

splunk®

.conf2017

© 2017 SPLUNK INC.

# 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 27<sup>th</sup>, 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

130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category\_id=GIFTS&JSESSIONID=5D15L9FF1ADFF3 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product\_id=F1-5W-01"  
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product\_id=FL-DSH-01&JSESSIONID=5D35L7FF6ADFF0 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-268product\_id=K9-CW-01"  
137.27.160.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item\_id=EST-26&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product\_id=AV-CB-01&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/clearance.do?action=shopping\_id=RP-LI-02"  
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category\_id=GIFTS&JSESSIONID=5D15L9FF1ADFF3 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product\_id=F1-5W-01"  
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product\_id=FL-DSH-01&JSESSIONID=5D35L7FF6ADFF0 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-268product\_id=K9-CW-01"  
137.27.160.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item\_id=EST-26&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product\_id=AV-CB-01&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/clearance.do?action=shopping\_id=RP-LI-02"  
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category\_id=GIFTS&JSESSIONID=5D15L9FF1ADFF3 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product\_id=F1-5W-01"  
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product\_id=FL-DSH-01&JSESSIONID=5D35L7FF6ADFF0 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-268product\_id=K9-CW-01"  
137.27.160.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item\_id=EST-26&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product\_id=AV-CB-01&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/clearance.do?action=shopping\_id=RP-LI-02"  
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category\_id=GIFTS&JSESSIONID=5D15L9FF1ADFF3 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product\_id=F1-5W-01"  
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product\_id=FL-DSH-01&JSESSIONID=5D35L7FF6ADFF0 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-268product\_id=K9-CW-01"  
137.27.160.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item\_id=EST-26&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product\_id=AV-CB-01&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/clearance.do?action=shopping\_id=RP-LI-02"



# Introduction

---

# Personal Introduction



- ▶ Tim Plona, Freeport-McMoRan
- ▶ Business Solution Architect



- ▶ Kyle Maxwell, Accenture
- ▶ Security Principal



- ▶ Brandt Varni, Accenture
- ▶ Security Consulting Senior Analyst

130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category\_id=GIFTS&JSESSIONID=5D5SLAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product\_id=FI-SW-03" "Mozilla/5.0 (Windows NT 6.0; rv:34.0; like-firefox/34.0; .NET CLR 1.1.4322)" 468 125.17 14.1.10.10  
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product\_id=FL-DSH-01&JSESSIONID=5D5SL7FF6ADFF0 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/category.screen?category\_id=GIFTS" "Mozilla/5.0 (Windows NT 6.0; rv:34.0; like-firefox/34.0; .NET CLR 1.1.4322)" 468 125.17 14.1.10.10  
317 27.160.0.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item\_id=EST-26&JSESSIONID=5D5SL9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product\_id=AV-CB-01&JSESSIONID=5D5SL9FF1ADFF3" "Mozilla/5.0 (Windows NT 6.0; rv:34.0; like-firefox/34.0; .NET CLR 1.1.4322)" 468 125.17 14.1.10.10  
10 - - [07/Jan 18:10:56:187] "GET /category.screen?category\_id=FLOWERS&JSESSIONID=5D5SL9FF1ADFF3 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/category.screen?category\_id=FLOWERS" "Mozilla/5.0 (Windows NT 6.0; rv:34.0; like-firefox/34.0; .NET CLR 1.1.4322)" 468 125.17 14.1.10.10  
10 - - [07/Jan 18:10:56:188] "GET /category.screen?category\_id=FLOWERS&JSESSIONID=5D5SL9FF1ADFF3 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/category.screen?category\_id=FLOWERS" "Mozilla/5.0 (Windows NT 6.0; rv:34.0; like-firefox/34.0; .NET CLR 1.1.4322)" 468 125.17 14.1.10.10  
10 - - [07/Jan 18:10:56:189] "GET /category.screen?category\_id=FLOWERS&JSESSIONID=5D5SL9FF1ADFF3 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/category.screen?category\_id=FLOWERS" "Mozilla/5.0 (Windows NT 6.0; rv:34.0; like-firefox/34.0; .NET CLR 1.1.4322)" 468 125.17 14.1.10.10  
10 - - [07/Jan 18:10:56:190] "GET /category.action=remove&itemId=EST-18 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-18" "Mozilla/5.0 (Windows NT 6.0; rv:34.0; like-firefox/34.0; .NET CLR 1.1.4322)" 468 125.17 14.1.10.10

# Freeport-McMoRan Inc.



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.



