Monitoring and Mitigating Insider Threat Risk With Splunk Enterprise and Splunk UBA

Ken Westin | Senior Security Strategist, Splunk
Kena Baity | Security Operations Analyst, Citrix

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

Agenda

- Insider Threat Overview
- Developing an Insider Threat Program & Governance
- Citrix Insider Threat Use Cases
- Security Essentials for Insider Threat
- Machine Learning for Insider Threat

Kena Baity

- Currently a Security Engineer at Citrix Systems, Inc.
- Citrix for 5 years but have over 15 years of Security experience.
- Started with Splunk in 2016
- Uses Splunk for Threat Hunting, Incident Response, Malware Investigations, other security use cases
- CISSP, CISA, GCIH

Ken Westin

- Senior Security Strategist
- Based in Portland
- At Splunk 3 years
- Trained in offensive and defensive security M.Sc, OSCP, ITPM
- Presented at security conferences around the world: DEF CON, Black hat, BSides etc

kwestin@splunk.com
@kwestin

BBC | Sign in | News | Sport | Weather | Shop | More

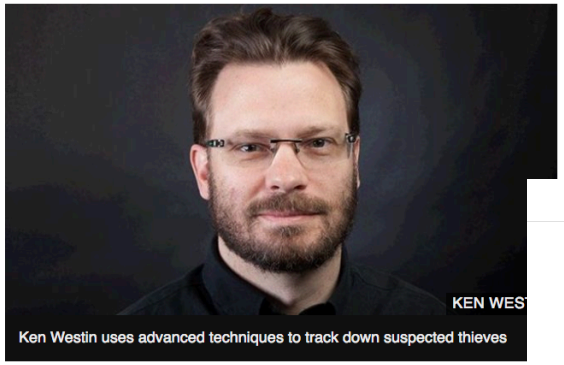
NEWS

Home | Video | World | US & Canada | UK | Business | Tech | Science | Sto

'I'm a professional cyberstalker'

Dave Lee
North America technology reporter

10 August 2015 | Share



Ken Westin uses advanced techniques to track down suspected thieves

"Stupidity is the best vulnerability. That and greed."

Ken Westin openly, and enthusiastically, calls himself a professional cyberstalker. And foolish people are his target.

He uses some of the tools that are popular with the web's creepiest patrons, hacks used to spy on webcams.

Meet the Real-Life Mr. Robot

Confessions of a professional cyber stalker.

SHARE | TWEET

J.M. Porup
Oct 20 2015, 7:04am

Photo: Ken Westin/Google Plus

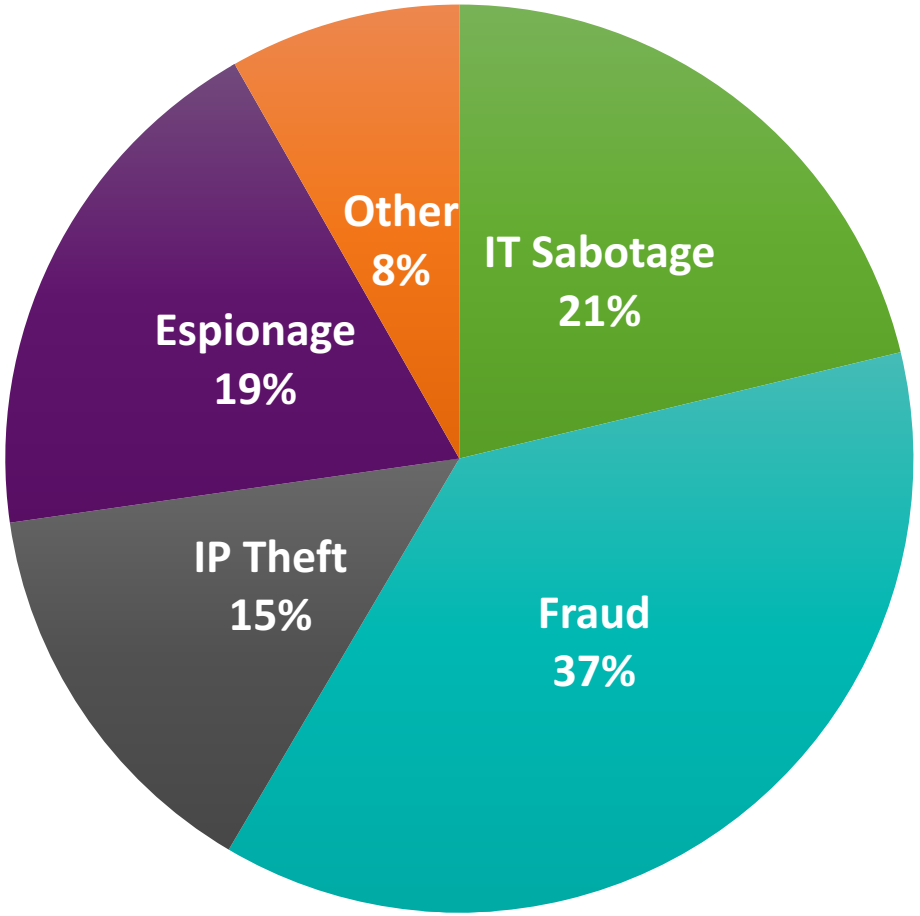
Ken Westin is an online stalker. He writes malware, tracks his targets through their devices, and uses social media to gather intel on how to break

