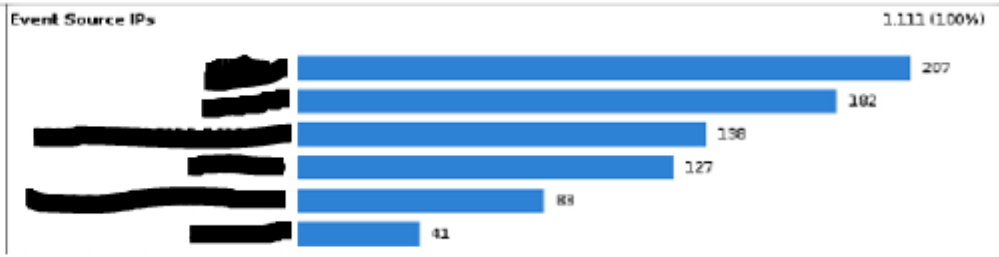
Failed Service Account Logins





Users Logged in from Multiple Clients





Weekly Reporting

Weekly reports- IT Administrators Activities

- Weekly Active Directory changes and configuration
- Weekly logon activities on Core Servers (Linux and Windows)
- Weekly Database administrator activities and changes. SQL and Oracle

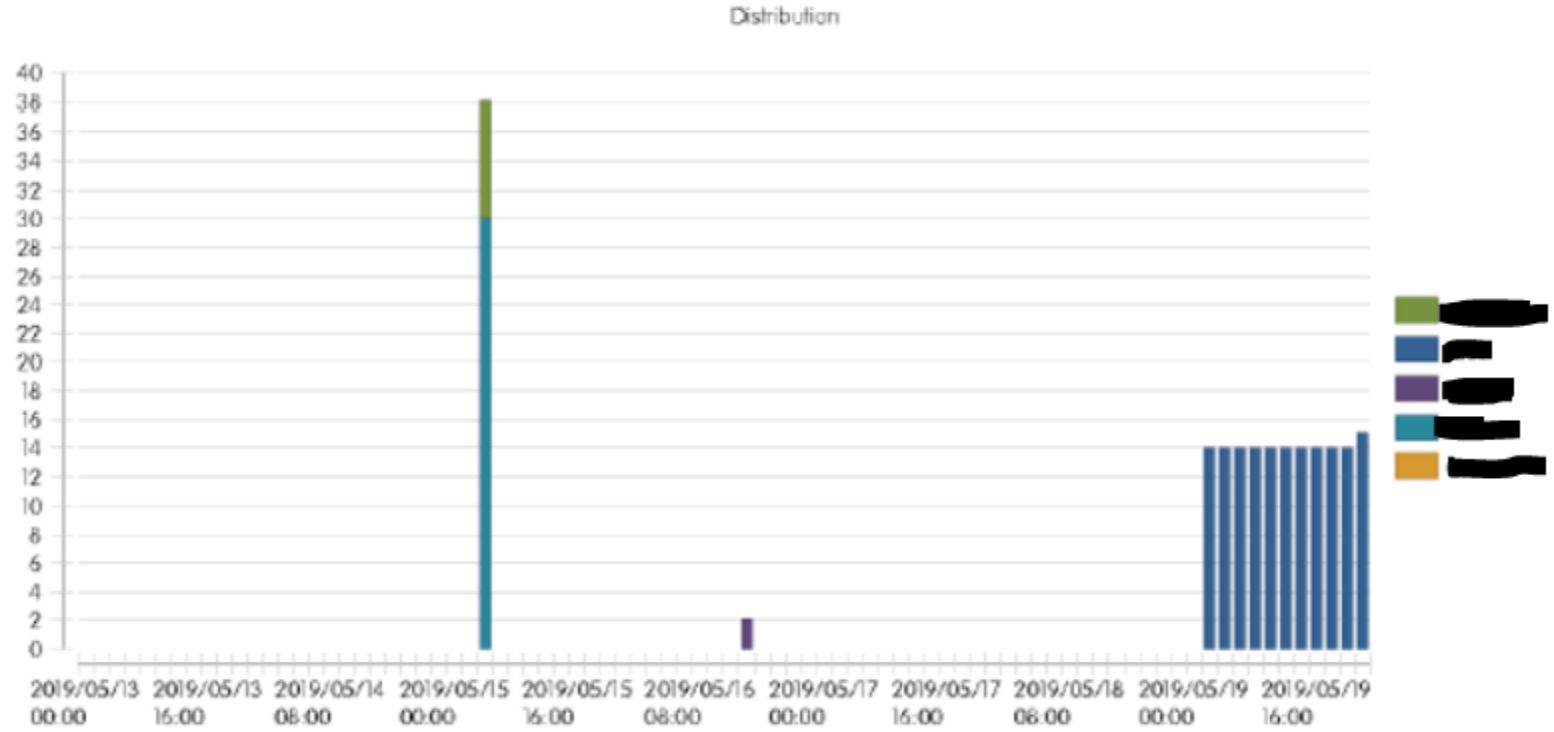
Weekly Reporting

Active Directory Changes

Last Time	Rule Message	Source User	Destination User	Object
2019/05/29 22:22:41	Domain Policy - User Changed Another Users Password	[redacted]	[redacted]	
2019/05/29 18:04:32	Domain Policy - User Changed Another Users Password	[redacted]	[redacted]	
2019/05/29 11:19:26	Domain Policy - User Added to Domain Security Group	[redacted]	[redacted]	[redacted]
2019/05/29 10:34:34	Domain Policy - User Changed Another Users Password	[redacted]	[redacted]	
2019/05/28 13:04:11	Domain Policy - User Changed Another Users Password	[redacted]	[redacted]	