130.60.4... [07/Jan 18:10:57:153] "GET /category.screen?category\_id=GIFTS&SESSIONID=SD1SLAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product\_id=FI-5W-03"  
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product\_id=FL-DSH-01&SESSIONID=SD35L7FF6ADFF9 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-268product\_id=KQ-CV-01"  
317 27.160.0.0 - - [07/Jan 18:10:56:156] "GET /product.screen?product\_id=FL-DSH-01&SESSIONID=SD35L7FF6ADFF9 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product\_id=AV-CB-01&SESSIONID=SD185L8FF2ADFF9 HTTP 1.1" 200 385 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-1189"  
10 - - [07/Jan 18:10:56:156] "GET /product.screen?product\_id=FL-DSH-01&SESSIONID=SD35L7FF6ADFF9 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product\_id=AV-CB-01&SESSIONID=SD185L8FF2ADFF9 HTTP 1.1" 200 385 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-1189"  
10 - - [07/Jan 18:10:56:156] "GET /product.screen?product\_id=FL-DSH-01&SESSIONID=SD35L7FF6ADFF9 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product\_id=AV-CB-01&SESSIONID=SD185L8FF2ADFF9 HTTP 1.1" 200 385 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-1189"  
10 - - [07/Jan 18:10:56:156] "GET /product.screen?product\_id=FL-DSH-01&SESSIONID=SD35L7FF6ADFF9 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product\_id=AV-CB-01&SESSIONID=SD185L8FF2ADFF9 HTTP 1.1" 200 385 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-1189"



# Threat Intelligence in Action

---



# 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

```

130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=5D15L4FF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-SW-01"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=5D35L7FF6ADFF0 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-268&product_id=K0-CU-01"
317.27.160.0.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=5D55L9FF1ADFF3"
10.0.0.1:5V1: - - [07/Jan 18:10:56:156] "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 3885 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-1"
10.0.0.1:5V1: .NET CLR 1.1.4322) 468 125.17 14.189] "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 3885 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-1"
  