Insider Threat Defined

An insider threat is a malicious threat to an organization that comes from people within the organization, such as employees, former employees, contractors or business associates, who have access to inside information concerning the organization' practices, data and computer systems.

Source: Intelligence-Based Security in Private Industry, Thomas A. Trier

Insider Threat: Malicious Intent



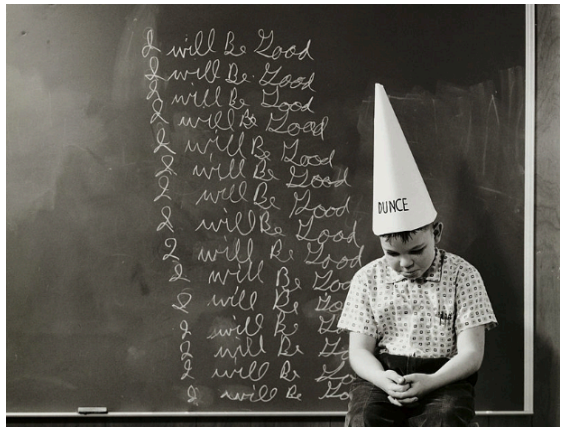
- IP Theft and IT Sabotage are usually done by short timers, or problem employees
- Fraud and Corporate Espionage are usually done over longer periods of time as users test limits of access or probing

Source: CERT Breakdown of Insider Crimes in the United States

Different Types of Insider Threat

Malicious User

Compromised User



Negligent Employees

Unintentional Insider Threat (UIT)

An unintentional insider threat is a current or former employee, contractor, or business partner who has or had authorized access to an organization's network, system, or data and who, through action or inaction without malicious intent, causes harm or substantially increases the probability of future serious harm to the confidentiality, integrity, or availability of the organization's information or information systems.

Source: Unintentional Insider Threats: A Foundational Study, CERT® Insider Threat Team
https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=58744

