Managed Security Service
Monthly Report

ACME

May 2017

IPSec SOC: https://soc.ipsec.com.au/
Changes: change@portal.ipsec.com.au
Incidents: incident@portal.ipsec.com.au
Phone: 1300 890 902
Fax: 1300 890 912

IPSec Pty Ltd - http://www.ipsec.com.au/

Table of Contents

Introduction

IPSec has been engaged by ACME to provide ongoing Managed Security Services (MSS) for the purpose of facilitating effective monitoring and management of the organisation's nominated information asset protection solutions and to provide effective response in the event that an issue arises as a consequence of or detected by those asset protection solutions.

As part of the provided MSS, IPSec provides ACME with a monthly report describing the activities and actions of the previous month's service delivery and which describes the performance of the solutions under management for that same period. This report, the monthly MSS report, details all changes made to the solution(s) by IPSec on ACME's behalf, all incidents responded to that occurred during the reporting period and the operational performance of the solutions under management.

The asset protection solutions managed by IPSec on behalf of ACME include the following:

- Firewall
  - The firewall provides the organisation's main internet gateway firewalling capabilities to provide internal systems and personnel with controlled access to the Internet, as well as to allow inbound access to a number of public facing sytems and external contractor access.
- Scanner
  - A vulnerability Scanner to assess the current security state of various systems.

Should you have any questions or concerns regarding the content of this report, please do not hesitate to contact the IPSec SOC on 1300 890 902 or via incident@portal.ipsec.com.au

This report includes the following sections, providing the following information:

- Raised MSS Incidents
- This section of the report describes all security or device incidents that were responded to by IPSec during the reporting period. A device incident is any incident that impacts the operational performance of the solution(s) under management by IPSec. A security incident is any incident that may impact the asset protection integrity of ACME detected by IPSec as a consequence of monitoring and managing ACME's asset protection solution(s).
- Resolved MSS Incidents
- This section of the report describes all security or device incidents that were resolved during the reporting period. A resolved incident is an incident where the issue identified has been investigated and/or mitigated to the satisfaction of both IPSec and ACME.
- Unresolved MSS Incidents
- This section of the report describes all security or device incidents that were unresolved at the conclusion of the reporting period.
- Raised MSS Changes
- This section of the report describes all solution changes that were requested, either by ACME's authorised representatives or by IPSec on behalf of ACME, during the reporting period.
- Resolved MSS Changes
- This section of the report describes all solution changes that were completed within the reporting period. A change is deemed by IPSec to be completed when the requirements of the change request have been fulfilled to the satisfaction of both IPSec and ACME.
- Unresolved MSS Changes
- This section of the report describes all solution changes that were not completed at the conclusion of the reporting period.
- Security Updates

- This section of the report details what updates were applied to ACME's asset protection solution(s) managed by IPSec as a result of an automated update process (e.g. one provided by the solution's vendor) and not as a result of a specific change request.

- Solution Performance
- This section of the report provides statistical data to represent the operational performance of the asset protection solution(s) managed by IPSec on behalf of ACME. Details describing how the managed solution is performing its primary, and other, functions may be identified within this section of the report.

Service Delivery Report

Raised MSS Incidents

This section of the report describes all security or device incidents that were responded to by IPSec during the reporting period. A device incident is any incident that impacts the operational performance of the solution(s) under management by IPSec. A security incident is any incident that may impact the asset protection integrity of ACME detected by IPSec as a consequence of monitoring and managing ACME's asset protection solution(s).

id	Subject				
	Client	Priority	Status	Date Reported	Date Closed
102466	**Please investigate delay in request processing**				
	Fred Nerf	Medium	Open	22/05/2017 11:17:00 AM	

Resolved MSS Incidents

This section of the report describes all security or device incidents that were resolved during the reporting period. A resolved incident is one where the issue identified has been investigated and/or mitigated to the satisfaction of both IPSec and ACME.

There were no MSS Incidents resolved during the reporting period.

Unresolved MSS Incidents

This section of the report describes all security or device incidents that were unresolved at the conclusion of the reporting period.

id	Subject				
	Client	Priority	Status	Date Reported	Date Closed
102466	**Please investigate delay in request processing**				
	Fred Nerf	Medium	Open	22/05/2017 11:17:00 AM	

Raised MSS Changes

This section of the report describes all solution changes that were requested, either by ACME's authorised representatives or by IPSec on behalf of ACME, during the reporting period.

id	Subject				
	Client	Priority	Status	Date Reported	Date Closed
102467	**Please create a new monthly report**				
	Fred Nerf	Medium	Open	22/05/2017 11:19:00 AM	

Resolved MSS Changes

This section of the report describes all solution changes that were completed within the reporting period. A change is deemed by IPSec to be completed when the requirements of the change request have been fulfilled to the satisfaction of both IPSec and ACME.

There were no MSS Changes resolved during the reporting period.

Unresolved MSS Changes

This section of the report describes all solution changes that were not completed at the conclusion of the reporting period.

id	Subject				
	Client	Priority	Status	Date Reported	Date Closed
102467	**Please create a new monthly report**				
	Fred Nerf	Medium	Open	22/05/2017 11:19:00 AM	

Daily Systems Review

This section of the report summarises the Daily Systems Review activities conducted by IPSec.

No Daily Systems Reviews were conducted during the reporting period.

Guard Service Report

IPSec Guard Report

This is the IPSec Guard Service Report intro.

This section of the report contains:

- Raised Incidents
- Resolved Incidents
- Unresolved Incidents
- Raised Changes
- Resolved Changes
- Unresolved Changes

Appendices

- Log Volume: Executive Summary
- Log Volume: By Log Source
- Security Events: Executive Summary

IPSec Guard Service Delivery Report

IPSec Guard Incidents Raised

IPSec Guard Incidents created by or on behalf of ACME during the reporting period.

id	Subject				
	Client	Priority	Status	Date Reported	Date Closed
102464	**IPSec Guard Alarm - Risk: 97 - Name: AIE: Compromise: Corroborated Data Access Anomalie**				
	Fred Nerf	Medium	Open	22/05/2017 11:13:00 AM	
102463	**IPSec Guard Alarm - Risk 100 - Name: Alarm on Malware Rule**				
	Fred Nerf	Medium	Open	22/05/2017 11:08:00 AM	

IPSec Guard Incidents Closed

IPSec Guard Incidents closed by or on behalf of ACME during the reporting period.

There were no IPSec Guard Incidents closed during the reporting period.

IPSec Guard Incidents Unresolved

Unresolved IPSec Guard Incidents for ACME at the end of the reporting period.

id	Subject				
	Client	Priority	Status	Date Reported	Date Closed
102464	**IPSec Guard Alarm - Risk: 97 - Name: AIE: Compromise: Corroborated Data Access Anomalie**				
	Fred Nerf	Medium	Open	22/05/2017 11:13:00 AM	
102463	**IPSec Guard Alarm - Risk 100 - Name: Alarm on Malware Rule**				
	Fred Nerf	Medium	Open	22/05/2017 11:08:00 AM	

IPSec Guard Changes Raised

IPSec Guard changes raised by or on behalf of ACME during the reporting period.

id	Subject			
	Client	Status	Date Reported	Date Closed
102465	Fred Nerf	Pending Approval	22/05/2017 11:14:00 AM	

IPSec Guard Changes Resolved

IPSec Guard changes closed by or on behalf of ACME during the reporting period.