```

# iDefense: CTI Provider

---

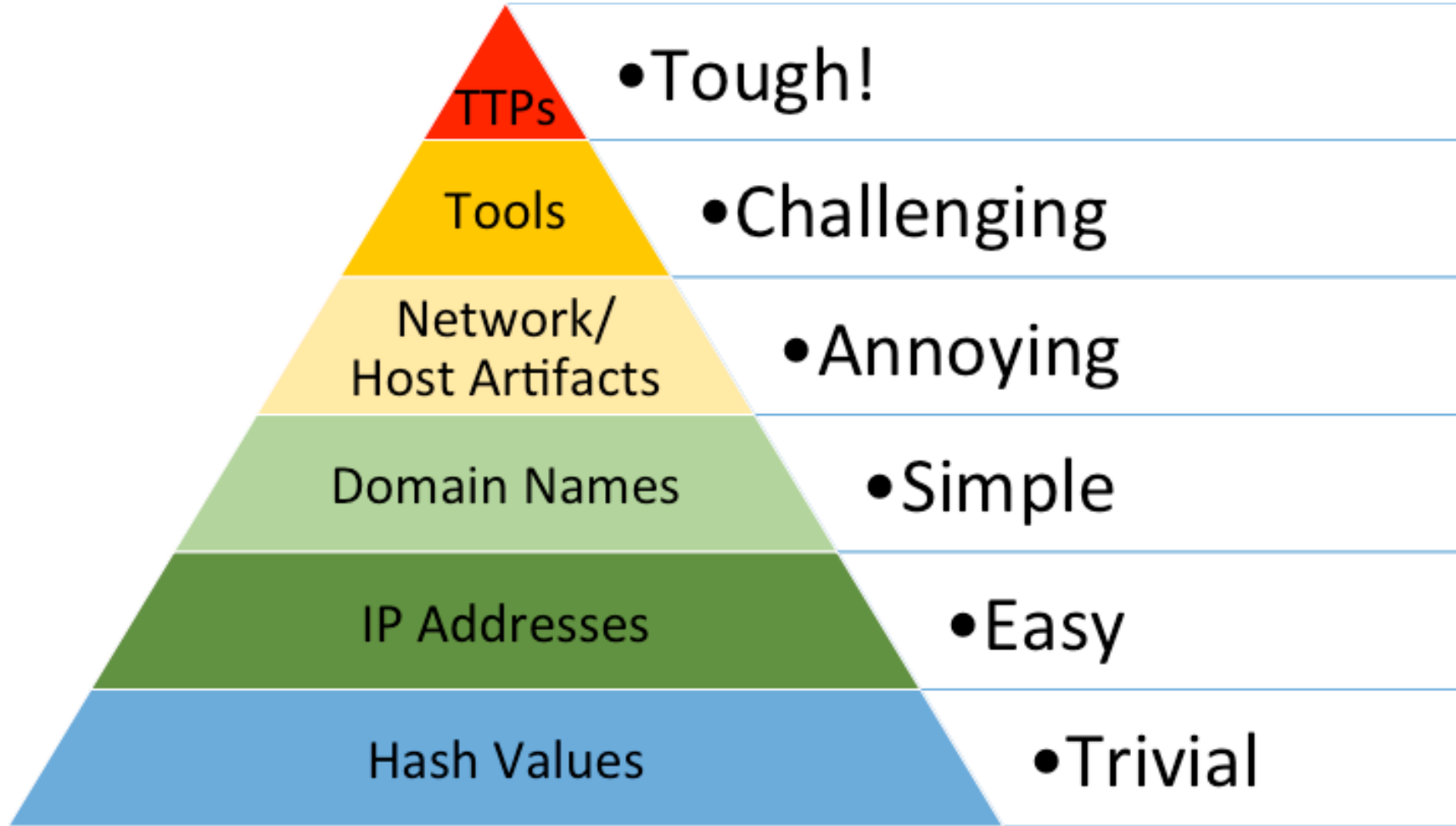
# iDefense: CTI Provider



```
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=5D15L9FF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=F1-SW-01" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17.14.108
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=5D55L7FF6ADFF0 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K0-CW-01" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17.14.108
317.27.160.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 385 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-1&product_id=FLOWERS&JSESSIONID=5D55L9FF1ADFF3" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17.14.108
```

