splunk> .conf2017

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.

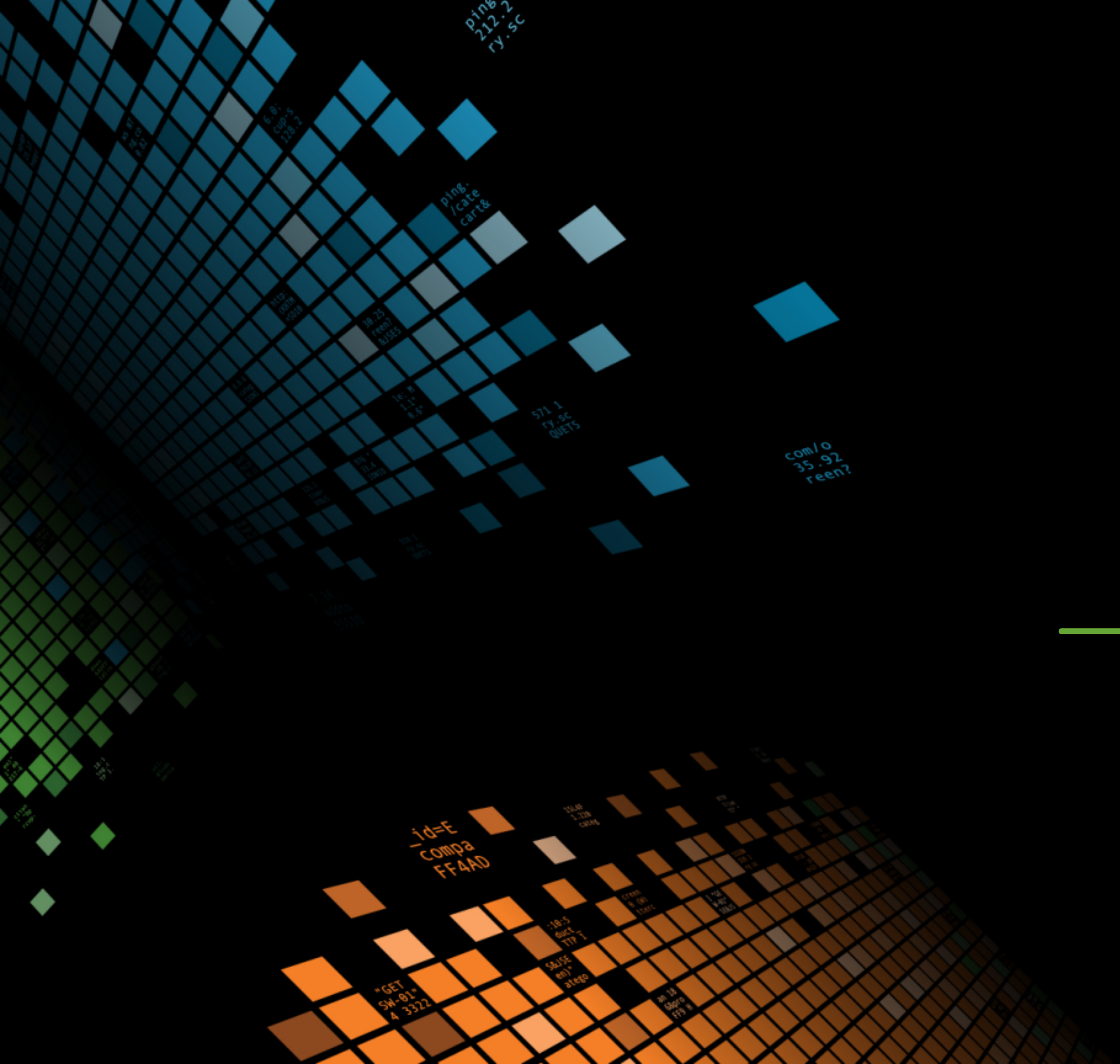
The forward-looking statements made in this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward looking statements 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.

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

Agenda

- Introduction
- Threat Intelligence in Action
- iDefense: CTI Provider
- Integrating iDefense Threat Intelligence in Splunk
- The Value Realized



Introduction

Personal Introduction

- Tim Plona, Freeport-McMoRan
- Business Solution Architect

- Kyle Maxwell, Accenture
- Security Principal

- Brandt Varni, Accenture
- Security Consulting Senior Analyst

Freeport-McMoRan Inc.

