The Key to Success in the Fight Against Coordinated Attacks

Timothy Lee | CISO, City of Los Angeles
Ernie Welchm | Staff Engineer, Splunk

September 2018 | Version 2.5

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.

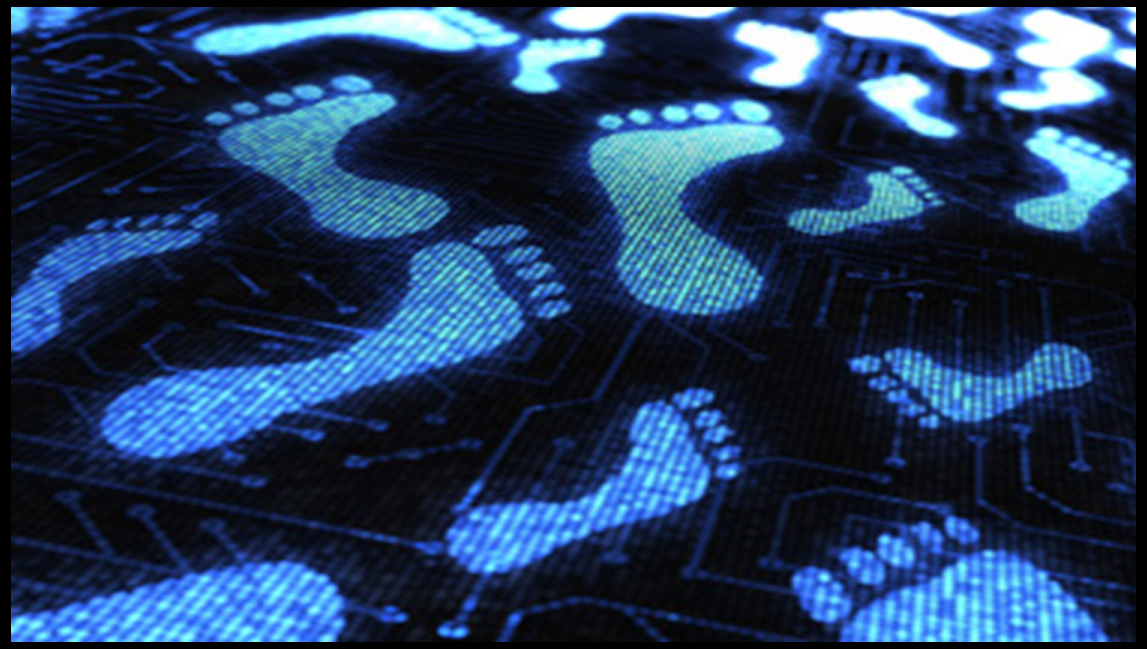
The forward-looking statements made in this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward-looking statements 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> .conf18

Our “Cyber Footprint”

A target rich environment

- World’s fifth busiest airport (LAX)
- High-profile police department (LAPD)
- Infrastructure supporting >4 million residents
- 48,000 employees
- 100,000 network connections



Our Threats

Threat assessment

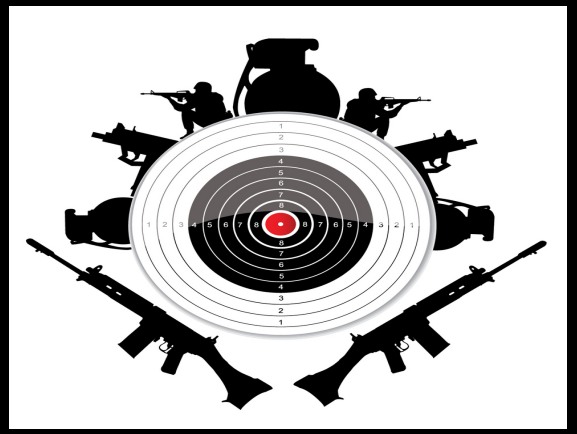
- 5 new cyber threats per second *(TechCrunch, June 2018)*
- City analyzes ~700 Million events per 24 hours
- City blocks 3 million automated attacks per day!
- Focus on critical service disruption, data theft, ransomware, social engineering