# Pyramid of Pain

A model for tactical intelligence

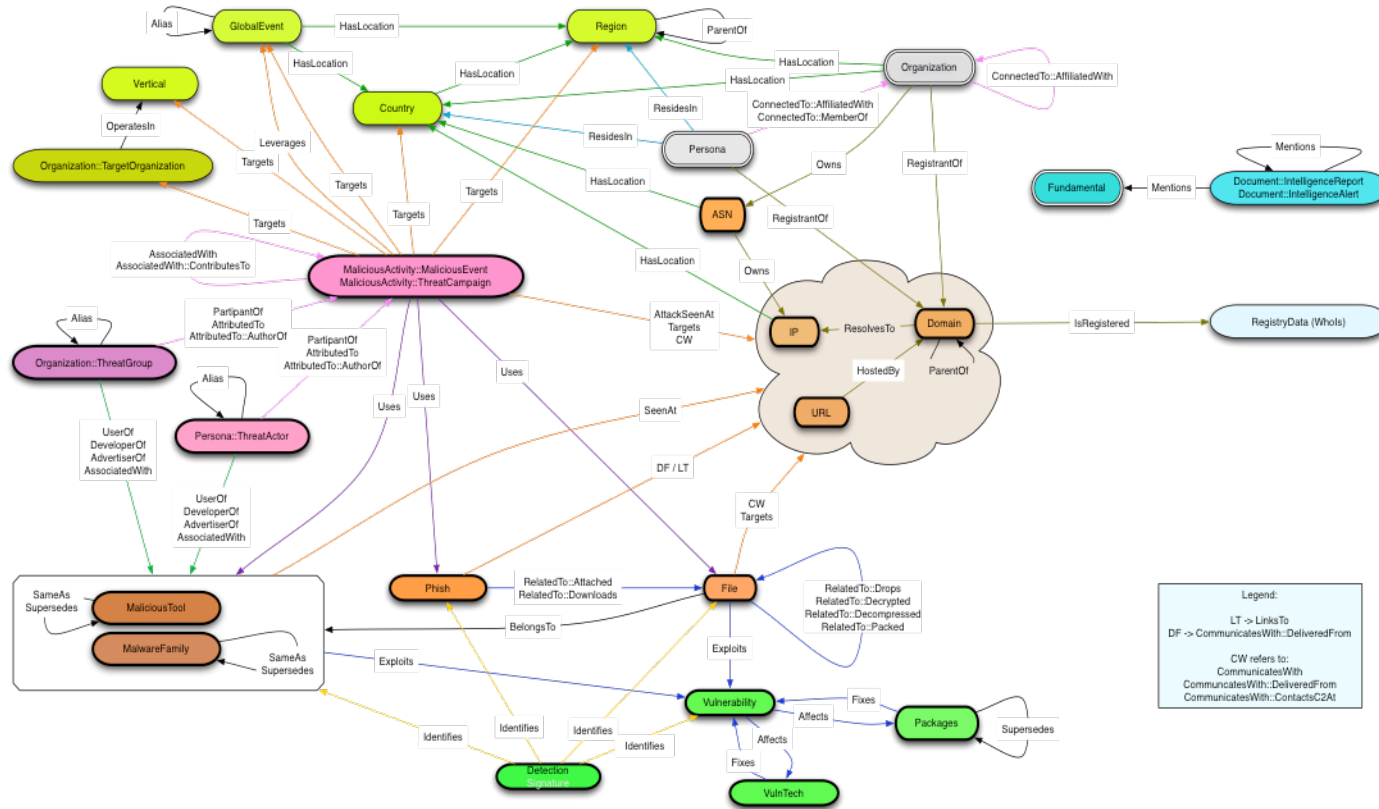


David Bianco

130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category\_id=GIFTS&JSESSIONID=5D15LAF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product\_id=FI-SW-01" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17 14.10.10.108  
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product\_id=FL-DSH-01&JSESSIONID=5D55L7FF6ADFF0 HTTP 1.1" 404 322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product\_id=AV-CB-01&JSESSIONID=5D15LAF10ADFF10 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-18&product\_id=AV-CB-01&JSESSIONID=5D15LAF10ADFF10 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-6&JSESSIONID=5D15LAF10ADFF10 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-18" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17 14.10.10.108  
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category\_id=GIFTS&JSESSIONID=5D15LAF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product\_id=FI-SW-01" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17 14.10.10.108  
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product\_id=FL-DSH-01&JSESSIONID=5D55L7FF6ADFF0 HTTP 1.1" 404 322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product\_id=AV-CB-01&JSESSIONID=5D15LAF10ADFF10 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-18&product\_id=AV-CB-01&JSESSIONID=5D15LAF10ADFF10 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-6&JSESSIONID=5D15LAF10ADFF10 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-18" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17 14.10.10.108  
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category\_id=GIFTS&JSESSIONID=5D15LAF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product\_id=FI-SW-01" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17 14.10.10.108  
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product\_id=FL-DSH-01&JSESSIONID=5D55L7FF6ADFF0 HTTP 1.1" 404 322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product\_id=AV-CB-01&JSESSIONID=5D15LAF10ADFF10 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-18&product\_id=AV-CB-01&JSESSIONID=5D15LAF10ADFF10 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-6&JSESSIONID=5D15LAF10ADFF10 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-18" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17 14.10.10.108