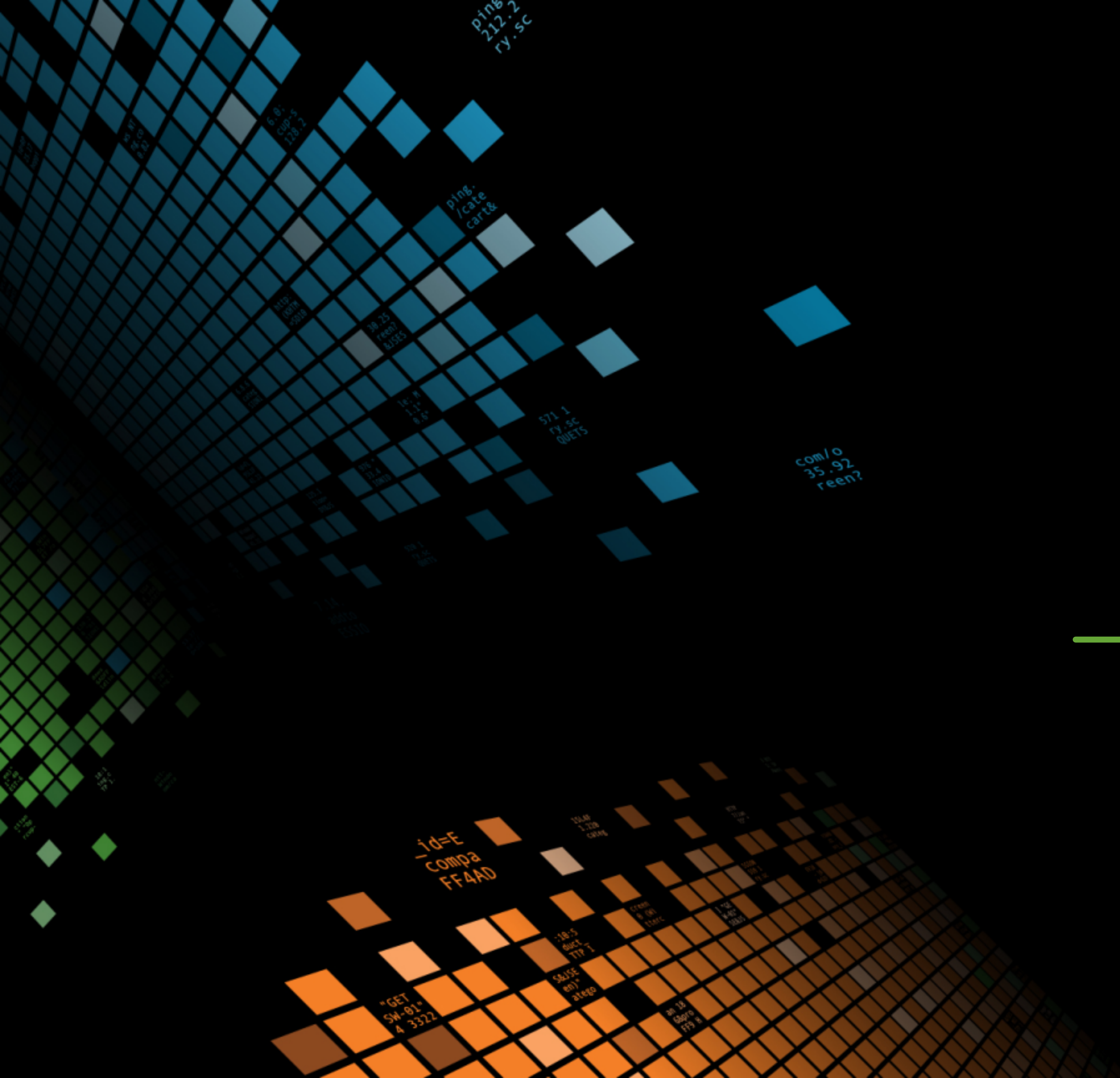
FREEPORT-McMoRAN

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

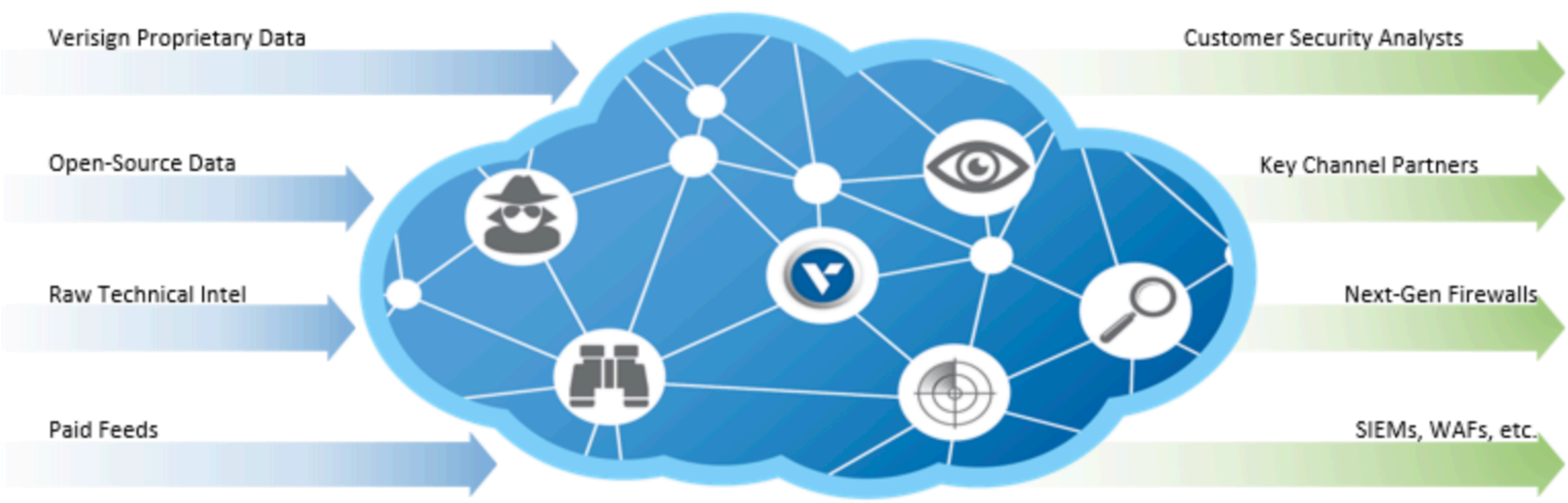
Threat Intelligence in Action

- 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



DATA SOURCES

- Verisign Proprietary Data
- Open-Source Data
- Raw Technical Intel
- Paid Feeds

