# Table of Contents

**Table of Contents**

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Table of Contents</td>
<td>2</td>
</tr>
<tr>
<td>Introduction</td>
<td>3</td>
</tr>
<tr>
<td><strong>Service Delivery Report</strong></td>
<td>5</td>
</tr>
<tr>
<td>Raised MSS Incidents</td>
<td>5</td>
</tr>
<tr>
<td>Resolved MSS Incidents</td>
<td>5</td>
</tr>
<tr>
<td>Unresolved MSS Incidents</td>
<td>5</td>
</tr>
<tr>
<td>Raised MSS Changes</td>
<td>5</td>
</tr>
<tr>
<td>Resolved MSS Changes</td>
<td>6</td>
</tr>
<tr>
<td>Unresolved MSS Changes</td>
<td>6</td>
</tr>
<tr>
<td>Daily Systems Review</td>
<td>6</td>
</tr>
<tr>
<td><strong>Guard Service Report</strong></td>
<td>7</td>
</tr>
<tr>
<td>IPSec Guard Report</td>
<td>7</td>
</tr>
<tr>
<td><strong>IPSec Guard Service Delivery Report</strong></td>
<td>8</td>
</tr>
<tr>
<td>IPSec Guard Incidents Raised</td>
<td>8</td>
</tr>
<tr>
<td>IPSec Guard Incidents Closed</td>
<td>8</td>
</tr>
<tr>
<td>IPSec Guard Incidents Unresolved</td>
<td>8</td>
</tr>
<tr>
<td>IPSec Guard Changes Raised</td>
<td>9</td>
</tr>
<tr>
<td>IPSec Guard Changes Resolved</td>
<td>9</td>
</tr>
<tr>
<td>IPSec Guard Changes Unresolved</td>
<td>9</td>
</tr>
<tr>
<td><strong>Appendices</strong></td>
<td>10</td>
</tr>
<tr>
<td>IPSec Guard: Executive Summary</td>
<td>10</td>
</tr>
<tr>
<td>IPSec Guard: Log Volume: by Log Source</td>
<td>13</td>
</tr>
<tr>
<td>IPSec Guard: Monthly Event Executive Summary</td>
<td>16</td>
</tr>
<tr>
<td>IPSec Monitor: Performance Statistics</td>
<td>24</td>
</tr>
</tbody>
</table>
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 systems 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).

<table>
<thead>
<tr>
<th>id</th>
<th>Subject</th>
<th>Client</th>
<th>Priority</th>
<th>Status</th>
<th>Date Reported</th>
<th>Date Closed</th>
</tr>
</thead>
<tbody>
<tr>
<td>102466</td>
<td>Please investigate delay in request processing</td>
<td>Fred Nerf</td>
<td>Medium</td>
<td>Open</td>
<td>22/05/2017</td>
<td>11:17:00 AM</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>id</th>
<th>Subject</th>
<th>Client</th>
<th>Priority</th>
<th>Status</th>
<th>Date Reported</th>
<th>Date Closed</th>
</tr>
</thead>
<tbody>
<tr>
<td>102466</td>
<td>Please investigate delay in request processing</td>
<td>Fred Nerf</td>
<td>Medium</td>
<td>Open</td>
<td>22/05/2017</td>
<td>11:17:00 AM</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>id</th>
<th>Subject</th>
<th>Client</th>
<th>Priority</th>
<th>Status</th>
<th>Date Reported</th>
<th>Date Closed</th>
</tr>
</thead>
<tbody>
<tr>
<td>102467</td>
<td>Please create a new monthly report</td>
<td>Fred Nerf</td>
<td>Medium</td>
<td>Open</td>
<td>22/05/2017</td>
<td>11:19:00 AM</td>
</tr>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th>id</th>
<th>Subject</th>
<th>Client</th>
<th>Priority</th>
<th>Status</th>
<th>Date Reported</th>
<th>Date Closed</th>
</tr>
</thead>
<tbody>
<tr>
<td>102467</td>
<td><strong>Please create a new monthly report</strong></td>
<td>Fred Nerf</td>
<td>Medium</td>
<td>Open</td>
<td>22/05/2017</td>
<td>11:19:00 AM</td>
</tr>
</tbody>
</table>

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.

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

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.