There were no IPSec Guard Changes closed during the reporting period.

IPSec Guard Changes Unresolved

IPSec Guard changes unresolved for ACMEat the end of the reporting period.

id	Subject			
	Client	Status	Date Reported	Date Closed
102465	Fred Nerf	Pending Approval	22/05/2017 11:14:00 AM	

Log Volume

Executive Summary

By Entity

Monday, 1 May 2017 12:00 AM to Thursday, 1 June 2017 12:00 AM AUSEST (UTC+10:00)

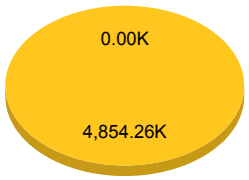
Log Volume
Executive Summary
By Entity
Monday, 1 May 2017 12:00 AM to Thursday, 1 June 2017 12:00 AM AUSEST (UTC+10:00)

Entity: ACME Inc

Logs Collected	4,854,263			The total number of log entries collected
Logs per day/sec	156,589	1.810		The average number of log entries collected per day and second
Archived Logs	4,854,263	100.00	%	Of the collected logs, the number that were archived.
Online Logs	4,854,263	100.00	%	Of the collected logs, the number that were online.
Identified Logs	4,854,259	100.00	%	Of the collected logs, the number that were identified.
Events Forwarded	33,948	0.70	%	Of the collected logs, the number that were forwarded as an event.
Events per day/sec	1,095	0.010		The average number of events forwarded per day and second

For ACME Inc

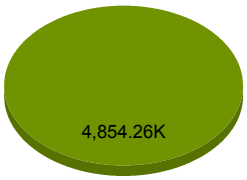
Identified Logs vs Unidentified Logs



Unidentified Logs	0.00K	0.0%
Identified Logs	4,854.26K	100.0%
Total:	4,854.26K	100.0%

For ACME Inc

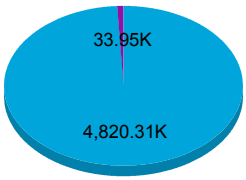
Archived vs Non-Archived Logs



Non-Archived Logs	0.00K	0.0%
Archived Logs	4,854.26K	100.0%
Total:	4,854.26K	100.0%

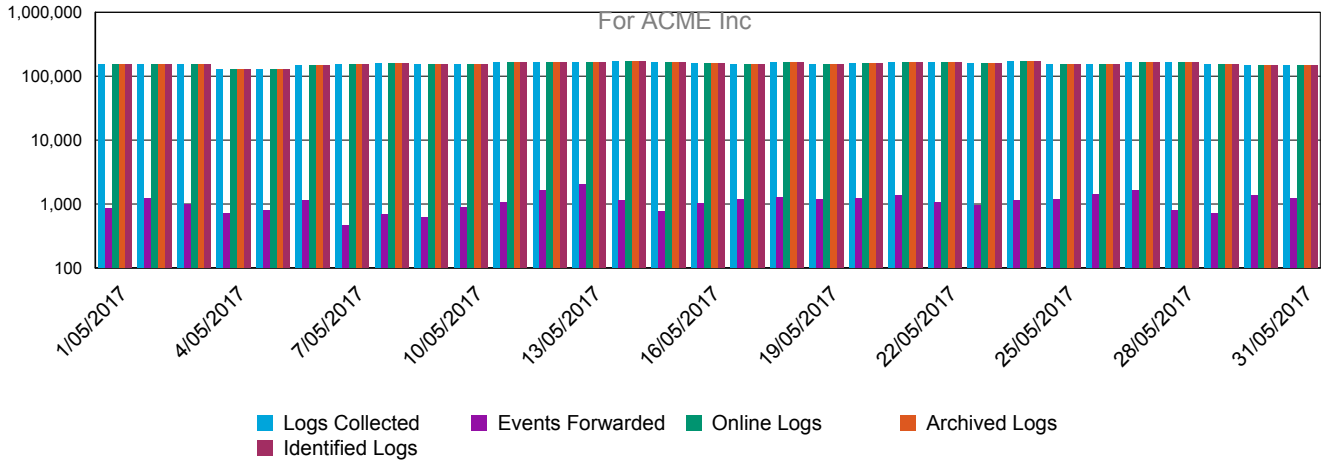
For ACME Inc

Logs vs. Events



Non-Event Logs	4,820.31K	99.3%
Events	33.95K	0.7%
Total:	4,854.26K	100.0%

Logs & Events per Day



Log Volume

By Log Source

Monday, 1 May 2017 12:00 AM to Thursday, 1 June 2017 12:00 AM AUSEST (UTC+10:00)

Log Volume
By Log Source
Monday, 1 May 2017 12:00 AM to Thursday, 1 June 2017 12:00 AM AUSEST (UTC+10:00)

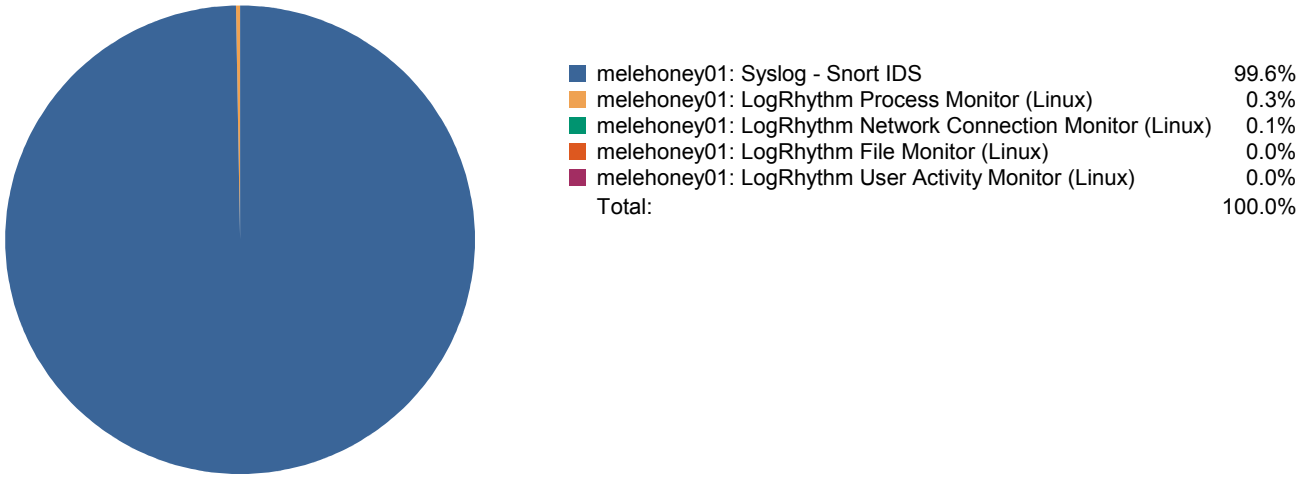
Entity: ACME Inc

Log Source Type

Log Host	Log Source Name	Total Logs	Logs/d	Logs/s	% Evt	% Id	% Arc	% On

Top 7 Log Sources

For ACME Inc



LogRhythm File Monitor (Linux)

melehoney01		LinuxFileMon	735	24	0.000	100.00	100.00	100.00	100.00
Total:	LogRhythm File Monitor (Linux)		735	24	0.000	100.00	100.00	100.00	100.00