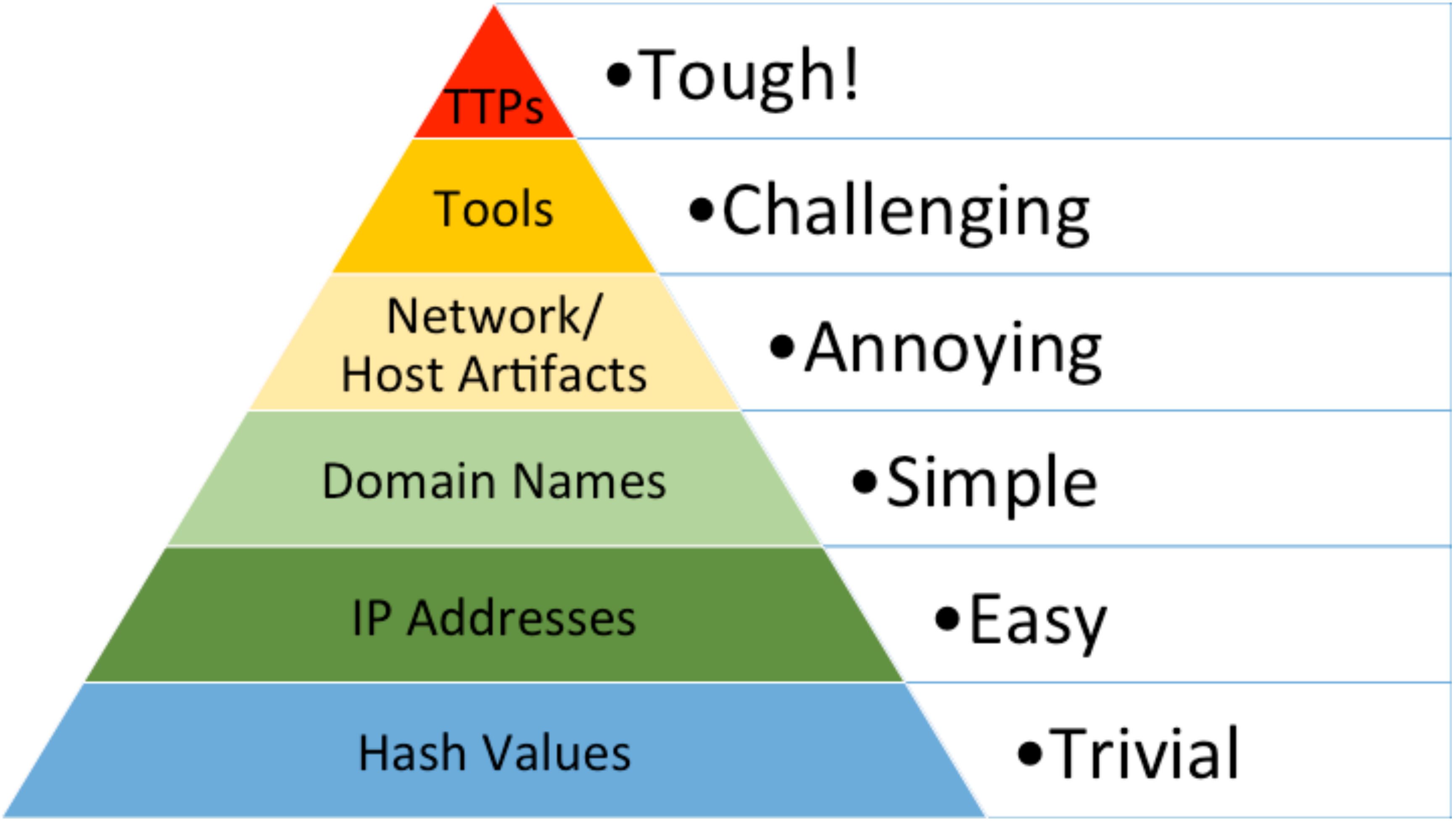
DISTRIBUTION CHANNELS

- Customer Security Analysts
- Key Channel Partners
- Next-Gen Firewalls
- SIEMs, WAFs, etc.