Their Motivation

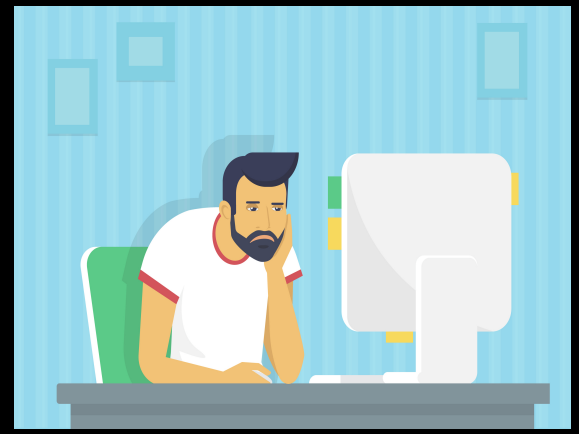
What are the driving motivators?

Political

Financial



State Sponsored



Bored


DAILY NEWS

World - Business - Finance - Lifestyle - Travel - Sport - Weather

Issue: 240104 THE WORLDS BEST SELLING NATIONAL NEWSPAPER Est - 1965

First Edition Monday 5th June

WANNACRY TAKES DOWN 300,000 BUSINESSES IN 150 COUNTRIES

HOSPITALS AND PUBLIC SERVICES AFFECTED ACROSS UK

Cyber Threat Landscape

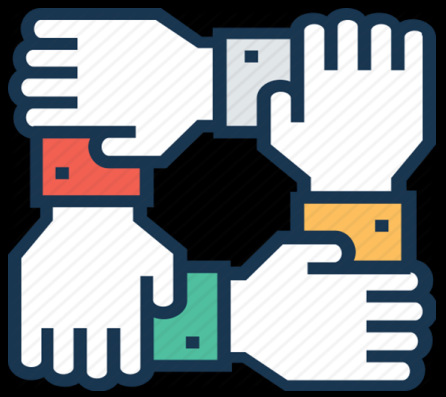
Less Predictable

More Persistent

More Organized

More Connected

Why Cyber Collaboration?



average time to detect a breach

191 days

average time from discovery to containment

66 days

Ponemon Institute 2017

How Long Does it Take to Breach a Network?

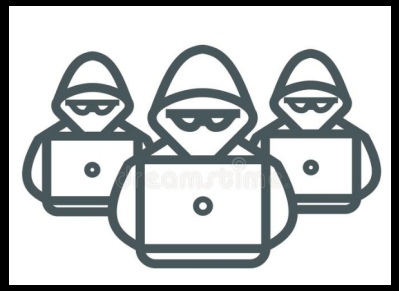
< 15 Hours

Nuix Report 2018

Bad Guys are Collaborating

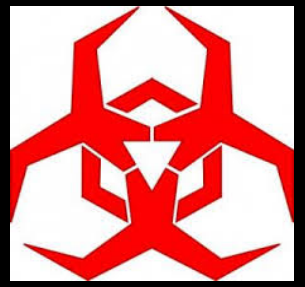
We must do the same

1. Research



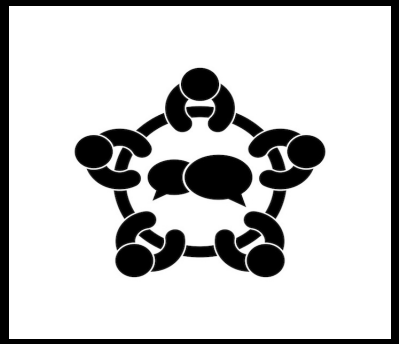
2. Infiltration

3. Execution



4. Command & Control

5. Exfiltration



$$$ Hacking Ecosystem

Timothy Lee, May 17th 2018

splunk> .conf18

Collaborative Defense against Collaborative Attack

Our Strategy

Mayor's Executive Directive

- Cyber Intrusion Command Center
- Intergrated Security Operations Center
- Critical Asset Protection Program
- LA Cyber Lab (Public-Private Partnership)

LA CYBER LAB

LA launches CyberLab to share more threat information with region's businesses

The new tech platform and public-private partnership aims to protect critical IT infrastructure and aid businesses to fight cyberattacks in real time.