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

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

<table>
<thead>
<tr>
<th>id</th>
<th>Subject</th>
<th>Client</th>
<th>Status</th>
<th>Date Reported</th>
<th>Date Closed</th>
</tr>
</thead>
<tbody>
<tr>
<td>102465</td>
<td>Fred Nerf</td>
<td></td>
<td>Pending Approval</td>
<td>22/05/2017 11:14:00 AM</td>
<td></td>
</tr>
</tbody>
</table>

**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 ACME at the end of the reporting period.

<table>
<thead>
<tr>
<th>id</th>
<th>Subject</th>
<th>Client</th>
<th>Status</th>
<th>Date Reported</th>
<th>Date Closed</th>
</tr>
</thead>
<tbody>
<tr>
<td>102465</td>
<td>Fred Nerf</td>
<td></td>
<td>Pending Approval</td>
<td>22/05/2017 11:14:00 AM</td>
<td></td>
</tr>
</tbody>
</table>
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

Logs vs. Events

For ACME Inc

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

Logs & Events per Day

For ACME Inc

- Logs Collected
- Identified Logs
- Events Forwarded
- Online Logs
- Archived Logs

Report prepared as part of IPSec Guard: ACME: Monthly Digest for IPSec Pty Ltd on 20/06/2017 4:37 PM AUSEST
Copyright © 2017 LogRhythm, Inc. All Rights Reserved.
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

<table>
<thead>
<tr>
<th>Log Host</th>
<th>Log Source Name</th>
<th>Total Logs</th>
<th>Logs/d</th>
<th>Logs/s</th>
<th>% Evt</th>
<th>% Id</th>
<th>% Arc</th>
<th>% On</th>
</tr>
</thead>
<tbody>
<tr>
<td>melehoney01</td>
<td>Syslog - Snort IDS</td>
<td>4,837,049</td>
<td>156,034</td>
<td>1.810</td>
<td>100.00</td>
<td>100.00</td>
<td>100.00</td>
<td>100.00</td>
</tr>
<tr>
<td>melehoney01</td>
<td>LogRhythm Process Monitor (Linux)</td>
<td>12,933</td>
<td>417</td>
<td>0.000</td>
<td>99.97</td>
<td>100.00</td>
<td>100.00</td>
<td>100.00</td>
</tr>
<tr>
<td>melehoney01</td>
<td>LogRhythm Network Connection Monitor (Linux)</td>
<td>3,390</td>
<td>109</td>
<td>0.000</td>
<td>0.00</td>
<td>100.00</td>
<td>100.00</td>
<td>100.00</td>
</tr>
<tr>
<td>melehoney01</td>
<td>LogRhythm File Monitor (Linux)</td>
<td>735</td>
<td>24</td>
<td>0.000</td>
<td>100.00</td>
<td>100.00</td>
<td>100.00</td>
<td>100.00</td>
</tr>
<tr>
<td>melehoney01</td>
<td>LogRhythm User Activity Monitor (Linux)</td>
<td>156</td>
<td>5</td>
<td>0.000</td>
<td>100.00</td>
<td>100.00</td>
<td>100.00</td>
<td>100.00</td>
</tr>
</tbody>
</table>

### Top 7 Log Sources For ACME Inc

- **melehoney01: Syslog - Snort IDS**: 4,837,049 logs, 156,034 logs/day (1.810 logs/s), 100% event detection, 100% identification, 100% correlation, 100% on-time
- **melehoney01: LogRhythm Process Monitor (Linux)**: 12,933 logs, 417 logs/day (0.000 logs/s), 0% event detection, 100% identification, 100% correlation, 100% on-time
- **melehoney01: LogRhythm Network Connection Monitor (Linux)**: 3,390 logs, 109 logs/day (0.000 logs/s), 0% event detection, 100% identification, 100% correlation, 100% on-time
- **melehoney01: LogRhythm File Monitor (Linux)**: 735 logs, 24 logs/day (0.000 logs/s), 100% event detection, 100% identification, 100% correlation, 100% on-time
- **melehoney01: LogRhythm User Activity Monitor (Linux)**: 156 logs, 5 logs/day (0.000 logs/s), 100% event detection, 100% identification, 100% correlation, 100% on-time

Report prepared as part of IPSec Guard: ACME: Monthly Digest for IPSec Pty Ltd on 20/06/2017 4:37 PM AUSEST

Copyright © 2017 LogRhythm, Inc. All Rights Reserved.
## 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