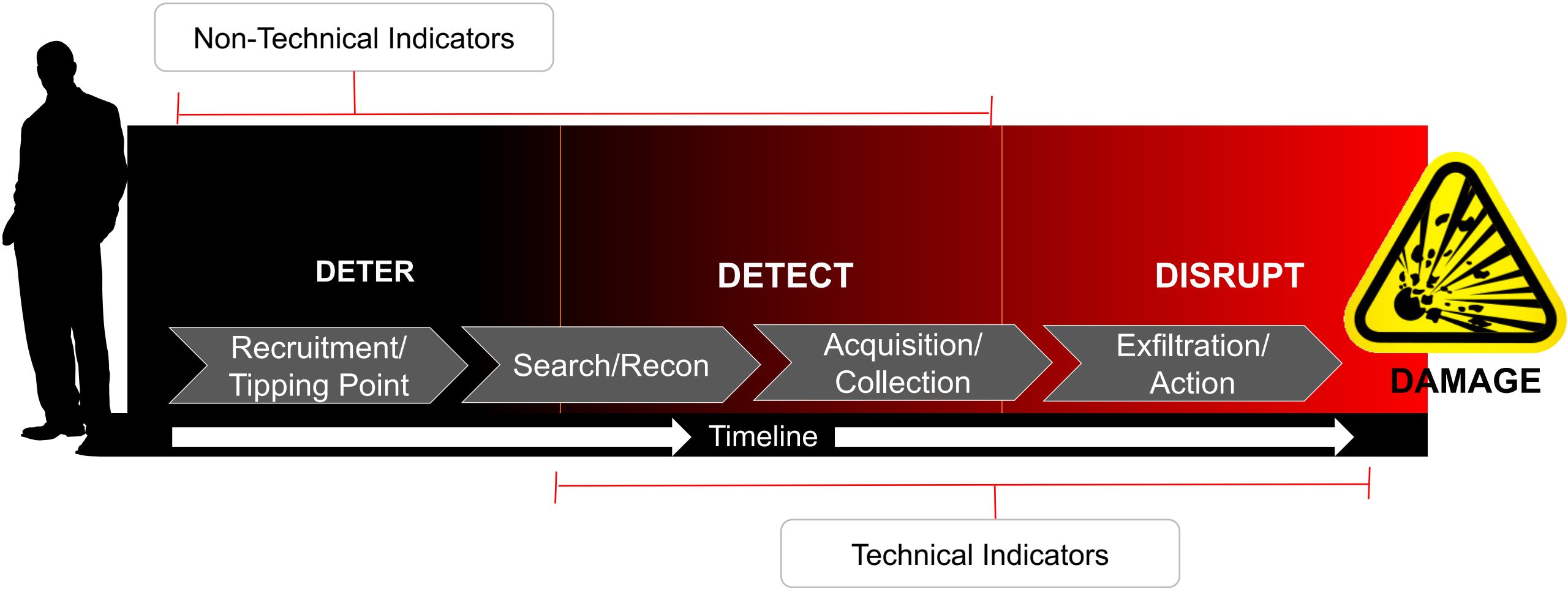
Detecting Insider Threats Is Hard

ANOMALOUS != MALICIOUS

NEED TO MONITOR MULTIPLE EVENTS

…OVER A LONG WINDOW OF TIME

Insider Threat Kill Chain



splunk> .conf18

Splunk as an Insider Threat Data Hub

Technical Data Sources

- Account Creation
- Active Directory
- Antivirus
- Application Logs
- Authentication
- Chat
- Configuration Change
- Data Loss Prevention
- DNS
- Email Logs
- File Access
- Firewall
- Help Desk Tickets
- Wireless Logs
- HTTP/SSL Proxy
- IDS/IPS
- MDM (Mobile Device Mgmt)
- Network Monitoring Logs
- Network Packet Tags
- Permission Change Monitor
- Printer/Scanner/Copier/Fax Logs
- Permission Change Monitor
- Removable Media Logs
- Telephone Records
- User Activity Monitoring
- VPN Logs

Non-Technical Data Sources

- Anonymous Reporting
- Asset Management
- AUP Violation Records
- Background Investigations
- Conflict of Interest Reporting
- Corporate Credit Card Records
- Foreign Contacts Reporting
- Performance Evaluations
- Personnel Records
- Physical Access Violations
- Security Clearance Reporting
- Travel Reporting

Real-Time Data

splunk>

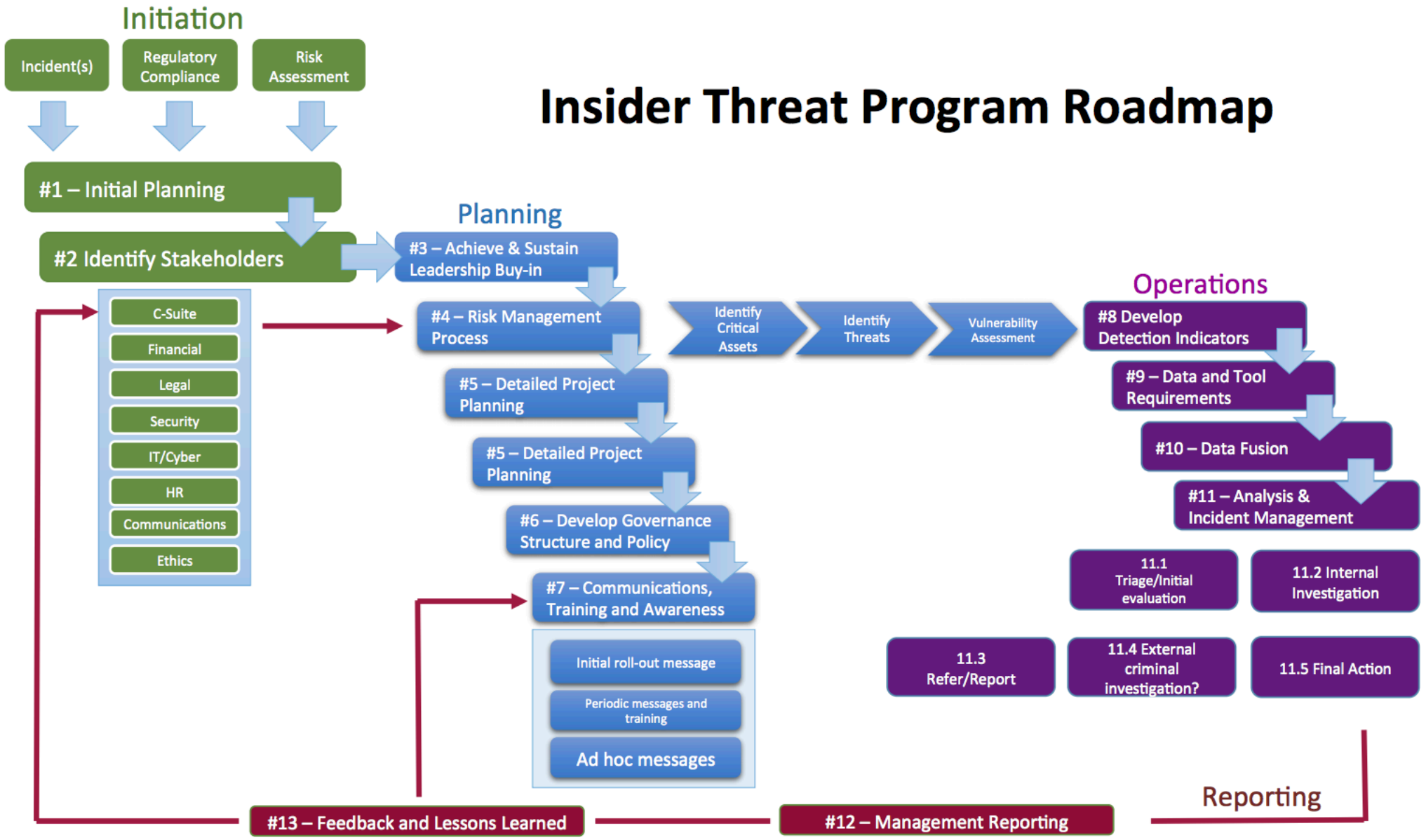
- Ad hoc search
- Monitor and alert
- Report and analyze
- Custom dashboards
- Developer Platform

