Threat Intelligence in Splunk

Do you really know my adversaries? Prove it.

Tim Plona  |  Business Solution Architect
Kyle Maxwell  |  Security Principal
Brandt Varni  |  Security Consulting Senior Analyst

September 27th, 2017  |  Washington, DC
Forward-Looking Statements

During the course of this presentation, we may make forward-looking statements regarding future events or the expected performance of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results could differ materially. For important factors that may cause actual results to differ from those contained in our forward-looking statements, please review our filings with the SEC.

The forward-looking statements made in this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward looking statements we may make. In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionality described or to include any such feature or functionality in a future release.

Splunk, Splunk>, Listen to Your Data, The Engine for Machine Data, Splunk Cloud, Splunk Light and SPL are trademarks and registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names, or trademarks belong to their respective owners. © 2017 Splunk Inc. All rights reserved.
What Will Be Learned In This Presentation

- How credible and reliable threat intelligence can enhance the capabilities of your Security Operations Center
- What is Accenture iDefense
- How to integrate iDefense Threat Intelligence into Splunk Enterprise Security
Introduction

Threat Intelligence in Action

iDefense: CTI Provider

Integrating iDefense Threat Intelligence in Splunk

The Value Realized
Personal Introduction

- Tim Plona, Freeport-McMoRan
  Business Solution Architect

- Kyle Maxwell, Accenture
  Security Principal

- Brandt Varni, Accenture
  Security Consulting Senior Analyst
Freeport-McMoRan is the world’s largest publicly traded copper producer, the world’s largest producer of molybdenum, and a significant gold producer. The global workforce includes over 50,000 employees and contractors worldwide. Partnered with Accenture Managed Security Services, Freeport-McMoRan has developed a Security Operations Center on Splunk to respond to their diverse and changing threat landscape.
Threat Intelligence in Action
Critical Severity Notable Event for iDefense Threat Activity Detected

Matched a known malware command and control URL

Identified that the traffic was not blocked by the security tools

iDefense associated the command and control address with a known Russian cyber espionage group

Allowed the SOC to identify an infection that would otherwise have been unknown
iDefense: CTI Provider
iDefense: CTI Provider
Pyramid of Pain
A model for tactical intelligence

- Tough!
- Challenging
- Annoying
- Simple
- Easy
- Trivial
IntelGraph Ontology

Graph Data Model
iDefense REST Customer API

REST Customer API Documentation

**document : Document API**

**fundamental : Fundamental API**

**threatindicator : ThreatIndicator API**

**vulnerability : Vulnerability API**

[ BASE URL: /rest , API VERSION: 0 ]
Integrating iDefense Threat Intelligence in Splunk
Technical Solution Overview

- Used the Splunk Add-on Builder to create the technology add-on
- Indexed the Threat indicator API and the mining and energy extraction threat intelligence from the Fundamental API for iDefense
- Scheduled searches to correlated common indicators to weight mining and energy extraction indicators higher and to create lookups
  - Utilized the ES framework to create a higher risk score for suspicious assets or identities
- Load the threat intelligence into Enterprise Security
- Created an automated workflow action
- Added context to our use cases
Use the Add-on Builder
iDefense APIs

- **Threat indicator API**
  - All known iDefense threat indicators

- **Fundamental API**
  - Industry specific threat indicators
  - Mining and Energy extraction indicators
Scheduled searches to correlate common indicators between the Threat Indicator API and the Mining and Energy Extraction threat indicators

- Increased the weight for Mining and Energy Extraction threat indicators. Utilizes the Enterprise Security Threat Intelligence framework to raise the risk score of an asset or identity. This allows incident responders to quickly identify relevant threats to the Freeport-McMoRan environment.

