Executive Report From 12-16-2016 to 01-15-2018

Security Incident Response Program

Report Date: 01-15-2018

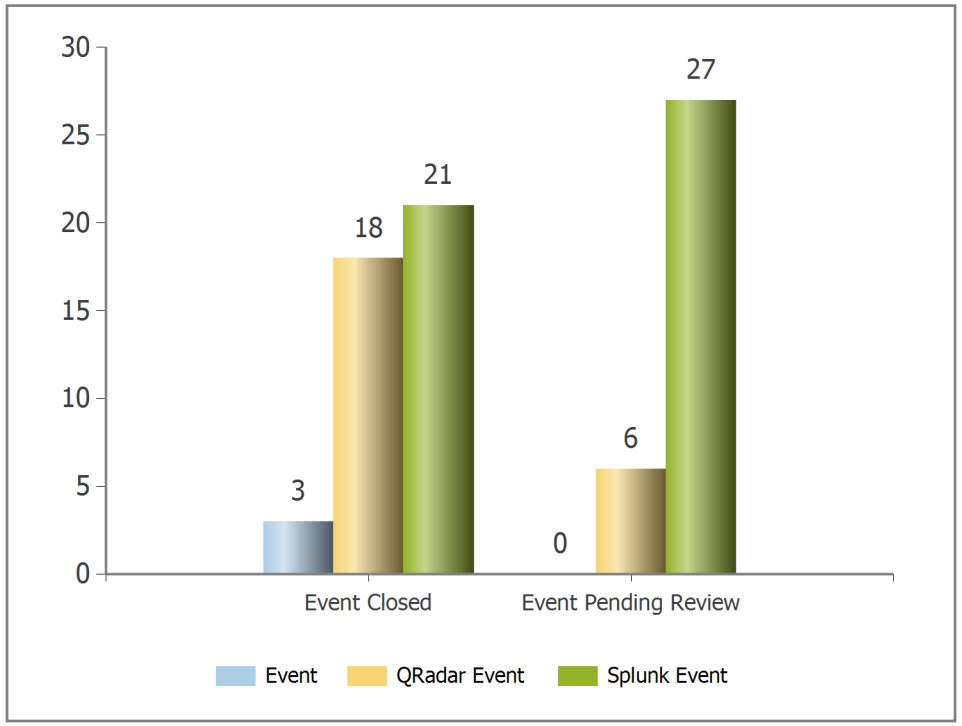
Overview

The following report summarizes security event and security incident activity over the reporting period.

Security Events

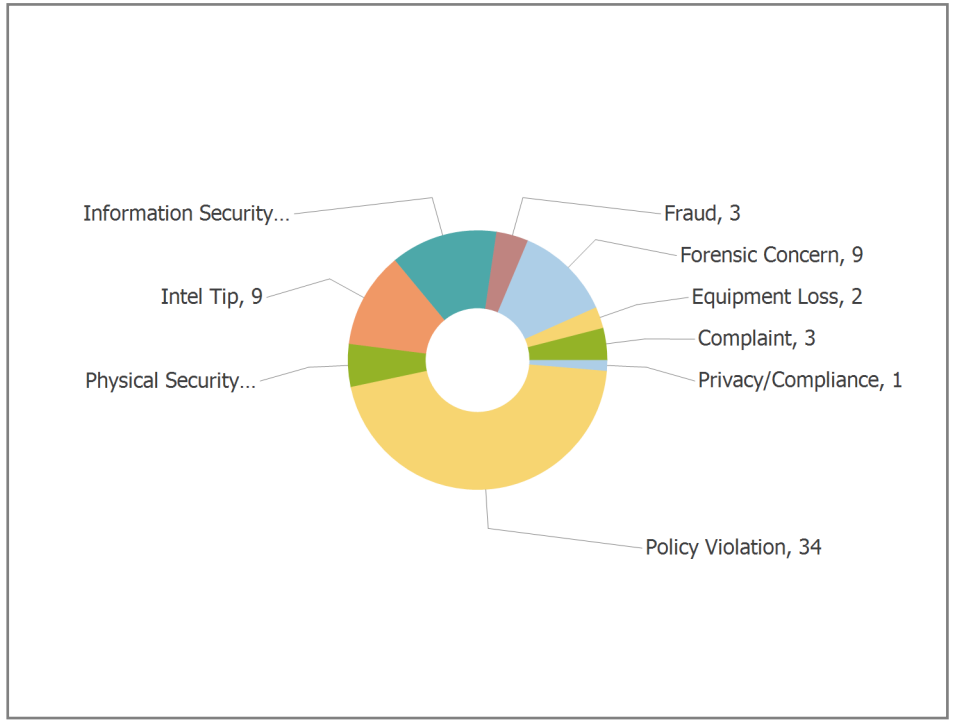
For the purposes of this report, "Security Events" are events being forwarded to the Rsam SIRP solution for manual and/or automated analysis. These Security Events may be closed or escalated to an Incident. Event Rules are run against these events to determine if an automated action can be performed. The following views show event data over the reporting period.