LogRhythm Network Connection Monitor (Linux)

melehoney01		NetworkConnectionMonitor	3,390	109	0.000	0.00	100.00	100.00	100.00
Total:	LogRhythm Network Connection Monitor (Linux)		3,390	109	0.000	0.00	100.00	100.00	100.00

LogRhythm Process Monitor (Linux)

melehoney01		ProcessMonitor	12,933	417	0.000	0.00	99.97	100.00	100.00
Total:	LogRhythm Process Monitor (Linux)		12,933	417	0.000	0.00	99.97	100.00	100.00

LogRhythm User Activity Monitor (Linux)

melehoney01		UserActivityMonitor	156	5	0.000	0.00	100.00	100.00	100.00
Total:	LogRhythm User Activity Monitor (Linux)		156	5	0.000	0.00	100.00	100.00	100.00

Syslog - Snort IDS

melehoney01		10.3.11.40 Snort IDS	4,837,049	156,034	1.810	0.69	100.00	100.00	100.00

Log Volume

By Log Source

Monday, 1 May 2017 12:00 AM to Thursday, 1 June 2017 12:00 AM AUSEST (UTC+10:00)

Entity: ACME Inc

Log Source Type

Log Host	Log Source Name	Total Logs	Logs/d	Logs/s	% Evt	% Id	% Arc	% On
Total:	Syslog - Snort IDS	4,837,049	156,034	1.810	0.69	100.00	100.00	100.00
Entity Total		4,854,263	156,589	1.810	0.70	100.00	100.00	100.00
Grand Total		4,854,263	156,589	1.810	0.70	100.00	100.00	100.00

IPSec Guard: Monthly Event Executive Summary

By Entity

Monday, 1 May 2017 12:00 AM to Thursday, 1 June 2017 12:00 AM AUSEST (UTC+10:00)

Report prepared as part of IPSec Guard: ACME: Monthly Digest for IPSecPtyLtd on 20/06/2017 4:37 PM AUSEST (UTC+10:00)

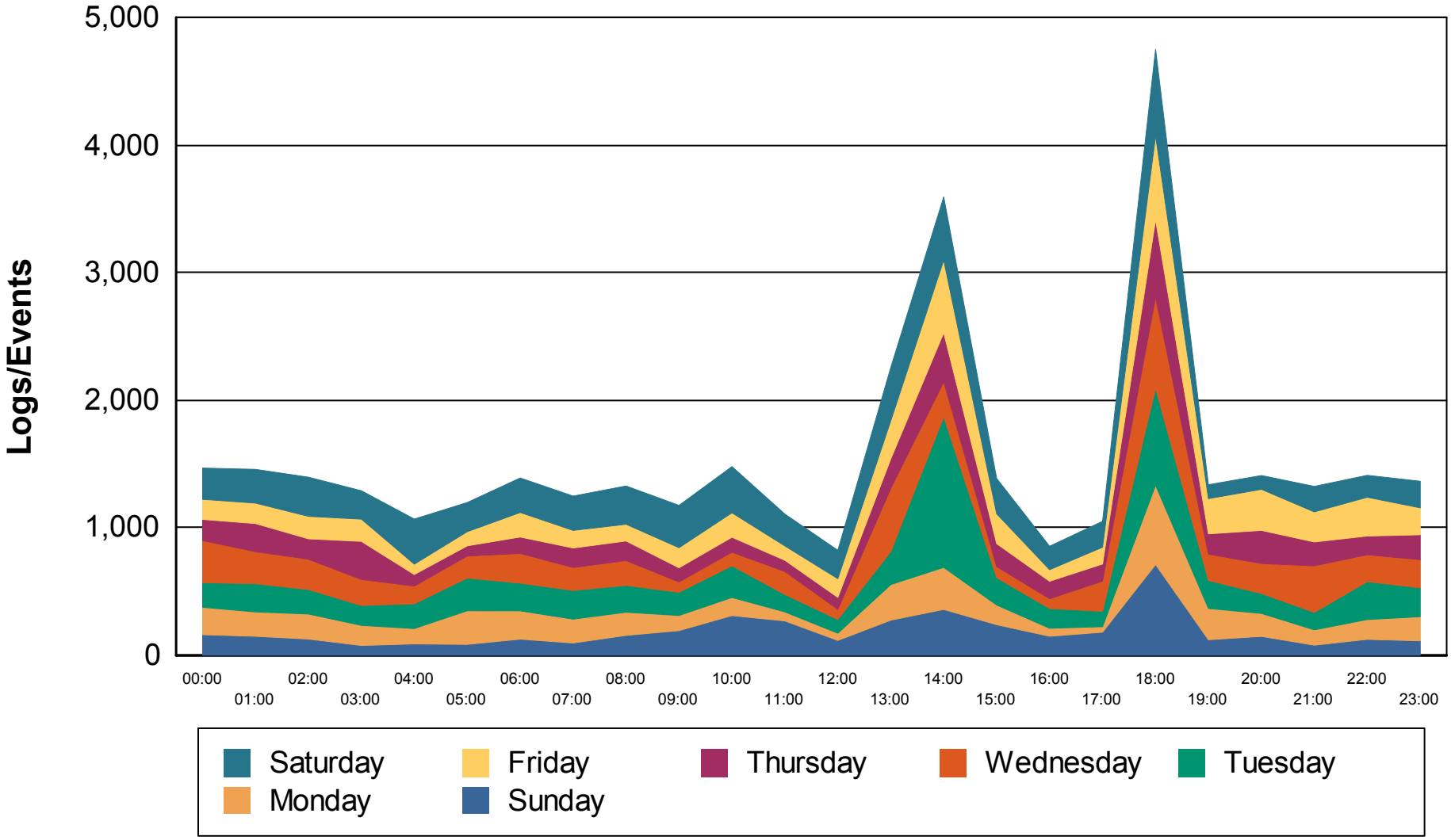
IPSec Guard: Monthly Event Executive Summary