By *Jason Shueh*

AUGUST 16, 2017 9:23 AM

BIO

Government

Academia

Business

A Public-Private Partnership
Benefits All

LA Cyber Lab Members

Current active members

- Public: City of LA, LAPD, FBI, DHS, CalOES
- Private: City National Bank, Riot Games, Hulu, Southern California Edison, Cisco, CGI, Westfield, Dell, PWC, mICROSOFT
- Acadamic: USC, Cal State Univsersity

Initiative 1: Cyber Alerts

1. Daily Threat Brief

LA CYBER LAB

LA Cyber Lab Threat Report

August 28, 2018

Daily Threat Report

Global Findings - Information Security

Australians Fooled into Giving Remote Access to Scammers
New Side-Channel Attack Uses Microphone to Read Screen Content
Google Tells Toomey Hackers Tried to Infiltrate Staff Email
Cyber Security and Digital Transformation Ministries Scrapped
Atlas Quantum Cryptocurrency Investment Platform Suffers Data Breach
Fortnite Android App Vulnerable to Man-in-the-Disk Attacks
Smartphones From 11 OEMs Vulnerable to Attacks via Hidden AT Commands
NewsGuard Browser Extension Aims to Alert You to Fake News Sites
UK-Based EE Fixed Two Security Vulnerabilities In A Week
North Korea-linked Hackers Stole $13.5 Million From Cosmos Bank: Report
'IRL' App Could Compromise Your Personal Information
Sacrilegious Spies: Russians Tried Hacking Orthodox Clergy
Hindu Mahasabha's Website Hacked, Beef Recipe Uploaded
Microsoft is Using Blockchain Technology to Curb Spam Calls in India
Turkish 'Hacktivists' Make Cyberattacks on U.S. Journalists
Facebook Bans Military Accounts in Myanmar as UN Accuses Leaders of Coordinating Genocide
Who's Behind the Screencam Extortion Scam? [Update]
Abbyy Leaked 203,000 Sensitive Customer Documents in Server Lapse
Fraudsters Can Access Sensitive Information from Abandoned Domains

2. Daily IOC (DHS + LA ISOC)

threat_collection	domain	file_hash	file_name	file_path	file_size	ip	src_user	url
file_intel		0568aec5bd0440c6	scan_01711_029pdf.arj		419593			
file_intel		3fad6aaa5ee4e422	shit.exe		15360			
file_intel		9da76f7682088603	Proforma Invoice.zip		666000			
file_intel		992a779e6d816c16	2199179228703-107-0_attach.1.Dec 201		1253965			
file_intel		deec3ab201c2fb081	Proforma Invoice.exe		1206784			
file_intel		62cb8c8a0bef0b6f1	scan_01711_029pdf.exe		779776			
file_intel		9a5d851fd674f851c	Complaint E-mail.exe		1132032			
file_intel		222ae4e0a8fc83ab6	Dec 2017-Proforma Invoice.exe		1368064			
file_intel		d89220f24e0c02e7f	Complaint E-mail.zip		569169			
email_intel							support@onoffapp.com	
email_intel							marketing@dreamfine.com	
email_intel							noreply@secureserver.net	
email_intel							info@standardchartered.ae	
email_intel							tsachs@WestmorelandCC.com	
email_intel							Info@naukri.com	
email_intel							accounts@elegantship.com	
email_intel							hlowry@hanklowryelectric.com	
email_intel							GBosen@northstarsl.com	
http_intel								https://bijuliman.com
http_intel								https://atoesp.org.br/
http_intel								https://nlh.gr/zjhshj.h
http_intel								https://smcbmc-europ
http_intel								https://discoveryfood
ip_intel						113.13.186.55		
ip_intel						67.11.192.51		
ip_intel						76.103.101.152		
ip_intel						59.33.43.228		
ip_intel						59.33.69.178		
ip_intel						116.28.54.63		
ip_intel						5.196.68.118		

Initiative 2: Mutual Information Exchange

- **Implementation of near-real time threat information exchange in STIX/TAXII format**

- **Los Angeles Integrated SOC, Private sector partners, Federal partners (DHS, NCCIC)**

Initiative 3: Cybersecurity Innovation Incubator

- hosts networking events for the business community , connecting attendees to federal law enforcement resources and cutting-edge practitioners in cybersecurity

- partners with academia to provide cybersecurity career training for students and best practices for business executives

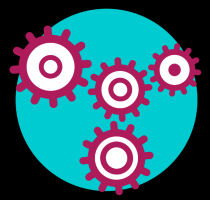
- **Cyber Simulator: develop, test, train and improve**

Cyber Threat Information Sharing

What is Cyber Threat Information?