# IntelGraph Ontology

## Graph Data Model



130.60.4 - - [07/Jan 18:10:57:123] "GET /category.screen?category\_id=GIFTS&SESSIONID=SD5SLAFF10ADFF10 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product\_id=FI-5W-03" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17 14.0.0.0

# IntelGraph API

## Swagger / OpenAPI interface

Accenture Security default (/api-docs) ▾  Explore

### iDefense REST Customer API

REST Customer API Documentation

document : <a href="#">Document API</a>	Show/Hide	List Operations	Expand Operations
fundamental : <a href="#">Fundamental API</a>	Show/Hide	List Operations	Expand Operations
threatindicator : <a href="#">ThreatIndicator API</a>	Show/Hide	List Operations	Expand Operations
vulnerability : <a href="#">Vulnerability API</a>	Show/Hide	List Operations	Expand Operations

[ BASE URL: /rest , API VERSION: 0 ]

```

130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=5D1SLAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-SW-01"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=5D35L7FF6ADFF0 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=KQ-CB-01"
ows NT 5.1; SV1; .NET CLR 1.1.4322) "GET /oldlink?item_id=EST-26&JSESSIONID=5D35L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=5D18SL8FF2ADFF9"
do?buttercup-shopping_id=RP-LI-02" 468 125.17 14.00.00.00 "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D35L9FF1ADFF3 HTTP 1.1" 200 3885 "http://buttercup-shopping.com/category.screen?category_id=FLOWERS&JSESSIONID=5D35L9FF1ADFF3"
shopping.com/cart.do?action=purchase&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=5D18SL8FF2ADFF9"
shopping.com/cart.do?action=remove&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=5D18SL8FF2ADFF9"

```

# 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



130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category\_id=GIFTS&JSESSIONID=5D15LAF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product\_id=FI-5W-01"  
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product\_id=FL-DSH-01&JSESSIONID=5D55L7FF6ADFF0 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-268&product\_id=KQ-CU-01"  
317.27.160.0.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item\_id=EST-26&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/changequantity&itemId=EST-18&product\_id=AV-CB-01&JSESSIONID=5D55L7FF6ADFF0 HTTP 1.1"  
...  
10.10.10.10 - - [07/Jan 18:10:55:187] "GET /category.screen?category\_id=FLOWERS&JSESSIONID=5D55L7FF6ADFF0 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-14&product\_id=FI-5W-01"  
...  
10.10.10.10 - - [07/Jan 18:10:55:188] "GET /category.screen?category\_id=FLOWERS&JSESSIONID=5D55L7FF6ADFF0 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-14&product\_id=FI-5W-01"  
...