By Entity

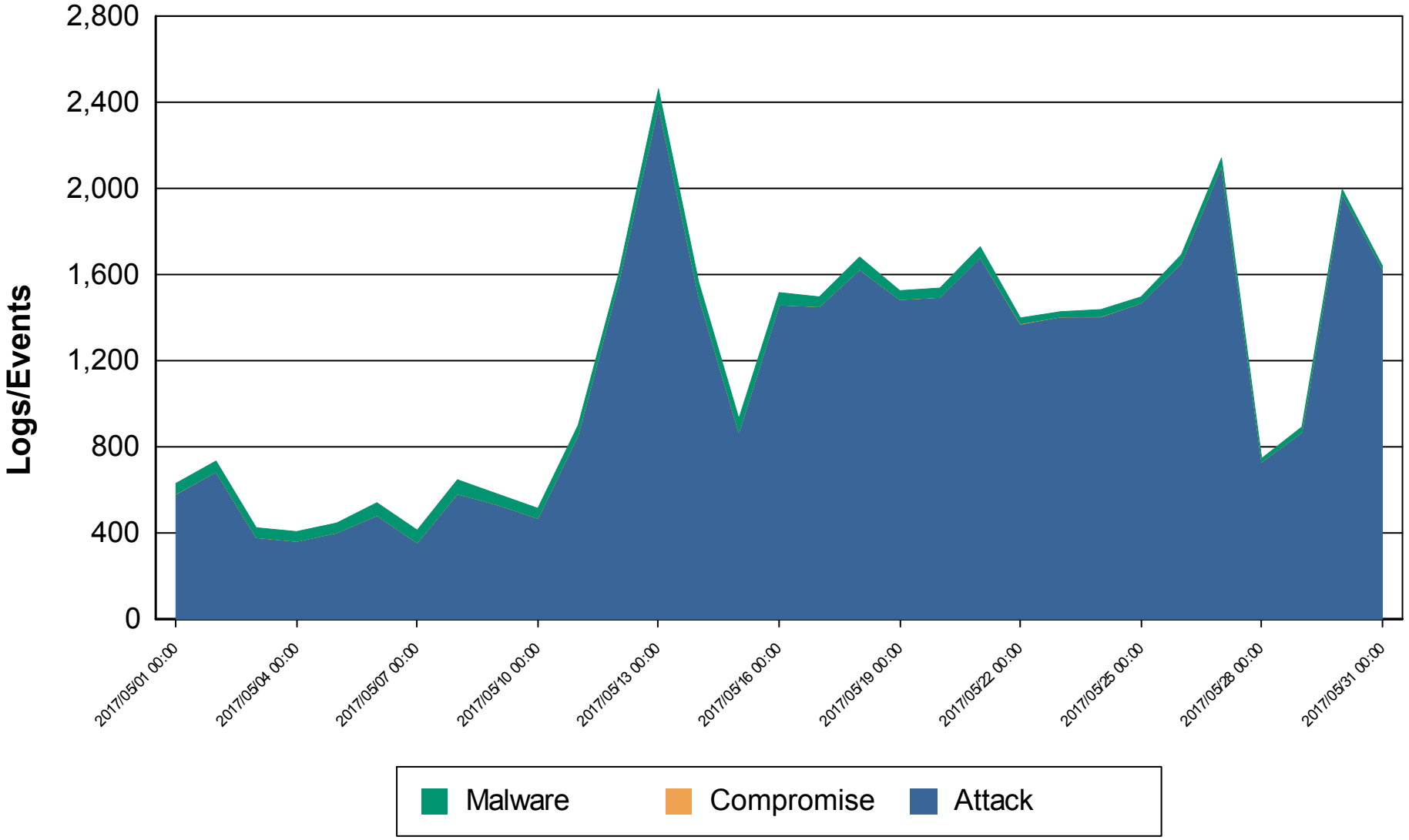
Monday, 1 May 2017 12:00 AM to Thursday, 1 June 2017 12:00 AM AUSEST (UTC+10:00)

Impacted Entity: All

Logs/Events By Day Of Week And Hour Of Day



Logs/Events By Classification By Time



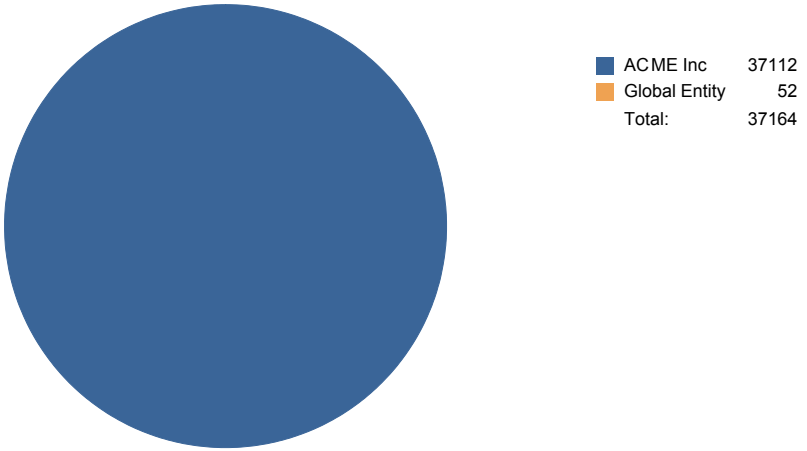
IPSec Guard: Monthly Event Executive Summary

By Entity

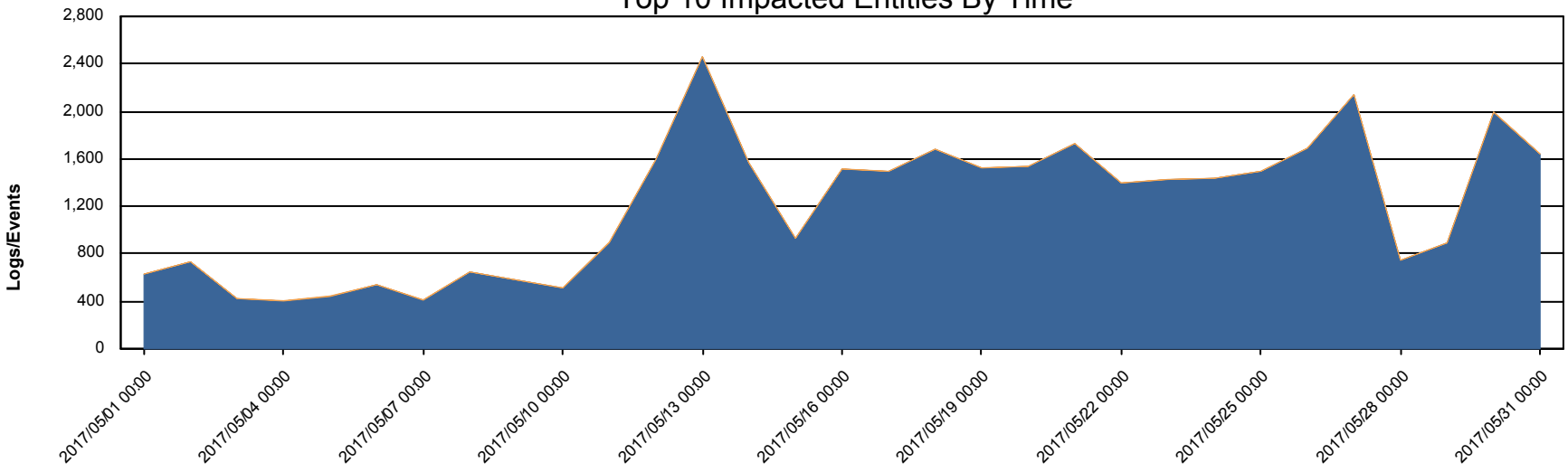
Monday, 1 May 2017 12:00 AM to Thursday, 1 June 2017 12:00 AM AUSEST (UTC+10:00)