- **References** – Coded fields, mappings, aliases
- **Dynamic information** – Stored in non-traditional formats
- **Environmental context** – Human maintained files, documents
- **System/application** – Available only using application request
- **Intelligence/analytics** – Indicators, anomaly, research, white/blacklist

Splunk for Insider Threat Governance

splunk> .conf18

Insider Threat Program Roadmap



Citrix Insider Risk Use Cases

splunk> .conf18

Insider Threat: Email Logs

1. Anomalies in user email behavior
   - Help identify an employee that is planning to leave the organization
2. Possible Data exfiltration
   - Due to malware or unauthorized user behavior
3. Email policy violations
   - Identifying the transfer of confidential information
4. Broken or unsafe processes

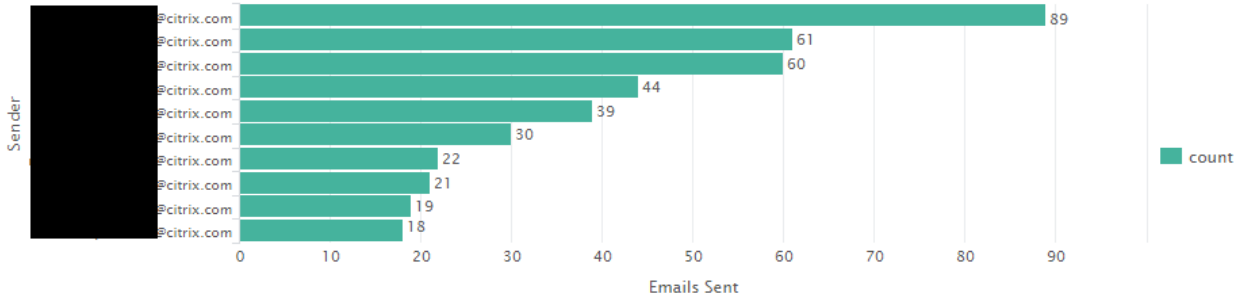
GSO - External Emails - Employees (Personal)

Edit | Export | ...