Event by Workflow State



This chart shows the status of event workflow queues.

Events by Category

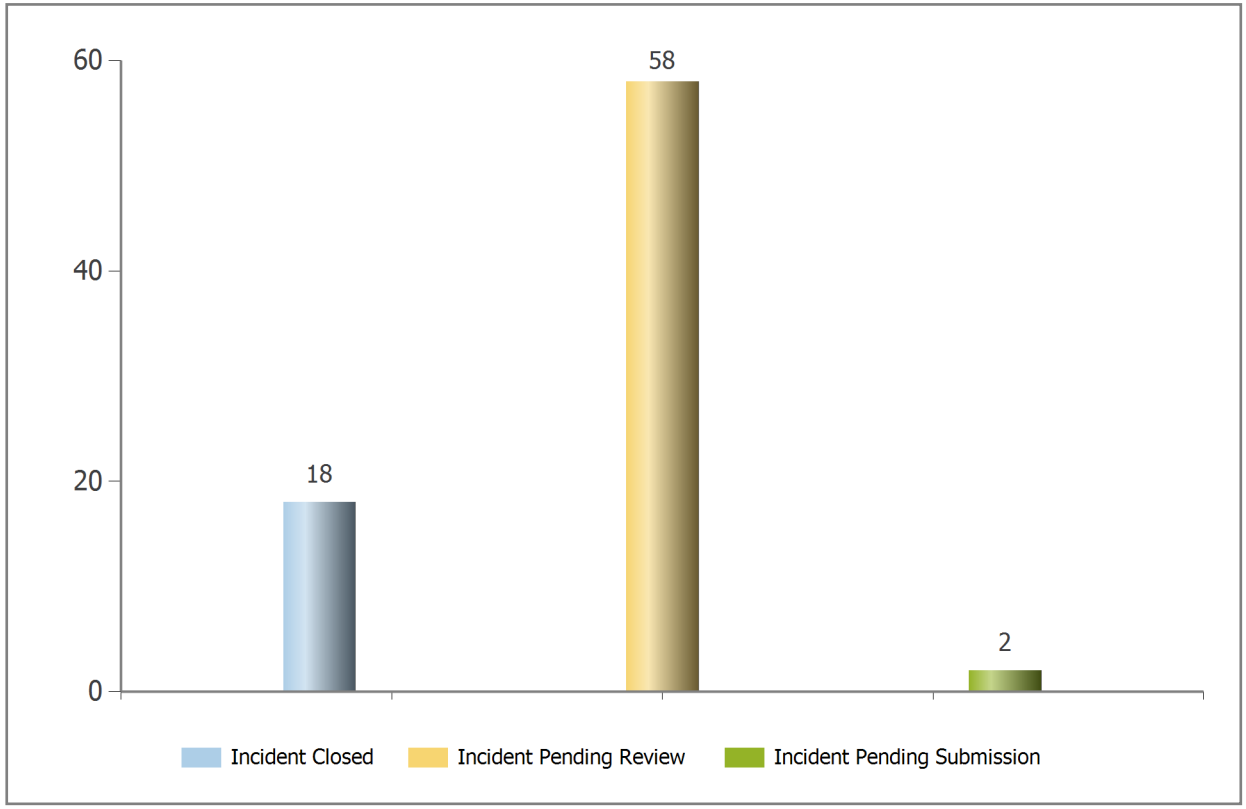


This chart shows events forwarded over the reporting period (by category).