Impacted Entity: All

Top 10 Impacted Entities



Top 10 Impacted Entities By Time



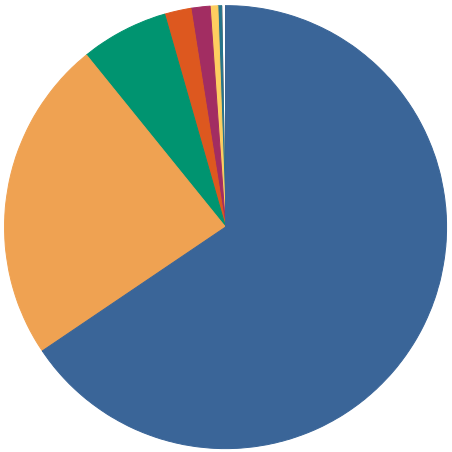
IPSec Guard: Monthly Event Executive Summary

By Entity

Monday, 1 May 2017 12:00 AM to Thursday, 1 June 2017 12:00 AM AUSEST (UTC+10:00)

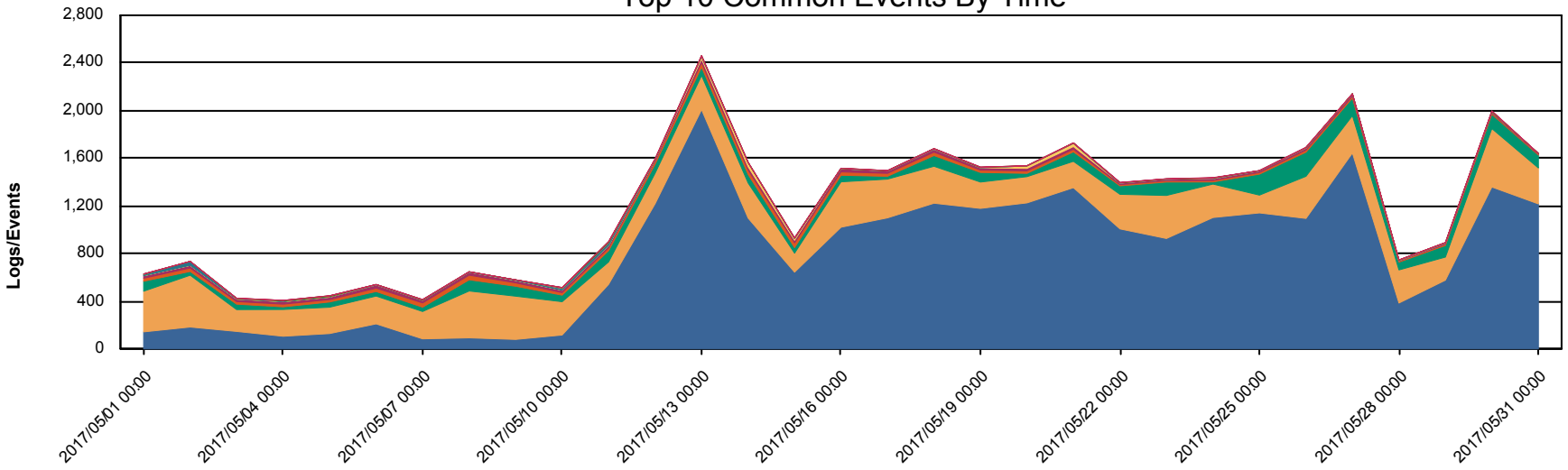
Impacted Entity: All

Top 10 Common Events



AIE: IPSec Guard: ISO-27001: Attack Detected Rule	24357
General Attack Activity	8789
Buffer Overflow/Underflow	2360
Detected Worm Activity	698
AIE: IPSec Guard: ISO-27001: Alarm on Malware Rule	586
AIE: ISO-27001: Config Change After Attack	118
Protocol Anomaly	105
Detected Trojan Activity	92
Spoofing Activity	50
AIE: IPSec Guard: Malware: Spamming Bot	6
Total:	37161

Top 10 Common Events By Time



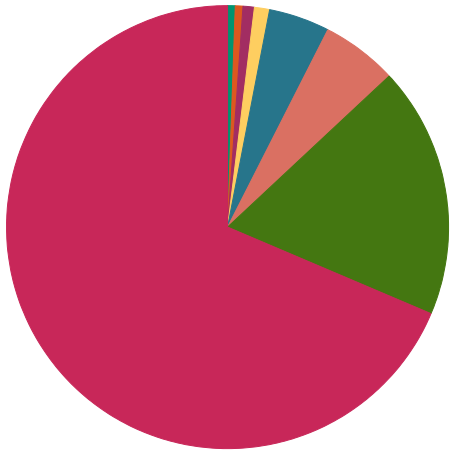
IPSec Guard: Monthly Event Executive Summary

By Entity

Monday, 1 May 2017 12:00 AM to Thursday, 1 June 2017 12:00 AM AUSEST (UTC+10:00)