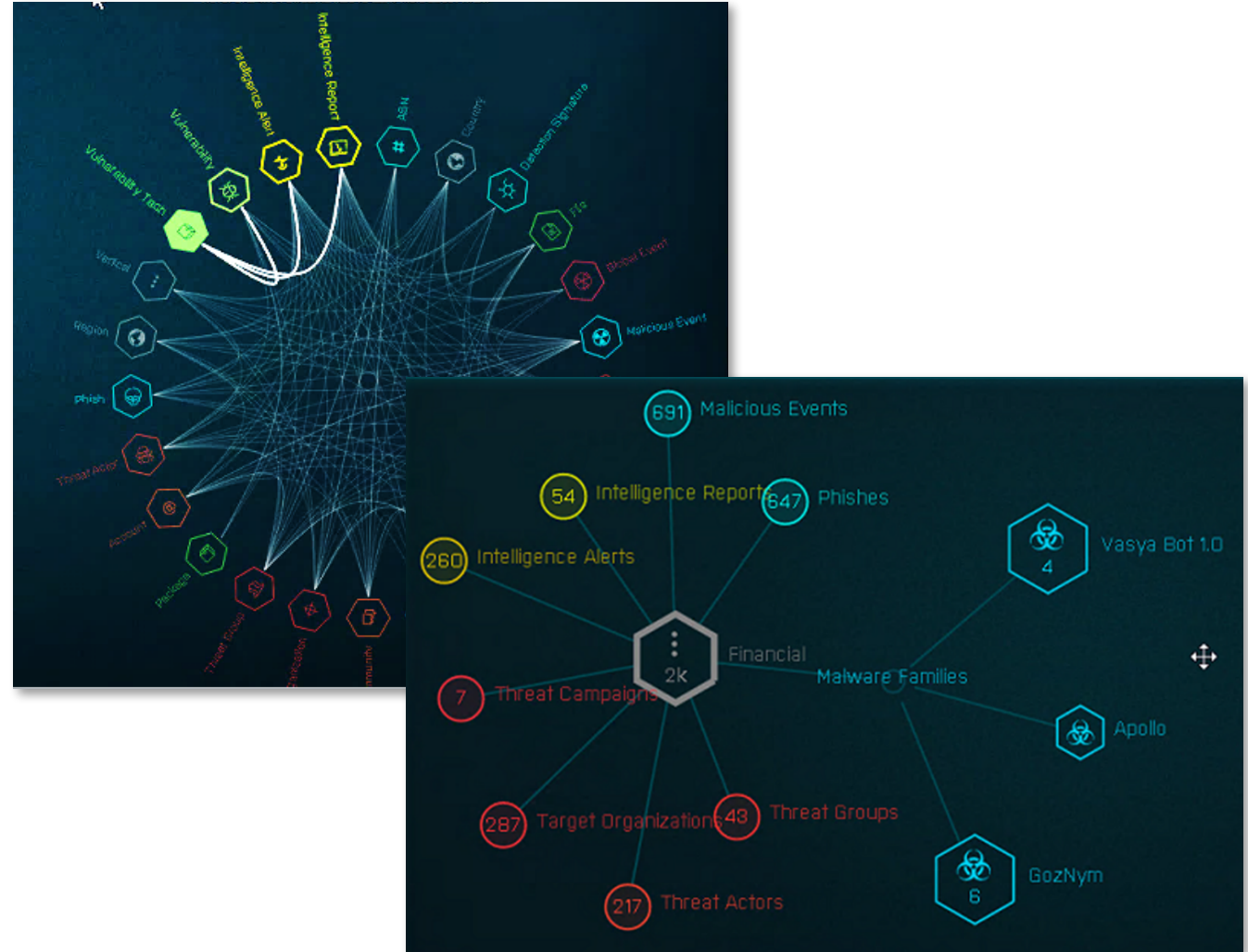
# iDefense APIs

## ▶ Threat indicator API

- All known iDefense threat indicators

## ▶ Fundamental API

- Industry specific threat indicators
- Mining and Energy extraction indicators



# Threat Indicator Weighting

- ▶ Scheduled searches to correlated 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

description ^	file_hash	file_name	weight
Mining and Energy Extraction Indicator last seen as: MALWARE_C2, last published: 2016-09-26T18:50:31.000Z 2016-09-26T18:50:33.000Z 2016-09-26T18:50:35.000Z, last modified: 2017-04-16T14:17:18.000Z 2017-04-16T14:17:20.000Z, threat types: Cyber Espionage	7012f07e82092ab2daede774b9000d64		100
last seen as: EXPLOIT, last published: 2017-08-11T12:46:32.000Z, last modified: 2017-08-11T12:46:32.000Z, threat types: Cyber Crime	60bcad2e2ead668366814498		60
last seen as: MALWARE_C2 MALWARE_DOWNLOAD, last published: 2013-12-03T04:11:59.000Z, last modified: 2017-05-08T13:29:48.000Z, threat types: Cyber Espionage	37c7b4752644df7a210c6f425e8f7944		80