Security Incidents

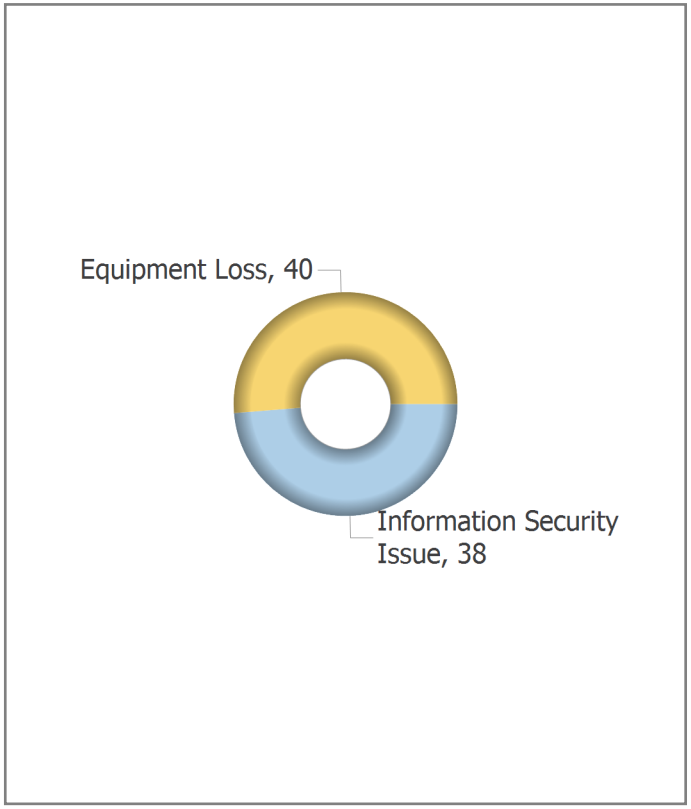
"Security Incidents" are events that have been escalated or are being directly reported by end users. End users may include security/technology users or the larger enterprise user population. While these incidents may not indicate something as serious as a breach, they do require analysis by the Incident Management team. The Incident Management team has defined a series of Playbook Rules that automatically create common incident handling tasks. These tasks may include instructions for contacting other teams, SLA guidance, API calls to other systems, etc.

Incidents by Workflow State



This chart shows the status of incident workflow queues.

Incident by Category

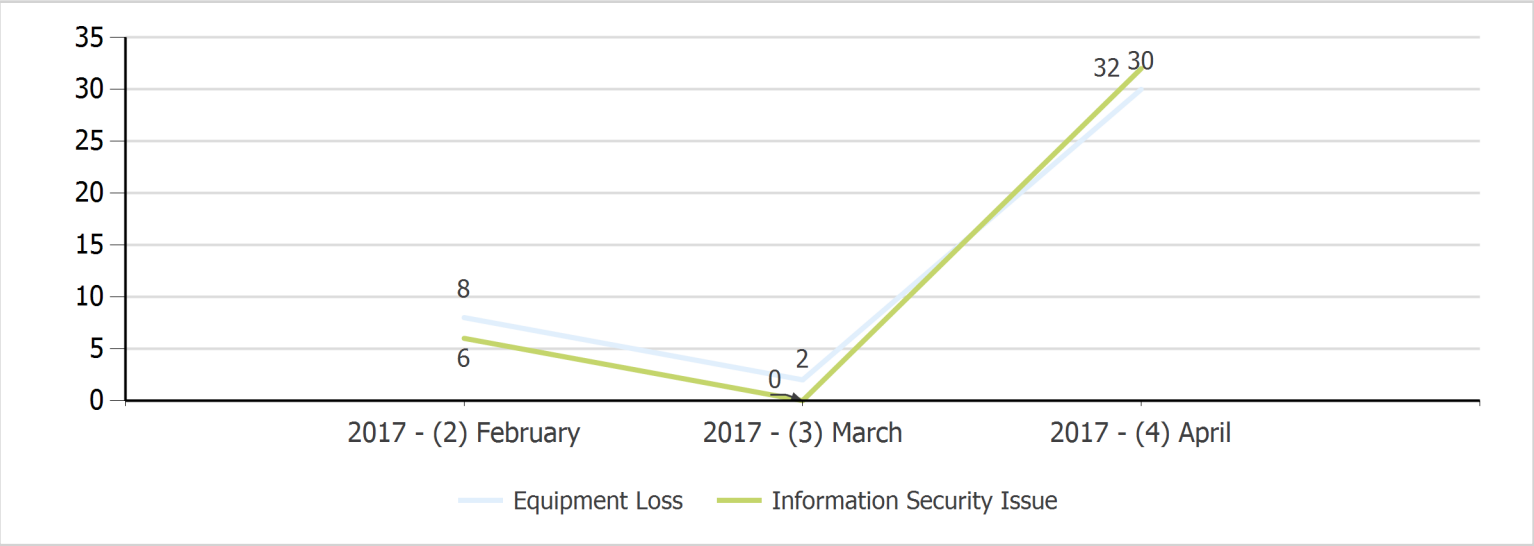


This chart shows incidents reported over the reporting period (by category).