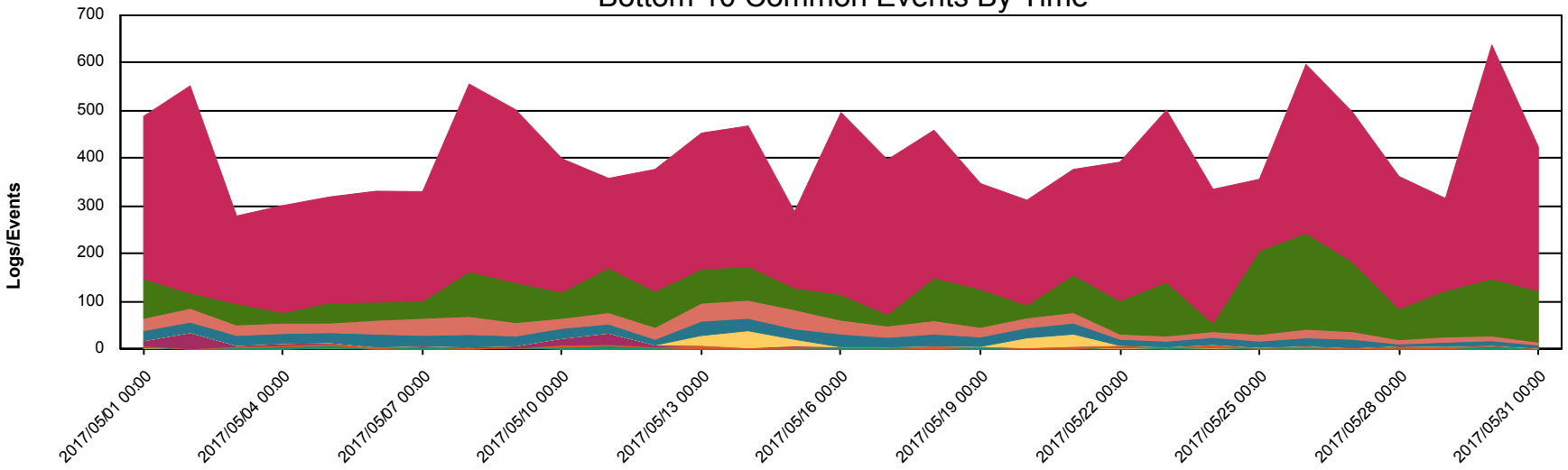
Impacted Entity: All

Bottom 10 Common Events

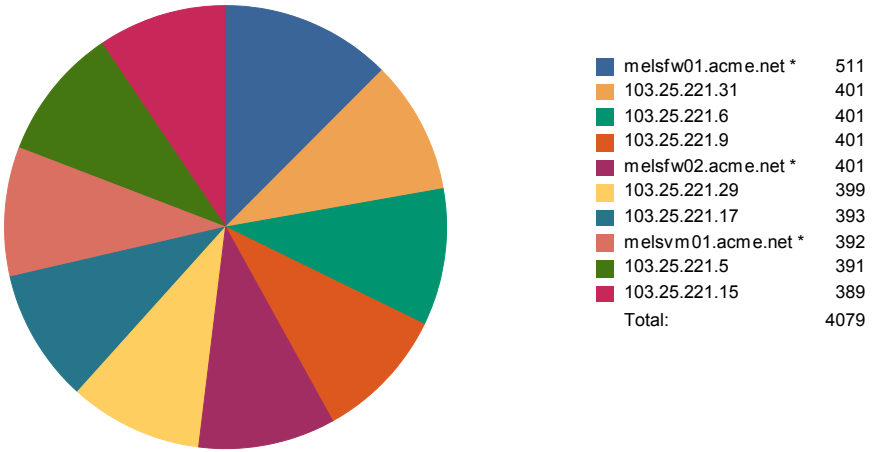


AIE: C2: Abnormal Process Activity	3
AIE: IPSec Guard: Malware: Spamming Bot	6
Spoofing Activity	50
Detected Trojan Activity	92
Protocol Anomaly	105
AIE: ISO-27001: Config Change After Attack	118
AIE: IPSec Guard: ISO-27001: Alarm on Malware Rule	586
Detected Worm Activity	698
Buffer Overflow/Underflow	2360
General Attack Activity	8789
Total:	12807