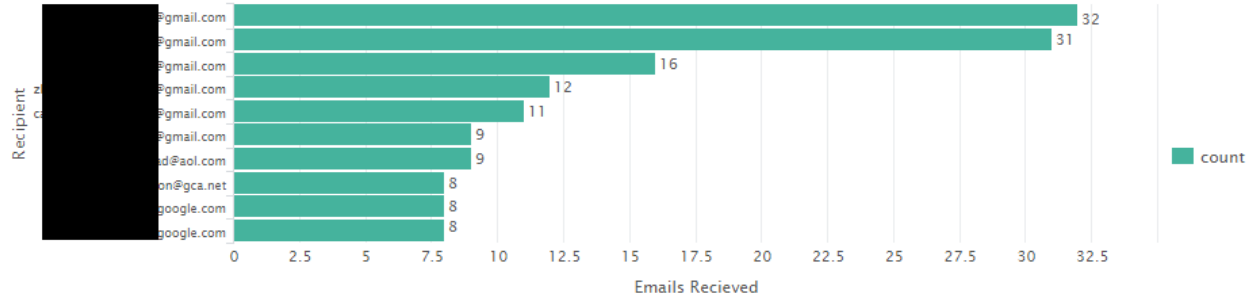
Date / Time

Last 24 hours | Submit | Hide Filters

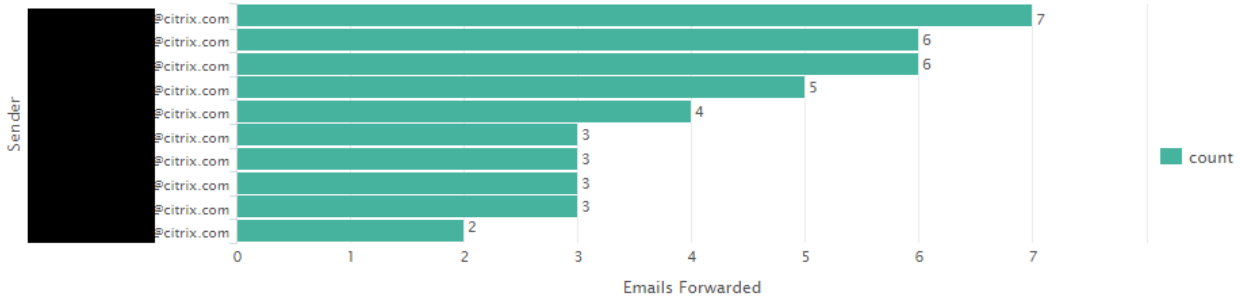
Top Senders to Personal Domains



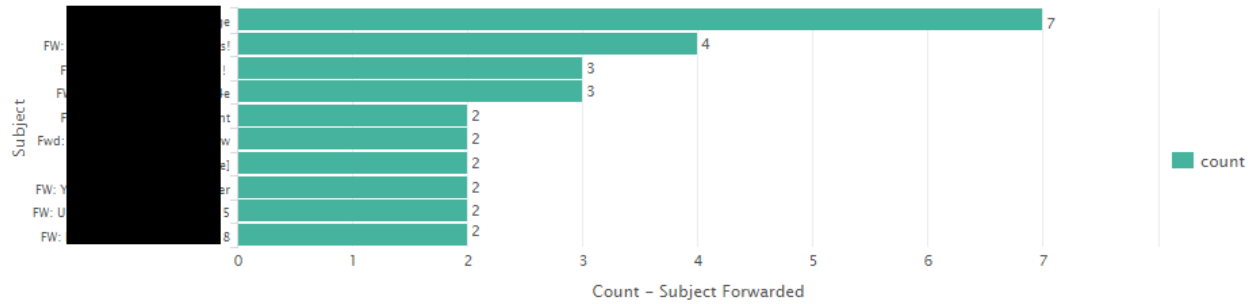
Top Recipient Personal Email Addresses



Top Users Forwarding Emails

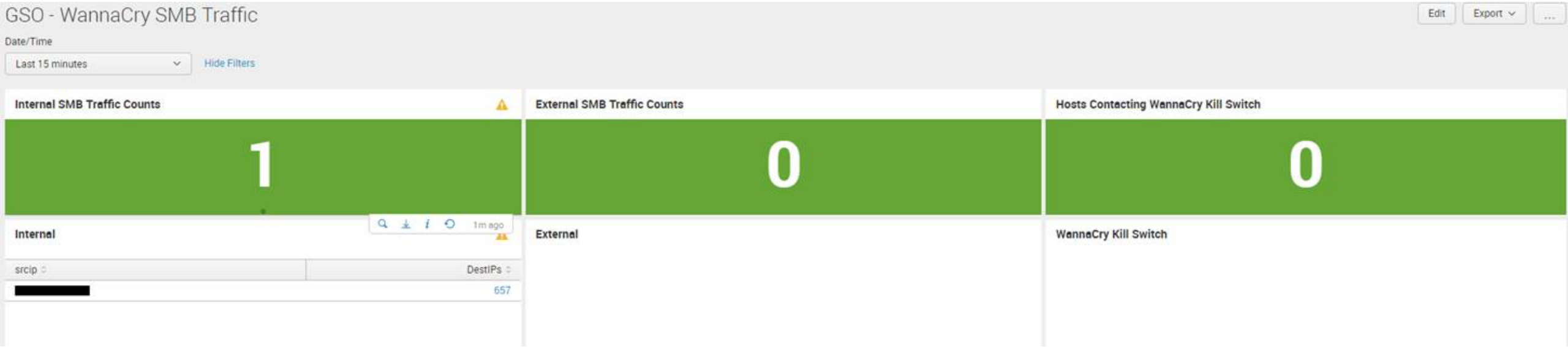


Top Forwarded Subject Lines



splunk> .conf18

Ransomware as Unintentional Insider Threat



GSO - WannaCry SMB Traffic

Edit | Export | ...