- Output lookup to be imported into Enterprise Security

<table>
<thead>
<tr>
<th>description</th>
<th>file_hash</th>
<th>weight</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mining and Energy Extraction Indicator</td>
<td>7012f07e82092ab2daede774b9000d64</td>
<td>100</td>
</tr>
<tr>
<td>last seen as: MALWARE_C2, last published: 2016-09-26T18:50:31.000Z, threat types: Cyber Espionage</td>
<td></td>
<td></td>
</tr>
<tr>
<td>last seen as: EXPLOIT, last published: 2017-08-11T12:46:32.000Z, threat types: Cyber Crime</td>
<td></td>
<td></td>
</tr>
<tr>
<td>last seen as: MALWARE_C2_2, last published: 2013-12-03T04:11:59.000Z, last modified: 2017-05-08T13:29:48.000Z, threat types: Cyber Espionage</td>
<td>60bcad2e2ead6836681449</td>
<td>60</td>
</tr>
<tr>
<td>last seen as: MALWARE_DOWNLOAD, last published: 2013-12-03T04:11:59.000Z, last modified: 2017-05-08T13:29:48.000Z, threat types: Cyber Espionage</td>
<td>37c7d4752644d7a210c6f425e8f7944</td>
<td>80</td>
</tr>
</tbody>
</table>
Load the Threat Indicators into ES

- Web UI
  - Enterprise Security > Configure > Data Enrichment > Threat Intelligence Downloads
- Inputs.conf

<table>
<thead>
<tr>
<th>iDefense</th>
<th>threatlist</th>
<th>iDefense Threat Intelligence pertaining to</th>
<th>lookup://iDefense_domain_intel</th>
</tr>
</thead>
<tbody>
<tr>
<td>domain</td>
<td>threatlist</td>
<td>iDefense Threat Intelligence pertaining to</td>
<td>lookup://iDefense_file_intel</td>
</tr>
<tr>
<td>file</td>
<td>threatlist</td>
<td>iDefense Threat Intelligence pertaining to</td>
<td>lookup://iDefense_http_intel</td>
</tr>
<tr>
<td>http</td>
<td>threatlist</td>
<td>iDefense Threat Intelligence pertaining to</td>
<td>lookup://iDefense_ip_intel</td>
</tr>
</tbody>
</table>
Created a new workflow action in workflow_actions.conf

- Search for any notable event field in the iDefense Intel Graph. Allows incident responders to quickly identify related indicators to search for in Splunk.
Contextual Enrichment to Correlation Searches

<table>
<thead>
<tr>
<th>Description:</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host 51.15.42.180 was detected sweeping 160 hosts for udp/5061.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Additional Fields</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Action</td>
<td>blocked</td>
</tr>
<tr>
<td>Application</td>
<td>sip-tls</td>
</tr>
<tr>
<td>Destination Port</td>
<td>5061</td>
</tr>
<tr>
<td>Source</td>
<td>51.15.42.180 80</td>
</tr>
<tr>
<td>Source Expected</td>
<td>false</td>
</tr>
<tr>
<td>Source PCI Domain</td>
<td>untrust</td>
</tr>
<tr>
<td>Source Requires Antivirus</td>
<td>false</td>
</tr>
<tr>
<td>Source Should Time Synchronize</td>
<td>false</td>
</tr>
<tr>
<td>Source Should Update</td>
<td>false</td>
</tr>
<tr>
<td>Source Threat List Description</td>
<td>Unknown to iDefense</td>
</tr>
<tr>
<td>Source Zone</td>
<td>L3-untrusted</td>
</tr>
<tr>
<td>Transport Protocol</td>
<td>udp</td>
</tr>
</tbody>
</table>
The Value Realized
Value Realized

- Identified unblocked malicious activity in the environment related to iDefense threat intelligence
- Enhanced threat detection and response capabilities of the Freeport-McMoRan security team
- Increased efficiency of the SOC incident responders
Roadmap for Future Development

- Automate workflow actions leveraging Splunk’s Adaptive response capabilities
- Integrate the Vulnerability API to correlate with Vulnerability Scan data
- Including both the MD5 and SHA1 file hashes in the ThreatIndicator API
Thank You

Don't forget to rate this session in the .conf2017 mobile app