iDefense® IntelGraph

Pyramid of Pain

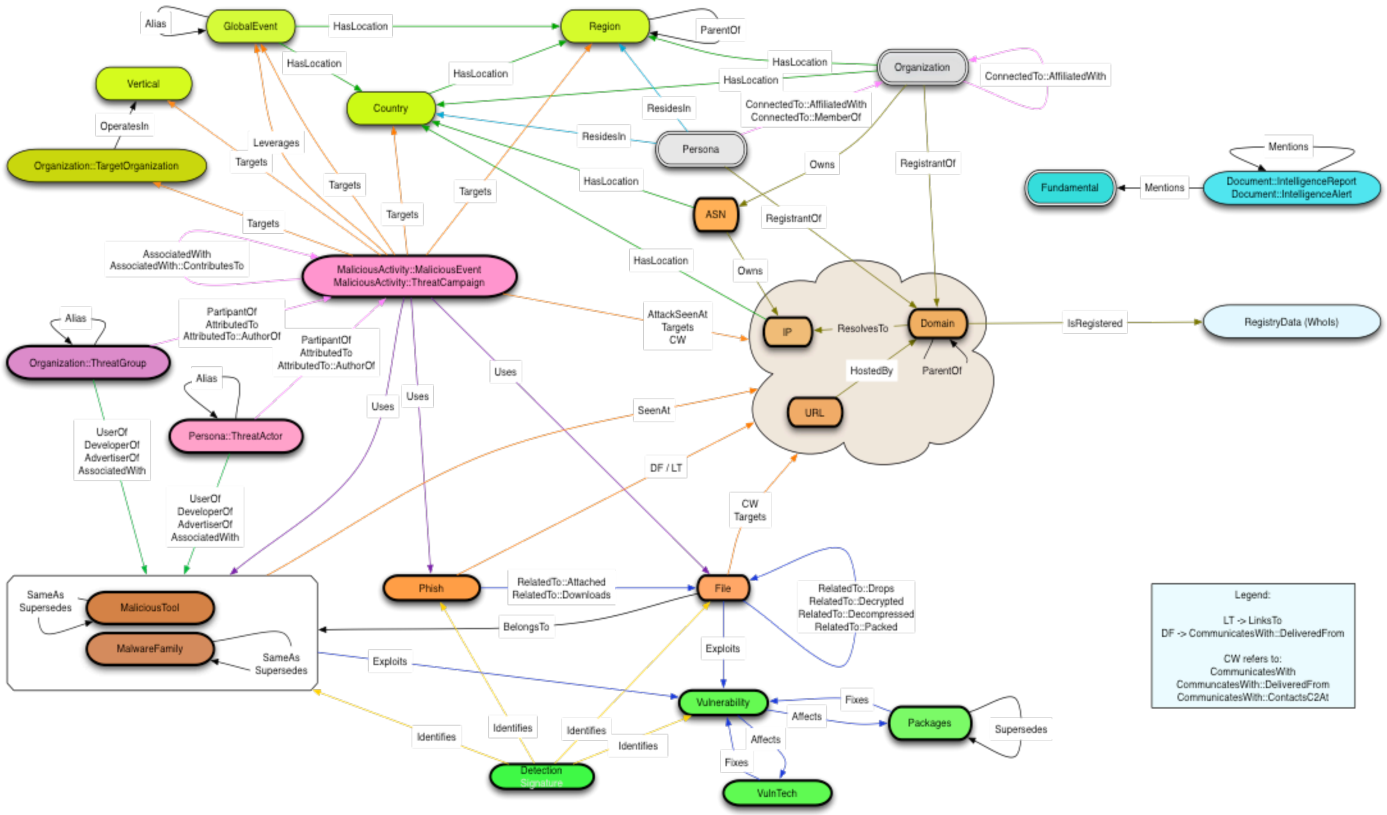
A model for tactical intelligence



David Bianco

IntelGraph Ontology

Graph Data Model



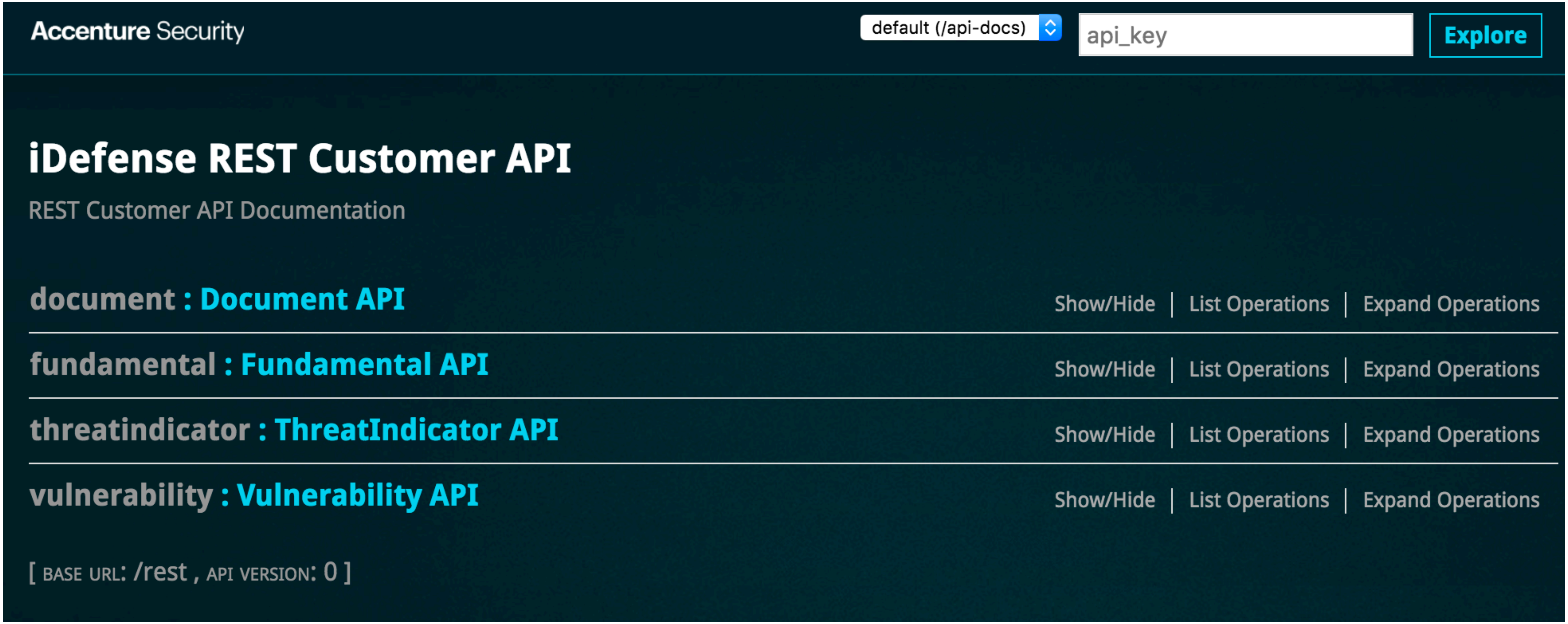
Legend:

LT -> LinksTo
DF -> CommunicatesWith::DeliveredFrom

CW refers to:
CommunicatesWith
CommuncatesWith::DeliveredFrom
CommunicatesWith::ContactsC2At

IntelGraph API

Swagger / OpenAPI interface



Accenture Security

iDefense REST Customer API

REST Customer API Documentation

document : **Document API** Show/Hide | List Operations | Expand Operations

fundamental : **Fundamental API** Show/Hide | List Operations | Expand Operations

threatindicator : **ThreatIndicator API** Show/Hide | List Operations | Expand Operations

vulnerability : **Vulnerability API** Show/Hide | List Operations | Expand Operations