Date/Time

during Sat, Aug 12, 2017 | Hide Filters

Internal SMB Traffic Counts

16

External SMB Traffic Counts

57

Hosts Contacting WannaCry Kill Switch

67

Stopped

Internal

srcip	DestIPs
BAN 1 Qualys Scan in progress	2549
10.[redacted]	7759
10.[redacted]	6417
10.[redacted]	4931
10.[redacted]	3766
10.[redacted]	1781
10.[redacted]	2675
10.[redacted]	2445
10.[redacted]	1728
10.[redacted]	1827
10.[redacted]	1747
10.[redacted]	2313
10.[redacted]	3318
FLL 1 Qualys Scan in progress	201622
AMS 1 Qualys Scan in progress	62034
10.[redacted]	4608

External

srcip	vd	DestIPs
10.[redacted]	sin1_ent1	16509
10.[redacted]	SJC1_Lab	445
10.[redacted]	SJC1_Lab	461
10.[redacted]	SJC1_Lab	344
10.[redacted]	ams1_ent1	15777
10.[redacted]	ams1_ent1	15958
10.[redacted]	ams1_ent1	16072
10.[redacted]	ams1_ent1	15958
10.[redacted]	ams1_ent1	8711
10.[redacted]	ams1_ent1	16277
10.[redacted]	ams1_ent1	16024
10.[redacted]	ams1_ent1	16228
10.[redacted]	ams1_ent1	16053
10.[redacted]	ams1_ent1	10707
10.[redacted]	ams1_ent1	10624
10.[redacted]	ams1_ent1	10777

WannaCry Kill Switch

srcip	dstip
10.[redacted]	104.17.38.137
10.[redacted]	104.17.40.137
10.[redacted]	104.17.37.137
10.[redacted]	104.17.38.137
10.[redacted]	104.17.41.137
10.[redacted]	104.17.39.137
10.[redacted]	104.17.41.137
10.[redacted]	104.17.40.137
10.[redacted]	104.17.41.137
10.[redacted]	104.17.37.137
10.[redacted]	104.17.38.137
10.[redacted]	104.17.38.137
10.[redacted]	104.17.40.137
10.[redacted]	104.17.38.137
10.[redacted]	104.17.41.137
10.[redacted]	104.17.39.137

splunk> .conf18

Splunk Security Essentials

splunk> .conf18

Splunk Security Essentials for Insider Threat

Insider Threat

Featuring 104 Examples!

Insider threats come from current or former employees, contractors, or partners who have access to the corporate network and intentionally or accidentally exfiltrate, misuse or destroy sensitive data. They often have legitimate access to access and download sensitive material, easily evading traditional security products. Nothing to fear, Splunk can also help here.

Security Content / User with Increase in Outgoing Email

Assistant: Detect Spikes

Export ...

Description

Both to detect data exfiltration and compromised account, we can analyze users that are sending out dramatically more data than normal. This search looks per source email address for big increases in volume.

Learn how to use this page

View: Demo Data | Live Data

Use Case Advanced Threat Detection, Insider Threat **Category** Data Exfiltration, Endpoint Compromise, SaaS **Alert Volume** Low (?) **SPL Difficulty** Hard	**Stage 3** **MITRE ATT&CK Tactics** Exfiltration **Kill Chain Phases** Actions on Objective **Data Sources** Email

- Related Splunk Capabilities
- How to Implement
- Known False Positives
- How To Respond
- Show Search
- Help

DEMO DATA You're looking at the *Demo* search right now. Did you know that we have 2 searches for this example? **Scroll Up** to the top to see the other searches.

Outlier(s)

2

Outlier(s)

Total Result(s)

231

Total Result(s)

Raw Event(s)

3,327

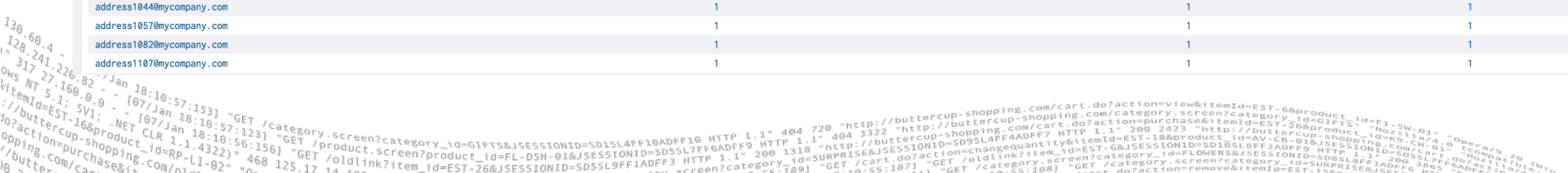
Raw Event(s)