<table>
<thead>
<tr>
<th>Log Host</th>
<th>Log Source Name</th>
<th>Total Logs</th>
<th>Logs/d</th>
<th>Logs/s</th>
<th>% Evt</th>
<th>% Id</th>
<th>% Arc</th>
<th>% On</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total:</td>
<td>Syslog - Snort IDS</td>
<td>4,837,049</td>
<td>156,034</td>
<td>1.810</td>
<td>0.69</td>
<td>100.00</td>
<td>100.00</td>
<td>100.00</td>
</tr>
<tr>
<td>Entity Total</td>
<td></td>
<td>4,854,263</td>
<td>156,589</td>
<td>1.810</td>
<td>0.70</td>
<td>100.00</td>
<td>100.00</td>
<td>100.00</td>
</tr>
<tr>
<td>Grand Total</td>
<td></td>
<td>4,854,263</td>
<td>156,589</td>
<td>1.810</td>
<td>0.70</td>
<td>100.00</td>
<td>100.00</td>
<td>100.00</td>
</tr>
</tbody>
</table>
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)
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 Classification By Time

- Malware
- Compromise
- Attack

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

Copyright © 2017 LogRhythm, Inc. All Rights Reserved.
Top 10 Impacted Entities

- ACME Inc: 37112
- Global Entity: 52
- Total: 37164

Top 10 Impacted Entities By Time

- 2017/05/01 00:00
- 2017/05/04 00:00
- 2017/05/07 00:00
- 2017/05/10 00:00
- 2017/05/13 00:00
- 2017/05/16 00:00
- 2017/05/19 00:00
- 2017/05/22 00:00
- 2017/05/25 00:00
- 2017/05/28 00:00
- 2017/05/31 00:00
IPSec Guard: Monthly Event Executive Summary
By Entity
Monday, 1 May 2017 12:00 AM to Thursday, 1 June 2017 12:00 AM AU EST (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

Log/Events

- 0
- 400
- 800
- 1200
- 1600
- 2000
- 2400
- 2800

2017/05/01 00:00 to 2017/05/31 00:00

Report prepared as part of IPSec Guard: ACME: Monthly Digest for IPSec Pty Ltd on 20/06/2017 4:37 PM AU EST (UTC+10:00)
Copyright © 2017 LogRhythm, Inc. All Rights Reserved.
IPSec Guard: Monthly Event Executive Summary

By Entity

Monday, 1 May 2017 12:00 AM to Thursday, 1 June 2017 12:00 AM AU EST (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
IPSec Guard: Monthly Event Executive Summary
By Entity
Monday, 1 May 2017 12:00 AM to Thursday, 1 June 2017 12:00 AM AUEST (UTC+10:00)
Impacted Entity: All

Top 10 Impacted Hosts

- melsfw01.acme.net * 511
- 103.25.221.31 401
- 103.25.221.6 401
- 103.25.221.9 401
- melsfw02.acme.net * 401
- 103.25.221.29 399
- 103.25.221.17 393
- melsvm01.acme.net * 392
- 103.25.221.5 391
- 103.25.221.15 389
Total: 4079

Top 10 Impacted Hosts By Time

Report prepared as part of IPSec Guard: ACME: Monthly Digest for IPSecPtyLtd on 20/06/2017 4:37 PM AUEST (UTC+10:00)
Copyright © 2017 LogRhythm, Inc. All Rights Reserved.
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 Known Applications

- SNMP - Simple Network Management Protocol: 8704
- NTP - Network Time Protocol: 1661
- MSSQL - SQL Server Monitor: 1396
- Unknown UDP Port: 89
- SNMP Trap: 75
- DNS - Domain Name System: 50
- Unknown TCP Port: 38
- TELNET: 6
- SSH - Secure Shell: 3
- HTTP: 2
- Total: 12024

Report prepared as part of IPSec Guard: ACME: Monthly Digest for IPSec Pty Ltd on 20/06/2017 4:37 PM AUSEST (UTC+10:00)
Copyright © 2017 LogRhythm, Inc. All Rights Reserved.
### 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