+

+



+

Actor

who are they?

Intent

What are they trying to achieve?

Capability

What is their ability to achieve the intended goals?

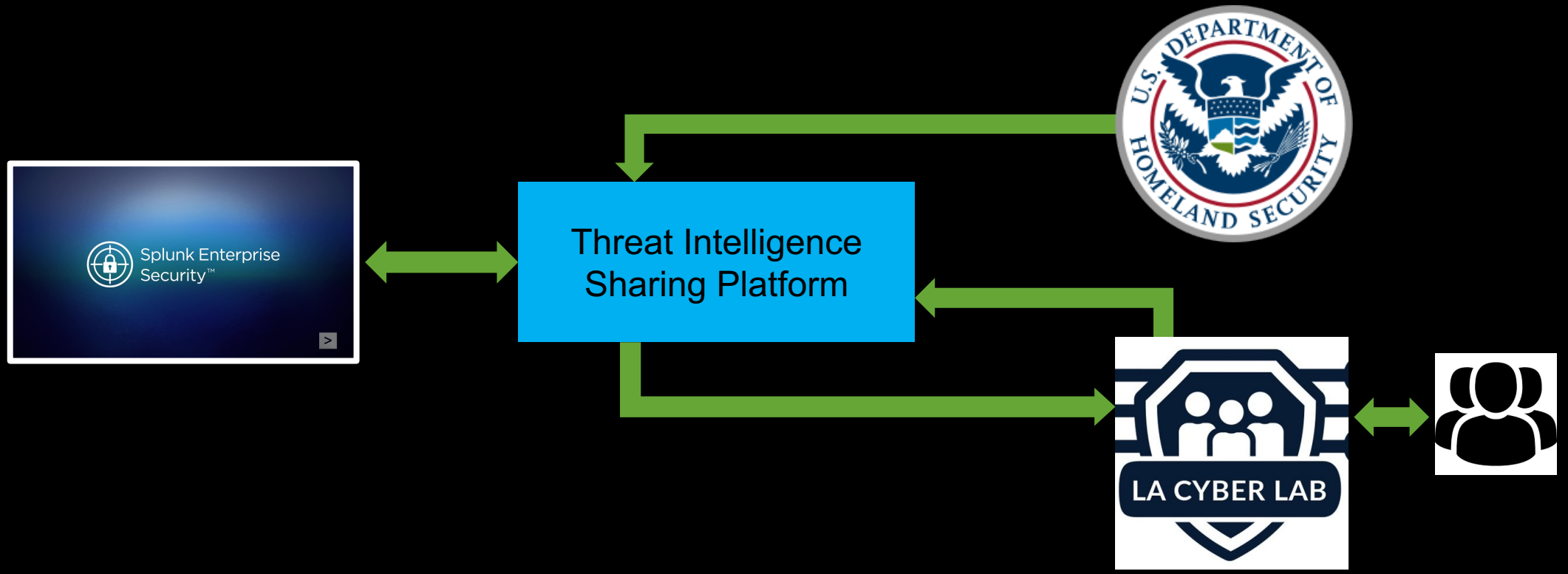
Opportunity

How much do they know about my environment and vulnerabilities?