Outliers Only

Sender	num_data_samples	count	avg	lowerBound	upperBound	isOutlier
address20@mycompany.com	23	102	10.285714285714286	-10.072506237139445	30.643934808568020	1
address89@mycompany.com	31	68	20.24137931034483	-9.48910130858416	49.97185992927382	1

All Data

Sender	num_data_samples	count	avg	lowerBound	upperBound
address20@mycompany.com	23	102	10.285714285714286	-10.072506237139445	30.643934808568020
address89@mycompany.com	31	68	20.24137931034483	-9.48910130858416	49.97185992927382
address103@mycompany.com	1		1	1	1
address1044@mycompany.com	1		1	1	1
address1057@mycompany.com	1		1	1	1
address1082@mycompany.com	1		1	1	1
address1107@mycompany.com	1		1	1	1



splunk> .conf18

Security Content / Flight Risk Emailing

Export ▾ ...

Assistant: Simple Search

Description

This search implements several heuristics to look for indications that a user is a flight risk. While most savvy employees will use a personal email address when emailing competitors, everyone in Security has some story of employees who don't, as it will happen. Detect when it does.

Learn how to use this page

View Demo Data | Live Data

Use Case

Insider Threat

Category

Insider Threat

Security Impact

Detecting users who are about to leave, before they actually give notice, can provide you the opportunity to potentially fix the situation for an unhappy employee, but also can help you prevent the exfiltration of sensitive data (which usually happens before an employee actually gives notice). Look for the indications that an employee may be leaving, by checking email logs.

Alert Volume

Medium (?)

SPL Difficulty

Medium

Stage 4

Data Sources

Email

Demo SPL for Flight Risk Emailing

```
| `Load_Sample_Log_Data("Email Logs")` | search
Sender=*@mycompany.com Recipient!=*@mycompany.com
```

```
// First we start by pulling our demo email logs, and filter
for outbound emails.
```

```
| lookup UC_raw_data_for_privilege_calculations mail as
Sender OUTPUT firstname lastname
```

```
// In order to understand if a user's name is in the
filename, we need to know what a user's name is. Lets look up
this data in LDAP output from the ldapsearch app, detailed in
the "Pull List of Privileged Users" example.
```

```
| eval hasNameInAttachment=case(like(lower(file_name), "%" .
lower(firstname) . "%"), 1, like(lower(file_name), "%" .
lower(lastname) . "%"), 1,like(lower(file_name), "%" .
lower(substr(firstname, 1, 1) . lastname) . "%"), 1, 1=1, 0)
```

```
// Now we use the first name and last name to look up
different incarnations in the attachment, storing the result
(1 or 0) in a field called hasNameInAttachment. (Why not
filter directly? We want to be able to make a big search in
the next line, and while you could do that with | where all
in one.. most people would prefer not to.) We're looking for
first name, or last name, or first initial + last name, so we
would get resume_jane.pdf and smith_resume.pdf and
jsmith.docx.
```

```
| search hasNameInAttachment=1 OR file_name=*resume* OR
(Recipient=careers@* OR Recipient=recruiting@* OR
Recipient=jobs*)
```

```
// Now we actually do the search. We look to see if the
filename is in the attachment, we look to see if the
recipient looks like a third party careers address, and we
look to see if there is a resume attached.
```

```
| bucket _time span=1d
```

```
// The bucket command flattens the timestamps so we can
easily see how many days we saw this behavior on.
```

Stage 1: Collection

You have the data onboard, what do you do first?

Flight Risk Web Browsing

This search implements several heuristics to look for indications that a user is a flight risk from Web Logs. Detect a user who may be leaving before they do.

Recommended
Searches Included
Web Proxy

Increase in Pages Printed

Find users who printed more pages than normal.

Recommended
Searches Included
Print Server Logs

Large Web Upload

Uses a basic threshold to detect a large web upload, which could be exfiltration from malware or a malicious insider.

Recommended
Searches Included
Web Proxy

Sources Sending a High Volume of DNS Traffic

A common method of data exfiltration is to send out a huge volume (in bytes) of DNS or ping requests, embedding data into the payload. This is often not logged.

Recommended
Searches Included
Network Communication

User Login with Local Credentials

Categorically, most interactive logins should use domain credentials. Detect when a new user logs on with local credentials that bypass most centralized logging and policy systems, but not Splunk!

Recommended
Searches Included

Detect Many Unauthorized Access Attempts

Most login failures are due to failed passwords. Login failure to sensitive systems where the users simply aren't authorized, though, can indicate malicious intent. Detect that.

Searches Included
Windows Security
Authentication

First Time USB Usage

Find systems the first time they generate Windows Event ID 20001, which for some customers occurs when a USB drive is plugged in.