[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

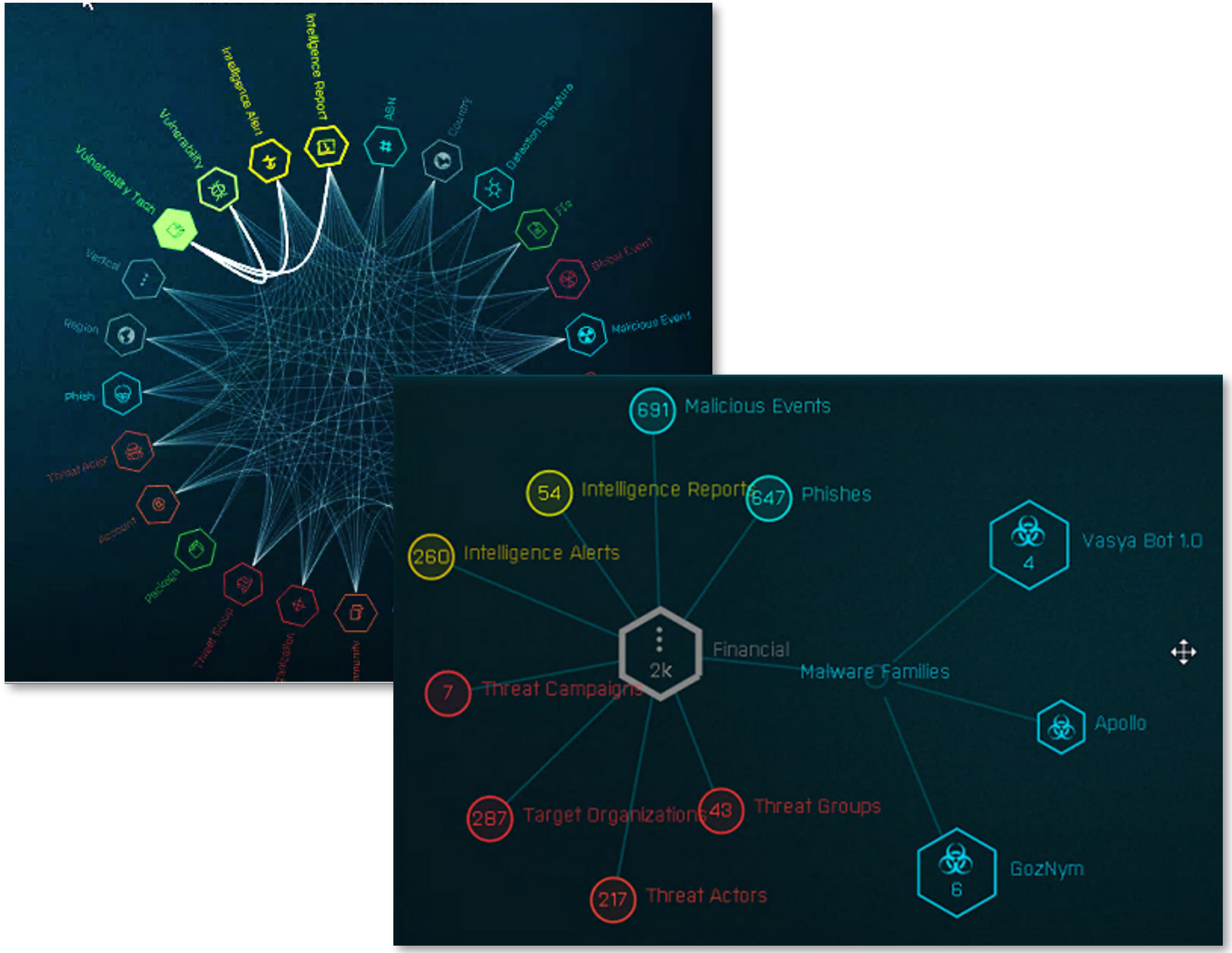
Use the Add-on Builder

Splunk Add-on Builder

python™

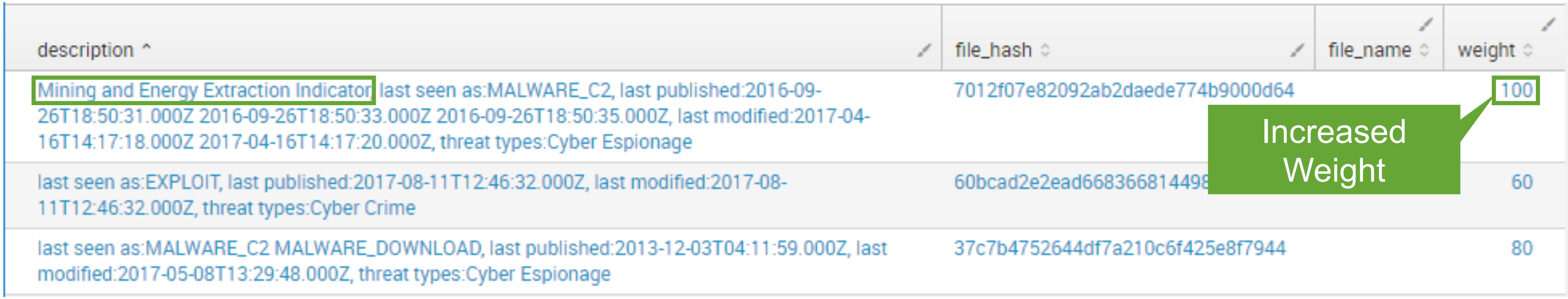
iDefense APIs

- 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

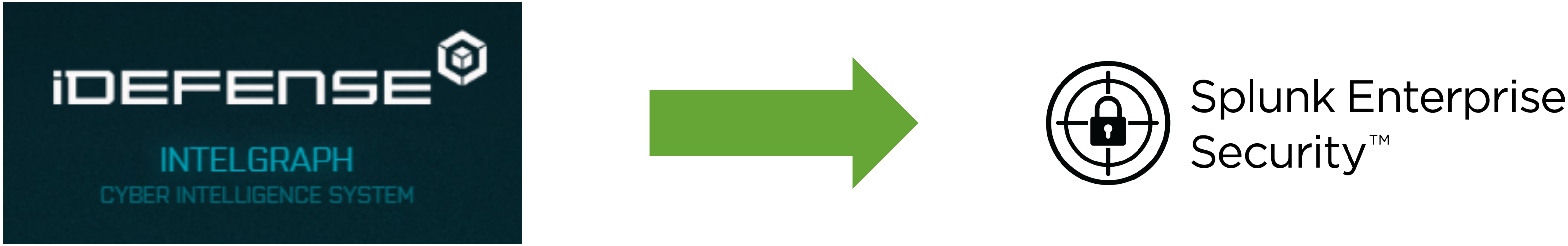


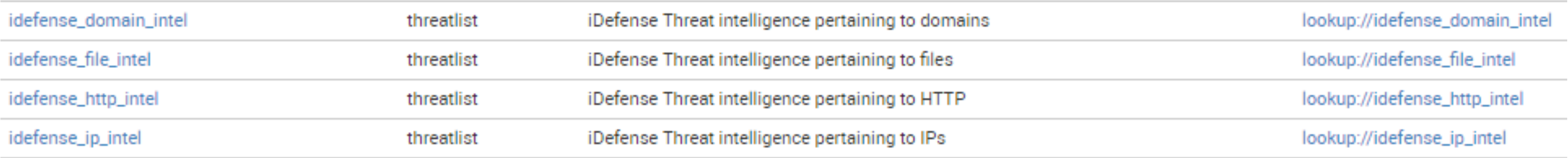
description ^	file_hash	file_name	weight
Mining and Energy Extraction Indicator last seen as:MALWARE_C2, last published:2016-09-26T18:50:31.000Z 2016-09-26T18:50:33.000Z 2016-09-26T18:50:35.000Z, last modified:2017-04-16T14:17:18.000Z 2017-04-16T14:17:20.000Z, threat types:Cyber