= Threat Information

LA Cyber Lab Data Flow

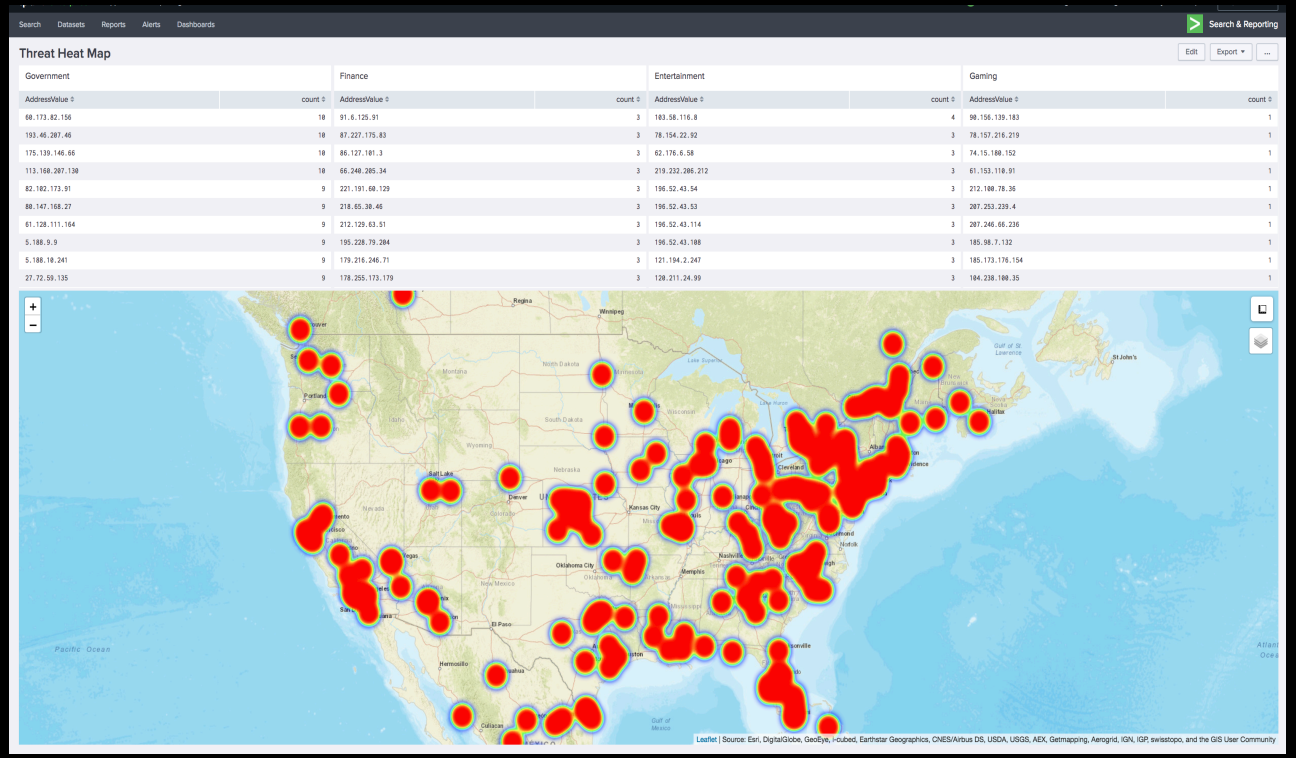
How we correlate and share threat intelligence



Use Case 1

Building a collaborative team

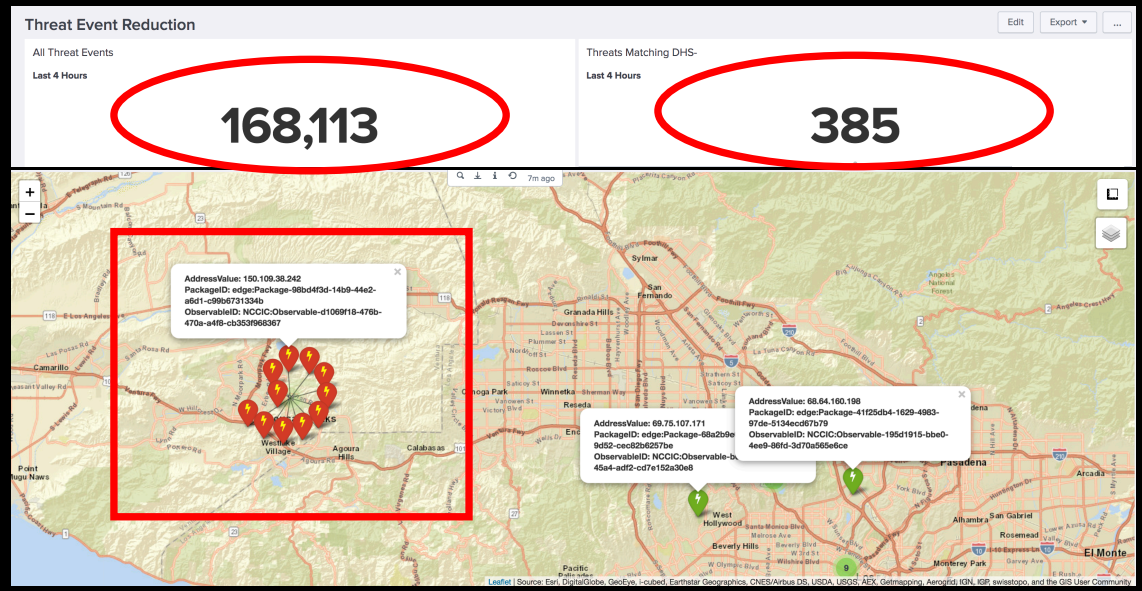
- Stronger through collaboration
- A wider set of data points around current threat activity.
- Visibility across multiple industries
  - Government
  - Finance
  - Entertainment
  - Gaming
- Identify possible threat attack patterns.
- Sharing platform for “DHS Identified” threat activity events