<table>
<thead>
<tr>
<th>NAME</th>
<th>MESSAGE</th>
<th>VENDOR</th>
<th>DEVICE</th>
<th>OBJECT TRIGGERED</th>
<th>SEVERITY</th>
<th>TIMESTAMP</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPSec - DeviceNonCritical - Warning - CPU - 99% - 10min</td>
<td>ACME consult-scanner CPU load is 28 %</td>
<td>consult-scanner</td>
<td>consult-scanner</td>
<td>▲</td>
<td>31 May 2017 22:42:34</td>
<td></td>
</tr>
<tr>
<td>IPSec - DeviceNonCritical - Warning - CPU - 99% - 10min</td>
<td>ACME consult-scanner CPU load is 9 %</td>
<td>consult-scanner</td>
<td>consult-scanner</td>
<td>▲</td>
<td>31 May 2017 19:23:05</td>
<td></td>
</tr>
<tr>
<td>IPSec - DeviceNonCritical - Warning - CPU - 99% - 10min</td>
<td>ACME consult-scanner CPU load is 34 %</td>
<td>consult-scanner</td>
<td>consult-scanner</td>
<td>▲</td>
<td>31 May 2017 16:03:30</td>
<td></td>
</tr>
<tr>
<td>IPSec - DeviceNonCritical - Warning - CPU - 99% - 10min</td>
<td>ACME consult-scanner CPU load is 3 %</td>
<td>consult-scanner</td>
<td>consult-scanner</td>
<td>▲</td>
<td>31 May 2017 13:23:02</td>
<td></td>
</tr>
<tr>
<td>IPSec - DeviceNonCritical - Warning - CPU - 99% - 10min</td>
<td>ACME consult-scanner CPU load is 3 %</td>
<td>consult-scanner</td>
<td>consult-scanner</td>
<td>▲</td>
<td>31 May 2017 12:32:53</td>
<td></td>
</tr>
<tr>
<td>IPSec - DeviceNonCritical - Warning - CPU - 99% - 10min</td>
<td>ACME consult-scanner CPU load is 3 %</td>
<td>consult-scanner</td>
<td>consult-scanner</td>
<td>▲</td>
<td>31 May 2017 11:52:43</td>
<td></td>
</tr>
<tr>
<td>IPSec - DeviceNonCritical - Serious - CPU - 99% - 60min</td>
<td>ACME melsfw02.lab.ipsec.net.au CPU load is 2 %</td>
<td>melsfw02.lab.ipsec.net.au</td>
<td>melsfw02.lab.ipsec.net.au</td>
<td>▲</td>
<td>31 May 2017 10:43:10</td>
<td></td>
</tr>
<tr>
<td>IPSec - DeviceNonCritical - Warning - CPU - 99% - 10min</td>
<td>ACME consult-scanner CPU load is 18 %</td>
<td>consult-scanner</td>
<td>consult-scanner</td>
<td>▲</td>
<td>31 May 2017 09:52:29</td>
<td></td>
</tr>
<tr>
<td>IPSec - DeviceNonCritical - Warning - CPU - 99% - 10min</td>
<td>ACME melsfw02.lab.ipsec.net.au CPU load is 2 %</td>
<td>melsfw02.lab.ipsec.net.au</td>
<td>melsfw02.lab.ipsec.net.au</td>
<td>▲</td>
<td>31 May 2017 09:52:29</td>
<td></td>
</tr>
<tr>
<td>IPSec - DeviceNonCritical - Warning - CPU - 99% - 10min</td>
<td>ACME consult-scanner CPU load is 15 %</td>
<td>consult-scanner</td>
<td>consult-scanner</td>
<td>▲</td>
<td>31 May 2017 08:23:13</td>
<td></td>
</tr>
<tr>
<td>IPSec - DeviceNonCritical - Warning - CPU - 99% - 10min</td>
<td>ACME consult-scanner CPU load is 34 %</td>
<td>consult-scanner</td>
<td>consult-scanner</td>
<td>▲</td>
<td>31 May 2017 07:33:04</td>
<td></td>
</tr>
<tr>
<td>IPSec - DeviceNonCritical - Warning - CPU - 99% - 10min</td>
<td>ACME consult-scanner CPU load is 3 %</td>
<td>consult-scanner</td>
<td>consult-scanner</td>
<td>▲</td>
<td>31 May 2017 04:32:32</td>
<td></td>
</tr>
<tr>
<td>IPSec - DeviceNonCritical - Warning - CPU - 99% - 10min</td>
<td>ACME consult-scanner CPU load is 3 %</td>
<td>consult-scanner</td>
<td>consult-scanner</td>
<td>▲</td>
<td>31 May 2017 04:12:28</td>
<td></td>
</tr>
<tr>
<td>IPSec - DeviceNonCritical - Warning - CPU - 99% - 10min</td>
<td>ACME consult-scanner CPU load is 3 %</td>
<td>consult-scanner</td>
<td>consult-scanner</td>
<td>▲</td>
<td>31 May 2017 01:53:02</td>
<td></td>
</tr>
<tr>
<td>IPSec - DeviceNonCritical - Warning - CPU - 99% - 10min</td>
<td>ACME consult-scanner CPU load is 3 %</td>
<td>consult-scanner</td>
<td>consult-scanner</td>
<td>▲</td>
<td>31 May 2017 00:12:49</td>
<td></td>
</tr>
<tr>
<td>IPSec - DeviceNonCritical - Warning - CPU - 99% - 10min</td>
<td>ACME consult-scanner CPU load is 3 %</td>
<td>consult-scanner</td>
<td>consult-scanner</td>
<td>▲</td>
<td>30 May 2017 23:12:38</td>
<td></td>
</tr>
<tr>
<td>IPSec - DeviceNonCritical - Serious - CPU - 99% - 60min</td>
<td>ACME melsfw02.lab.ipsec.net.au CPU load is 2 %</td>
<td>melsfw02.lab.ipsec.net.au</td>
<td>melsfw02.lab.ipsec.net.au</td>
<td>▲</td>
<td>30 May 2017 22:13:04</td>
<td></td>
</tr>
<tr>
<td>IPSec - DeviceNonCritical - Warning - CPU - 99% - 10min</td>
<td>ACME consult-scanner CPU load is 6 %</td>
<td>consult-scanner</td>
<td>consult-scanner</td>
<td>▲</td>
<td>30 May 2017 21:53:23</td>
<td></td>
</tr>
<tr>
<td>IPSec - DeviceNonCritical - Warning - CPU - 99% - 10min</td>
<td>ACME melsfw02.lab.ipsec.net.au CPU load is 2 %</td>
<td>melsfw02.lab.ipsec.net.au</td>
<td>melsfw02.lab.ipsec.net.au</td>
<td>▲</td>
<td>30 May 2017 21:22:18</td>
<td></td>
</tr>
<tr>
<td>IPSec - DeviceNonCritical - Warning - CPU - 99% - 10min</td>
<td>ACME consult-scanner CPU load is 3 %</td>
<td>consult-scanner</td>
<td>consult-scanner</td>
<td>▲</td>
<td>30 May 2017 19:53:02</td>
<td></td>
</tr>
</tbody>
</table>