Espionage	7012f07e82092ab2daede774b9000d64		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



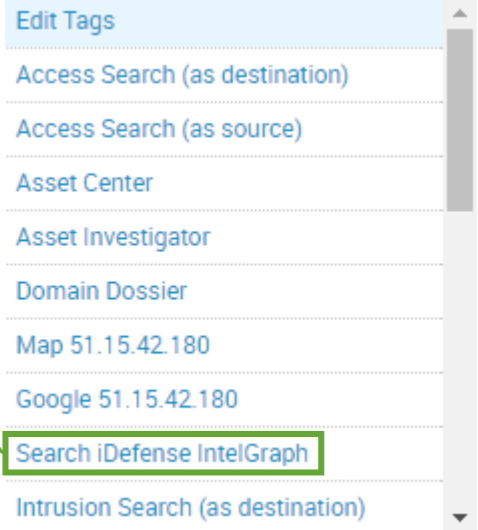


idefense_domain_intel	threatlist	iDefense Threat intelligence pertaining to domains	lookup://idefense_domain_intel
idefense_file_intel	threatlist	iDefense Threat intelligence pertaining to files	lookup://idefense_file_intel
idefense_http_intel	threatlist	iDefense Threat intelligence pertaining to HTTP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

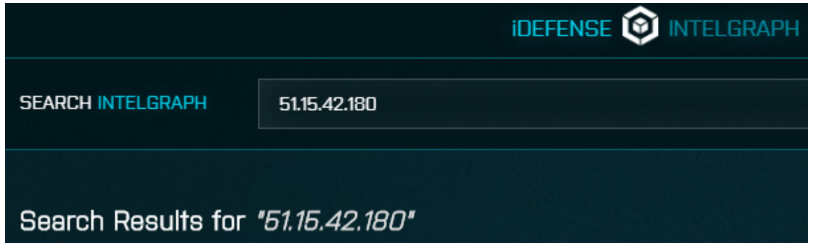
Workflow Action in ES

- 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.