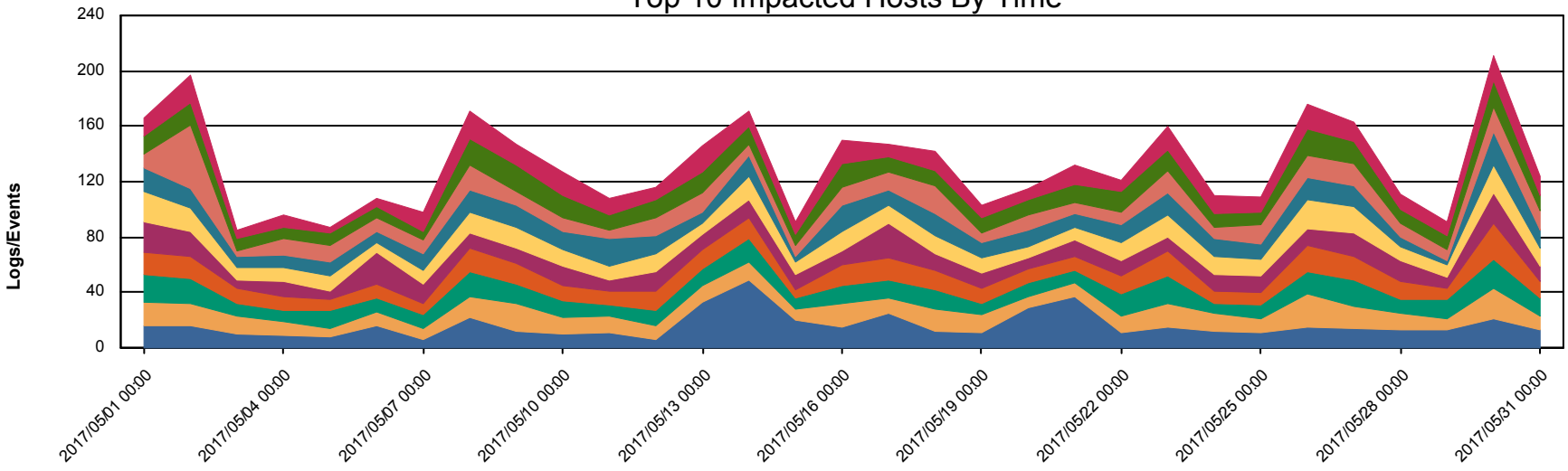
Bottom 10 Common Events By Time



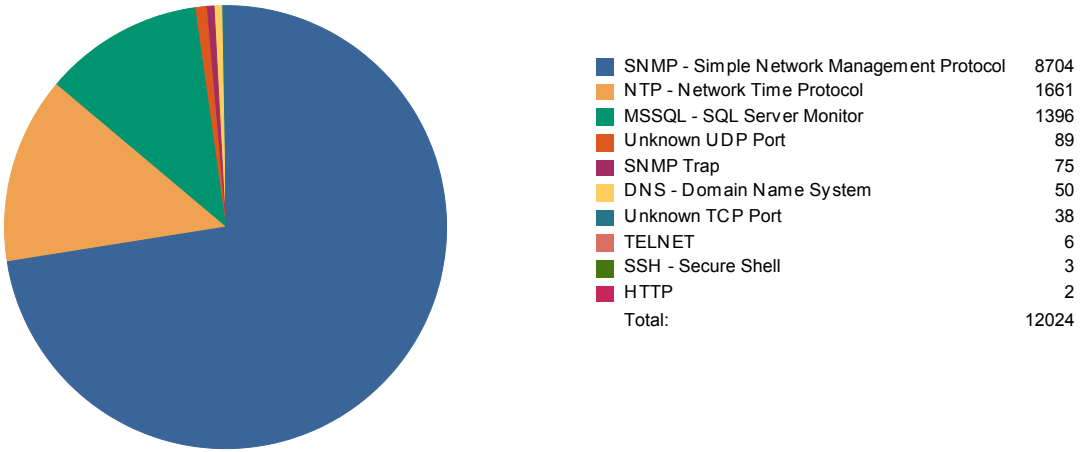
Top 10 Impacted Hosts



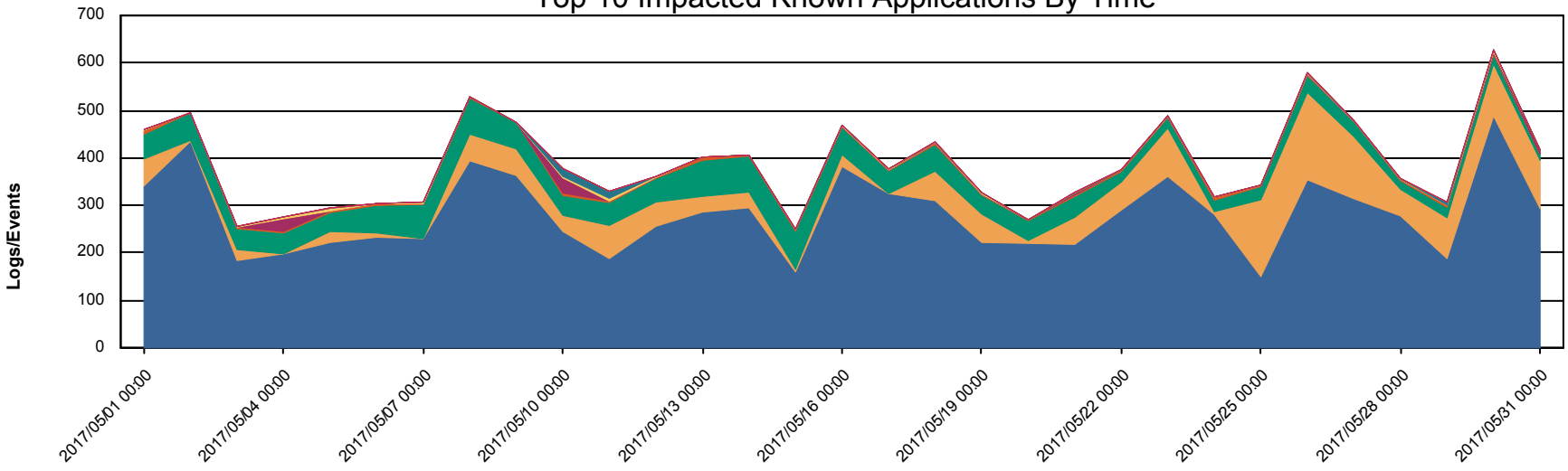
Top 10 Impacted Hosts By Time



Top 10 Impacted Known Applications



Top 10 Impacted Known Applications By Time



ACME Monthly digest report

Monthly digest report with list of events, CPU, Memory, Storage utilization for the previous month

Summary of Orion Objects: **ACME; ACME Alerts Monthly; ACME Active Alerts; ACME Status Monthly**
Summary of Time Periods: **Last 30 Days (May 22 - Jun 21, 2017)**

List of All the Events for the previous month for ACME Alerts Monthly

NAME	MESSAGE	VENDOR	DEVICE	OBJECT TRIGGERED	SEVERITY	TIMESTAMP
IPSec - DeviceNonCritical - Warning - CPU - 90% - 10min	ACME consult-scanner CPU load is 28 %		consult-scanner	consult-scanner		31 May 2017 22:42:34
IPSec - DeviceNonCritical - Warning - CPU - 90% - 10min	ACME consult-scanner CPU load is 9 %		consult-scanner	consult-scanner		31 May 2017 19:23:05
IPSec - DeviceNonCritical - Warning - CPU - 90% - 10min	ACME consult-scanner CPU load is 34 %		consult-scanner	consult-scanner		31 May 2017 16:03:30
IPSec - DeviceNonCritical - Warning - CPU - 90% - 10min	ACME consult-scanner CPU load is 3 %		consult-scanner	consult-scanner		31 May 2017 13:23:02
IPSec - DeviceNonCritical - Warning - CPU - 90% - 10min	ACME consult-scanner CPU load is 3 %		consult-scanner	consult-scanner		31 May 2017 12:32:53
IPSec - DeviceNonCritical - Warning - CPU - 90% - 10min	ACME consult-scanner CPU load is 3 %		consult-scanner	consult-scanner		31 May 2017 11:32:43
IPSec - DeviceNonCritical - Serious - CPU - 90% - 60min	ACME melsfw02.lab.ipsec.net.au CPU load is 2 %		melsfw02.lab.ipsec.net.au	melsfw02.lab.ipsec.net.au		31 May 2017 10:43:10
IPSec - DeviceNonCritical - Warning - CPU - 90% - 10min	ACME consult-scanner CPU load is 18 %		consult-scanner	consult-scanner		31 May 2017 09:52:29
IPSec - DeviceNonCritical - Warning - CPU - 90% - 10min	ACME melsfw02.lab.ipsec.net.au CPU load is 2 %		melsfw02.lab.ipsec.net.au	melsfw02.lab.ipsec.net.au		31 May 2017 09:52:29
IPSec - DeviceNonCritical - Warning - CPU - 90% - 10min	ACME consult-scanner CPU load is 15 %		consult-scanner	consult-scanner		31 May 2017 08:23:13
IPSec - DeviceNonCritical - Warning - CPU - 90% - 10min	ACME consult-scanner CPU load is 34 %		consult-scanner	consult-scanner		31 May 2017 07:33:04
IPSec - DeviceNonCritical - Warning - CPU - 90% - 10min	ACME consult-scanner CPU load is 34 %		consult-scanner	consult-scanner		31 May 2017 04:32:32
IPSec - DeviceNonCritical - Warning - CPU - 90% - 10min	ACME consult-scanner CPU load is 3 %		consult-scanner	consult-scanner		31 May 2017 04:12:28
IPSec - DeviceNonCritical - Warning - CPU - 90% - 10min	ACME consult-scanner CPU load is 3 %		consult-scanner	consult-scanner		31 May 2017 01:53:02
IPSec - DeviceNonCritical - Warning - CPU - 90% - 10min	ACME consult-scanner CPU load is 3 %		consult-scanner	consult-scanner		31 May 2017 00:12:49
IPSec - DeviceNonCritical - Warning - CPU - 90% - 10min	ACME consult-scanner CPU load is 3 %		consult-scanner	consult-scanner		30 May 2017 23:12:38
IPSec - DeviceNonCritical - Serious - CPU - 90% - 60min	ACME melsfw02.lab.ipsec.net.au CPU load is 2 %		melsfw02.lab.ipsec.net.au	melsfw02.lab.ipsec.net.au		30 May 2017 22:13:04
IPSec - DeviceNonCritical - Warning - CPU - 90% - 10min	ACME consult-scanner CPU load is 6 %		consult-scanner	consult-scanner		30 May 2017 21:53:23
IPSec - DeviceNonCritical - Warning - CPU - 90% - 10min	ACME melsfw02.lab.ipsec.net.au CPU load is 2 %		melsfw02.lab.ipsec.net.au	melsfw02.lab.ipsec.net.au		30 May 2017 21:22:18
IPSec - DeviceNonCritical - Warning - CPU - 90% - 10min	ACME consult-scanner CPU load is 3 %		consult-scanner	consult-scanner		30 May 2017 19:53:02