### List of All the Events for ACME Alerts Monthly

<table>
<thead>
<tr>
<th>NAME</th>
<th>MESSAGE</th>
<th>VENDOR</th>
<th>DEVICE</th>
<th>OBJECT TRIGGERED</th>
<th>ACTIVE SPACE</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPSec - DeviceNonCritical - Serious - Storage</td>
<td>C:\Label: EA9AC7C2 consult-scanner disk usage is 33 %</td>
<td>consult-scanner</td>
<td>C:\Label: EA9AC7C2</td>
<td>▲</td>
<td>16 May 2017 21:26:44</td>
</tr>
</tbody>
</table>

### Status Table for ACME Status Monthly

<table>
<thead>
<tr>
<th>DEVICE</th>
<th>MACHINE TYPE</th>
<th>VENDOR</th>
<th>MSS CLASS</th>
<th>TOTAL HEALTH</th>
<th>CRITICAL TIME</th>
<th>SERIOUS TIME</th>
<th>WARNING TIME</th>
</tr>
</thead>
<tbody>
<tr>
<td>melsfw02.lab.ipsec.net.au</td>
<td>Juniper Networks/NetScreen</td>
<td></td>
<td>Non Critical</td>
<td>0 %</td>
<td>65 %</td>
<td>65 %</td>
<td></td>
</tr>
<tr>
<td>opengear.lab.ipsec.net.au</td>
<td>OpenGear CM41xx</td>
<td></td>
<td>Non Critical</td>
<td>0 %</td>
<td>0 %</td>
<td>0 %</td>
<td></td>
</tr>
<tr>
<td>melsfw01.lab.ipsec.net.au</td>
<td>HP Switch</td>
<td></td>
<td>Non Critical</td>
<td>0 %</td>
<td>0 %</td>
<td>0 %</td>
<td></td>
</tr>
<tr>
<td>consult-scanner</td>
<td>Windows 10 Workstation</td>
<td></td>
<td>Non Critical</td>
<td>0 %</td>
<td>91 %</td>
<td>65 %</td>
<td></td>
</tr>
<tr>
<td>melehoney01</td>
<td>Ubuntu</td>
<td></td>
<td>Non Critical</td>
<td>0 %</td>
<td>0 %</td>
<td>0 %</td>
<td></td>
</tr>
</tbody>
</table>