Weekly Reporting

Event Distribution: Authentication Events



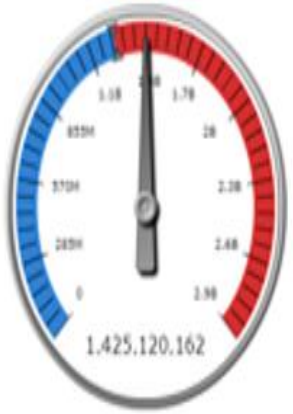
Minimum monthly reporting requirements

- Monthly executive report – overview of all security events for the month with Risk indicator/Security Posture, SLA indicator, Malware overview, Top failed AD account & Top lockouts, Perimeter security,
- Network changes report- Firewall changes
- Monthly Active Directory changes report

Monthly Reporting

3 Month Severity Trend

	April 2018	May 2018	June 2018
Trend Constant	3 %	3 %	3 %



Average Monthly Events rate 1.5B

SLA Compliance

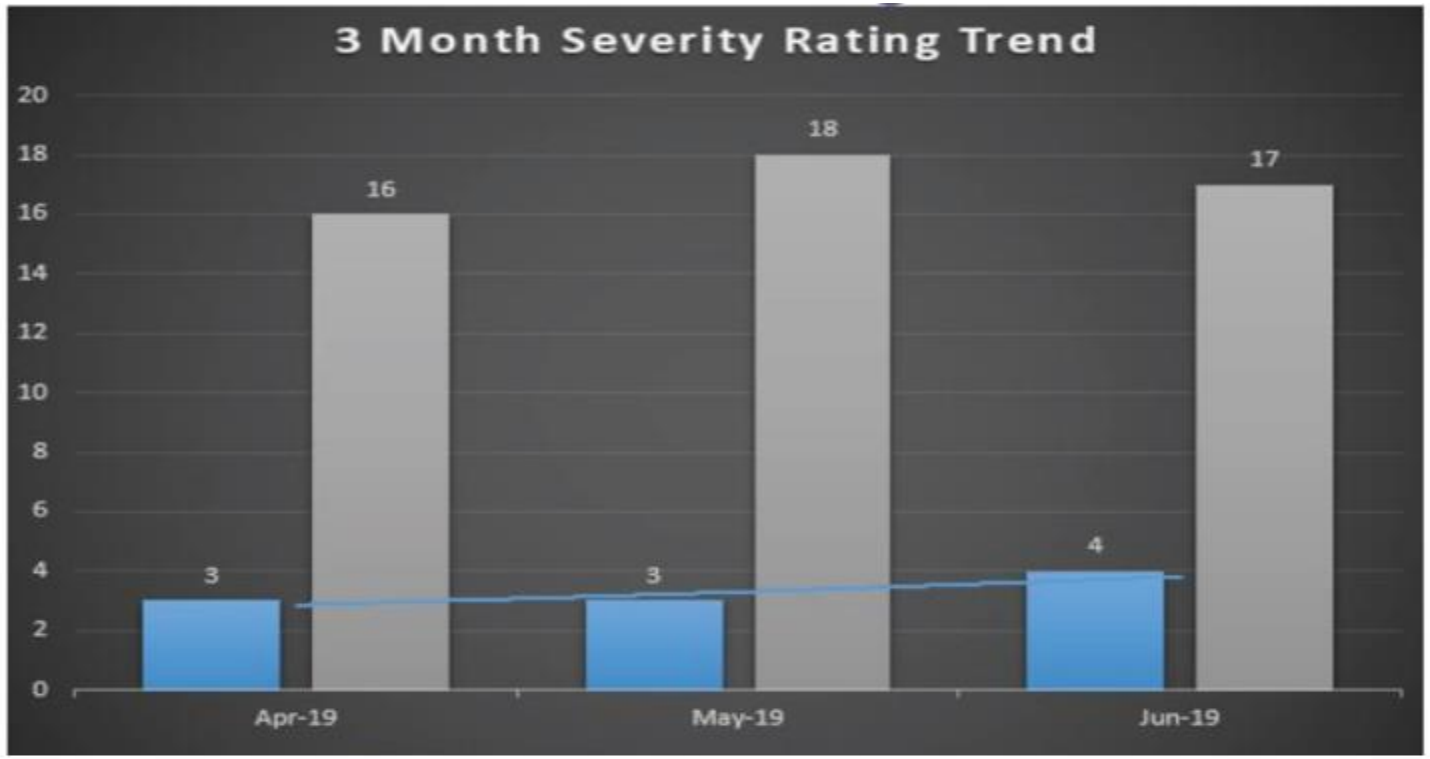
SLA Status Breakdown for June 2018

SLA Priority	0% - 49%	50% - 74%	75% - 89%	90% - 99%	BREACHED	Grand Total
1	0	0	0	0	0	**0**
3	3	2	1	1	**6**	**13**
5	0	0	0	0	0	**0**
Grand Total	**3**	**2**	**1**	**1**	**6**	**13**

Current SLA Compliance Status: 53.8% (6 calls were breached out of a total of 13)

Monthly Reporting

Risk Rating: Icasa vs Other Clients



Alerting




Email alerts on the following

Instant alerts on suspicious activities via email

- Active directory group policy changes
- All Firewall changes
- Suspicious traffic to malicious hosts not blocked by firewall
- Traffic using backdoor ports not blocked by firewall
- Malware events not mitigated by end point protection

Telephone alerts

- 24/7 telephone notifications and escalations on any high risk security alert or breach


Thank You