Increased Weight

# Load the Threat Indicators into ES

## ► Web UI

- Enterprise Security > Configure > Data Enrichment > Threat Intelligence Downloads

## ► Inputs.conf



Splunk Enterprise  
Security™

idefense_domain_intel	threatlist	iDefense Threat intelligence pertaining to domains	lookup://idefense_domain_intel
idefense_file_intel	threatlist	iDefense Threat intelligence pertaining to files	lookup://idefense_file_intel
idefense_http_intel	threatlist	iDefense Threat intelligence pertaining to HTTP	lookup://idefense_http_intel
idefense_ip_intel	threatlist	iDefense Threat intelligence pertaining to IPs	lookup://idefense_ip_intel

# Workflow Action in ES

- ▶ 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.

The diagram illustrates the process of creating a workflow action in Splunk. On the left, a dropdown menu is shown with the following options:

- Edit Tags
- Access Search (as destination)
- Access Search (as source)
- Asset Center
- Asset Investigator
- Domain Dossier
- Map 51.15.42.180
- Google 51.15.42.180
- Search iDefense IntelGraph** (highlighted with a green box)
- Intrusion Search (as destination)

A green speech bubble labeled "Workflow Action" points to the highlighted option. A large green arrow points from the dropdown menu to the right, where a screenshot of the iDefense IntelGraph interface is shown. The screenshot displays a search input field with "51.15.42.180" entered, and the search results below indicate "Search Results for '51.15.42.180'".

# Contextual Enrichment to Correlation Searches

## Description:

Host 51.15.42.180 was detected sweeping 160 hosts for udp/5061.

## Additional Fields

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

Context on  
known  
indicators

```

130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=5D5L9FF1ADFF3 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-SW-03"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=5D5L9FF1ADFF3 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-268&product_id=KQ-CU-01"
ows NT 5.1; SV1; .NET CLR 1.1.4322" 468 125.17 14.1.1.1 "GET /oldlink?item_id=EST-26&JSESSIONID=5D5L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=5D5L9FF1ADFF3"
://buttercup-16&product_id=RP-LI-02" 404 125.17 14.1.1.1 "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D5L9FF1ADFF3 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-189"
http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-108" "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D5L9FF1ADFF3 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-108"

```



# 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

```
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=5D15L9FF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-SW-01"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=5D35L7FF6ADFF0 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=KQ-CW-01"
ows NT 5.1; SV1; .NET CLR 1.1.4322" 468 125.17 14.1.1.1 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-16&product_id=RP-LI-02"
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=5D15L9FF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-SW-01"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=5D35L7FF6ADFF0 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=KQ-CW-01"
ows NT 5.1; SV1; .NET CLR 1.1.4322" 468 125.17 14.1.1.1 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-16&product_id=RP-LI-02"
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=5D55L9FF1ADFF3"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /oldlink?item_id=EST-26&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-18"
ows NT 5.1; SV1; .NET CLR 1.1.4322" 468 125.17 14.1.1.1 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-16&product_id=RP-LI-02"
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=5D55L9FF1ADFF3"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /oldlink?item_id=EST-26&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-18"
ows NT 5.1; SV1; .NET CLR 1.1.4322" 468 125.17 14.1.1.1 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-16&product_id=RP-LI-02"
```



# 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

```

130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=5D15LAF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-SW-01"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=5D35L7FF6ADFF0 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K0-CU-01"
317.27.160.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=5D5$L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=5D18L5L8FF2ADFF9 HTTP 1.1"
125.17.14.1 - - [07/Jan 18:10:55:187] "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-1&product_id=K0-CU-01"

```

# Q&A

Tim Plona | Business Solution Architect

Kyle Maxwell | Security Principal

Brandt Varni | Security Consulting Senior Analyst

# Thank You

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

splunk> .conf2017