Incident Trends

Viewing incident data over time can give insight into what kind of issues the business is facing and may help to prioritize mitigation for the most critical issues. The following view shows Incidents by Category over the selected period of time:

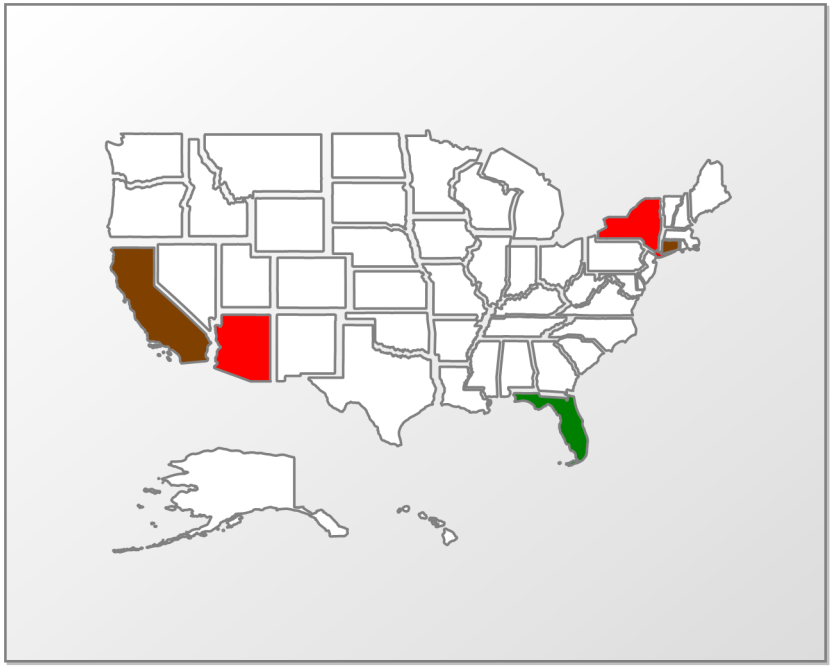
Incidents By Month



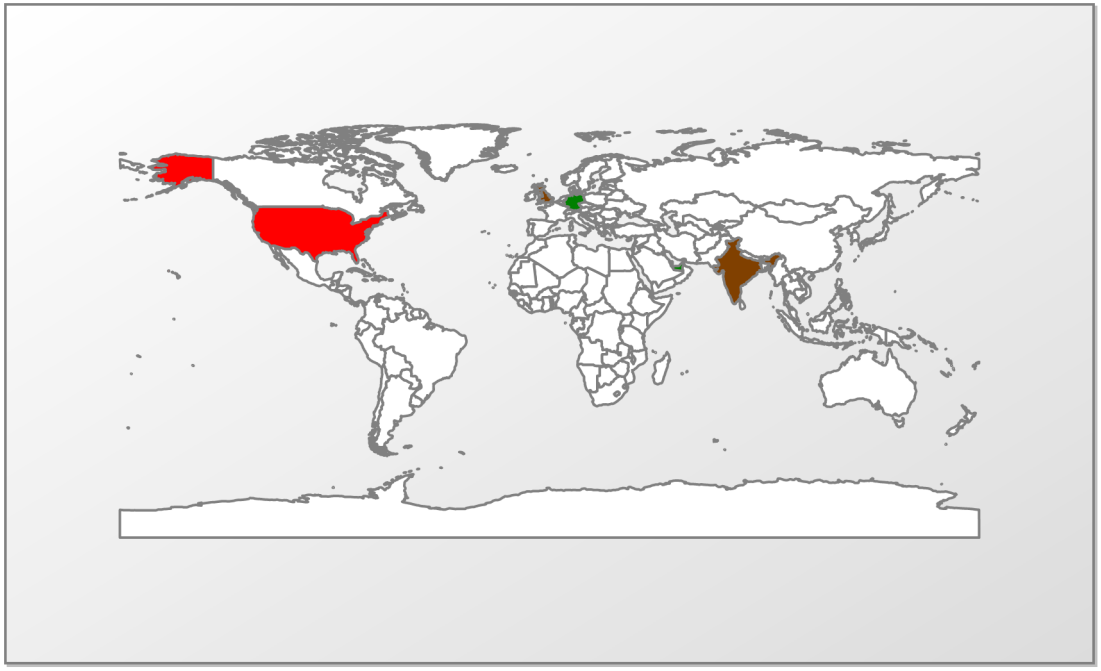
Incidents by Geography

It is also often helpful to view incidents by geographic location. Location data is typically provided by a user reporting an issue or can even be provided by a device with location determined by IP. The following views show Incidents reported in the reporting period grouped by state and country.

Incident Locations By State



Incident Locations By Country



Source IPs

Source IP addresses can also be used to identify specific attacks or threat actors. These IPs should be researched and possibly blocked by firewall or other control. If the IP addresses on the below lists are from an enterprise owned IP range, they may indicate a compromised host.

Top 5 Hosts by Event Count
192.208.49.168 (58)
192.9.200.36 (14)
192.9.200.34 (11)
192.9.200.35 (11)
192.192.32.150 (10)

Top 5 Hosts by Incident Count
172.18.47.21 (32)
172.18.47.22 (13)
1.1.37.72 (4)