Use Case 2

Better focus on relevant events

- Provide reduction of events for improved incident focus.
  - Reduced from 168K events down to 385
- Identify patterns, or clusters of threat event activity.
  - 11 distinct IOCs from a single location
- Pop-up includes descriptive details of the detected threat.
- Could include location screenshot from bing maps.

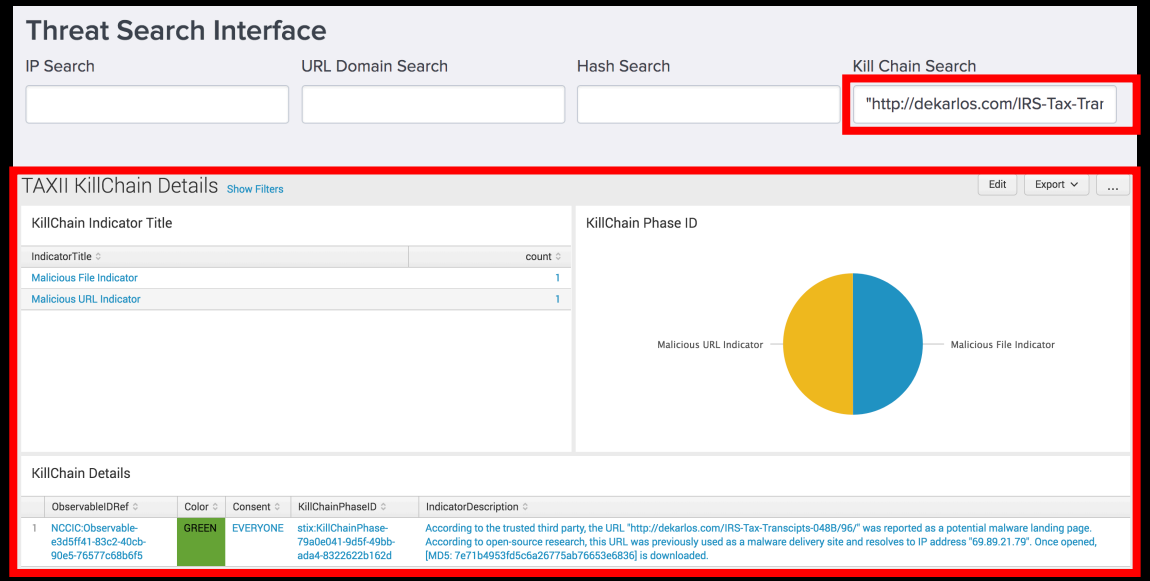


splunk> .conf18

Use Case 3

Searchable intelligence

- Currently - Prototype
  - Interactive search engine for threat lookups
- Search by key identifiers:
  - Suspected Bad IP Address
  - Suspected Bad URL
  - Suspected Host
  - KillChain
  - Free Text
- Delivers the details around the search results



splunk> .conf18

Before Splunk Enterprise Security

The challenges before Splunk Enterprise Security

The challenges:

- Threat data overload
- Quality of intelligence was low
- No platform for sharing
- No protocol for sharing
- Privacy concerns

Bringing Splunk Enterprise Security

How Splunk Enterprise Security helped solved the challenges

After Splunk Enterprise Security

A World-Class ISOC with Splunk providing

- A robust correlation and sharing platform
- Focused threat handling through event prioritization.
- Detail and share what we seeing.
- Collaborate and question what we may be missing.

What's Next?

Regional/Global
Cyber Collaboration

Prevention Focused

Cyber Alliance
(attack one
attack all)

Integrated Response

Thank You

Don't forget to rate this session in the .conf18 mobile app