Workflow Action



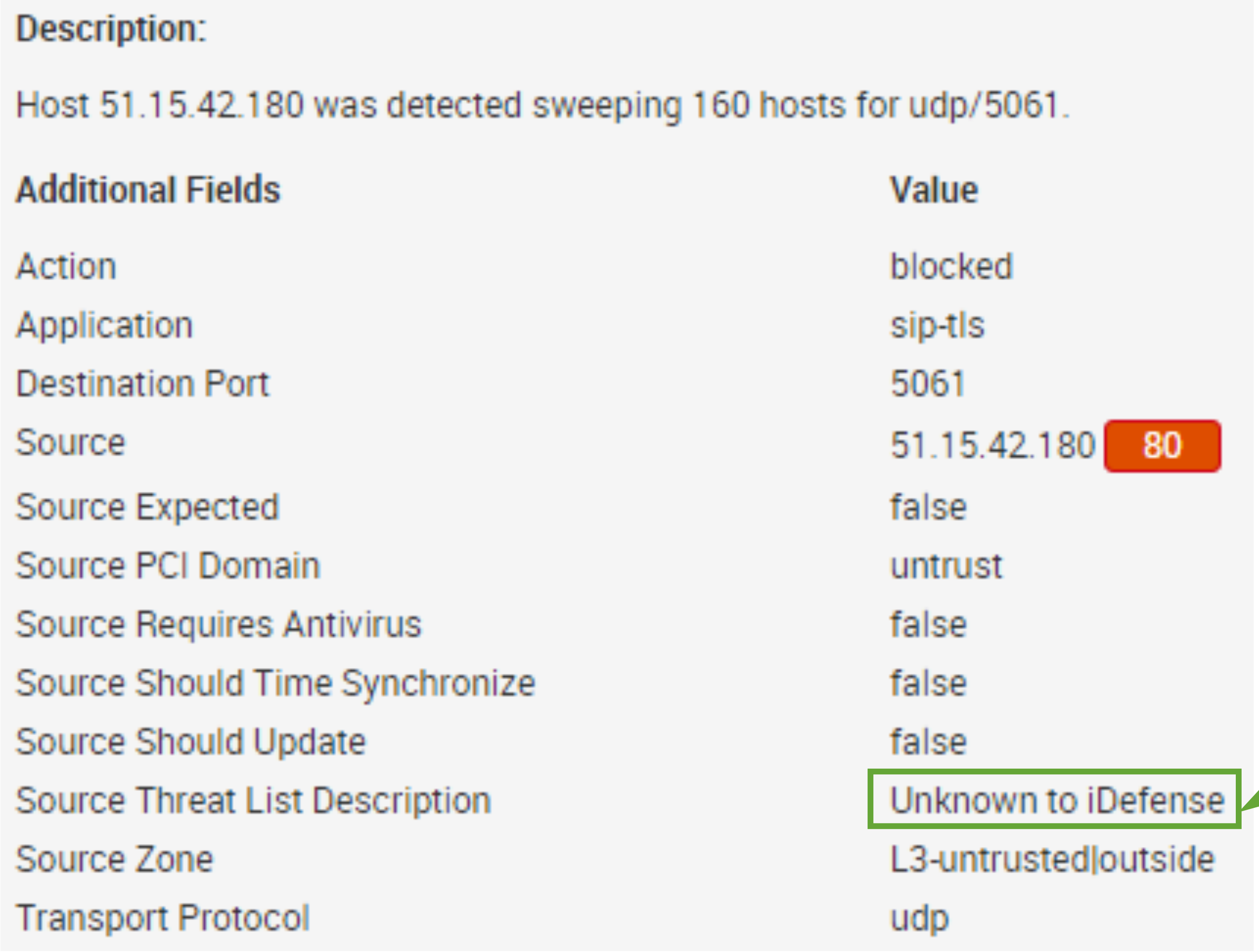
Edit Tags
Access Search (as destination)
Access Search (as source)
Asset Center
Asset Investigator
Domain Dossier
Map 51.15.42.180
Google 51.15.42.180
Search iDefense IntelGraph
Intrusion Search (as destination)



SEARCH INTELGRAPH: 51.15.42.180

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	Value
Action	blocked
Application	sip-tls
Destination Port	5061
Source	51.15.42.180 80
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

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

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