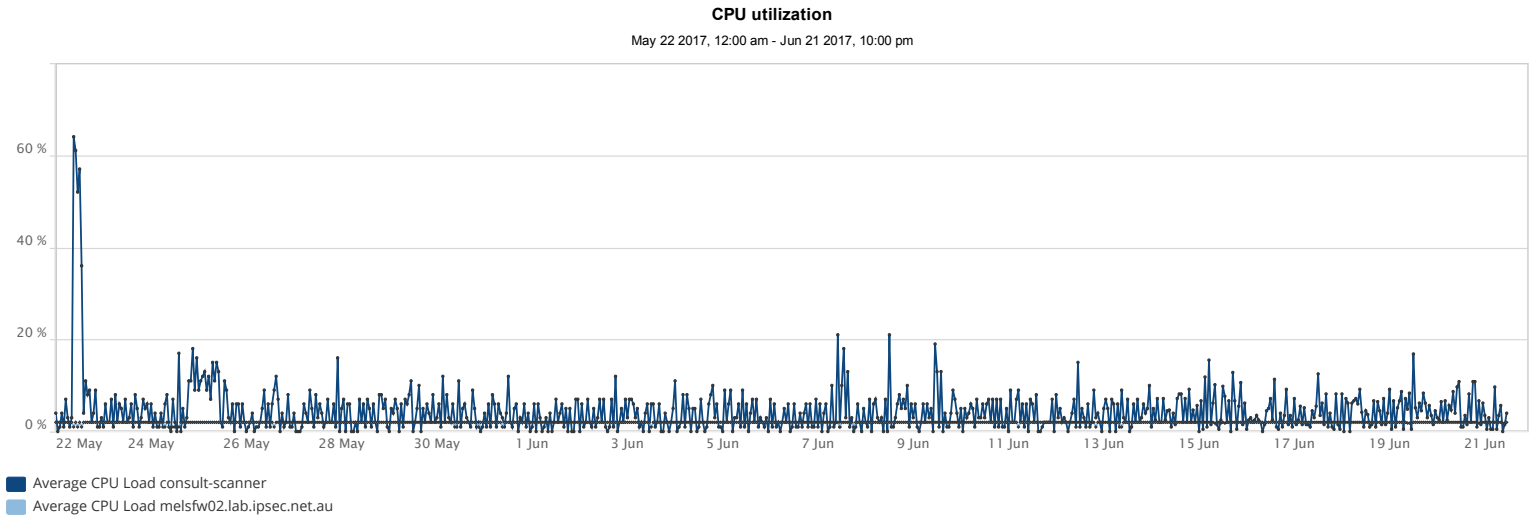
All Active Events for ACME Active Alerts

NAME	MESSAGE	VENDOR	DEVICE	OBJECT TRIGGERRED		ACTIVE SINCE
IPSec - DeviceNonCritical - Serious - Storage	C:\ Label: EA9AC7C2 consult-scanner disk usage is 33 %		consult-scanner	C:\ Label: EA9AC7C2		16 May 2017 21:26:44

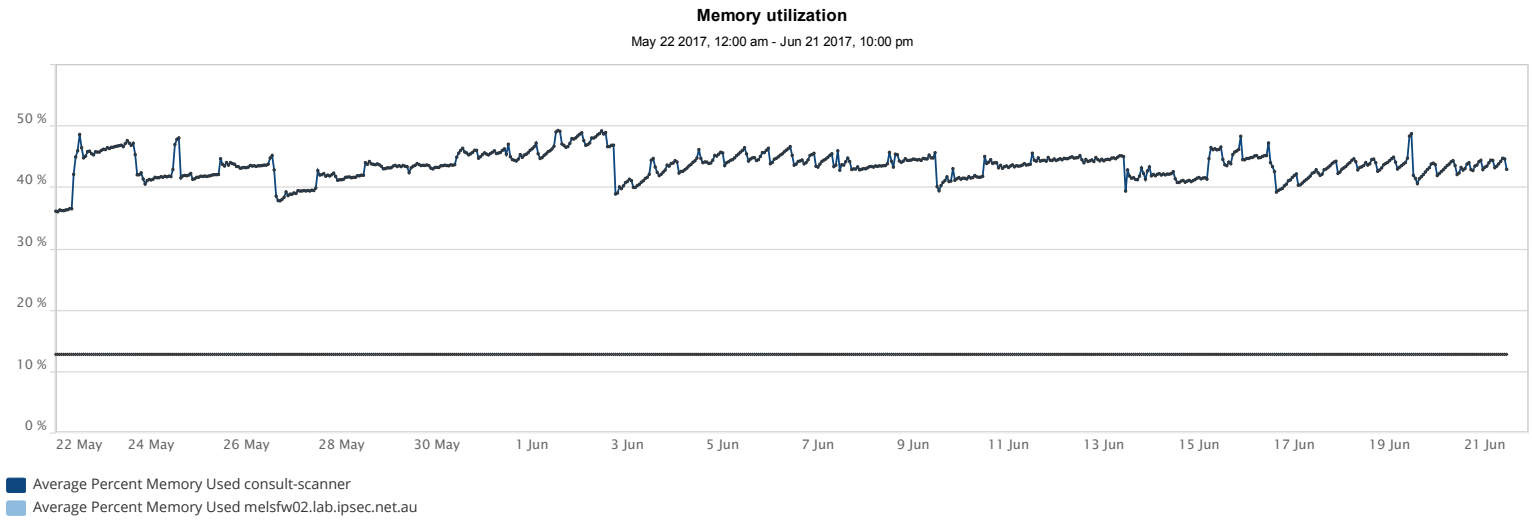
Status Table for ACME Status Monthly

DEVICE	MACHINE TYPE	VENDOR	MSS CLASS	TOTAL HEALTH	CRITICAL TIME	SERIOUS TIME	WARNING TIME
melsfw02.lab.ipsec.net.au	Juniper Networks/NetScreen		Non Critical		0 %	65 %	65 %
opengear.lab.ipsec.net.au	OpenGear CM41xx		Non Critical		0 %	0 %	0 %
mellsw01.lab.ipsec.net.au	HP Switch		Non Critical		0 %	0 %	0 %
consult-scanner	Windows 10 Workstation		Non Critical		0 %	91 %	65 %
melehoney01	Ubuntu		Non Critical		0 %	0 %	0 %

CPU utilization for **ACME** from **Last 30 Days (May 22 - Jun 21, 2017)**



Memory utilization for **ACME** from **Last 30 Days (May 22 - Jun 21, 2017)**



Storage utilization for **ACME** from **Last 30 Days (May 22 - Jun 21, 2017)**
Ordered by: Percent Disk Used - Descending