Searches Included
Endpoint Detection and Response
DLP

Flight Risk Printing

This search implements two heuristics to look for indications that a user is a flight risk. Many people will print offer letters, drafts of their resume, or related docs on the work environment (for convenience, or because they don't have a printer at home). Detect when that happens.

Searches Included

Personally Identifiable Information Detected

Detects personally identifiable information (PII) in log files. Some software can inadvertently provide sensitive information in log files, resulting in potential exposure to those reviewing the log files.

Try Splunk ES
Any Host Logs

Potential Day Trading

Detect users who exhibit a large amount of stock trading activity in their proxy logs.

Searches Included
Web Proxy

Sources Sending Many DNS Requests

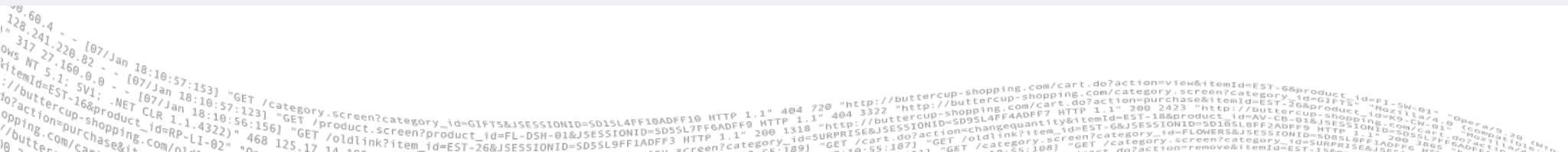
A common method for Data Exfiltration is to send out many DNS or Ping requests, embedding data into the payload. This is often not logged.

Searches Included
Network Communication

Web Browsing to Unauthorized Sites

Detect users who are persistently attempting to violate your proxy policy.

Searches Included
Web Proxy



splunk> .conf18

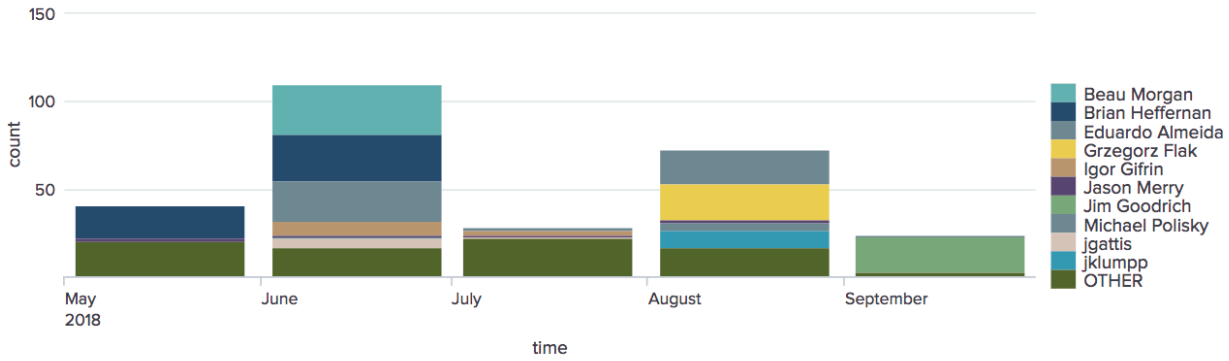
Splunk Enterprise Security

splunk> .conf18

Incident Review Audit

Export ▾ ...

Review Activity By Reviewer

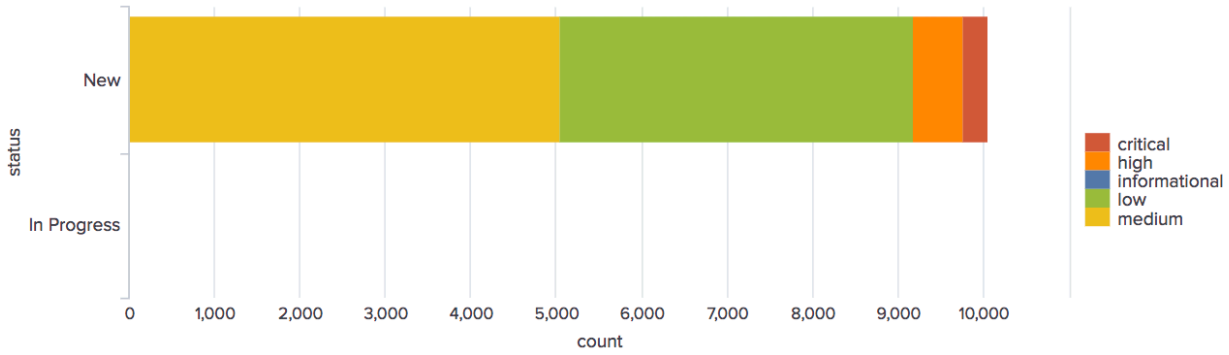


Top Reviewers

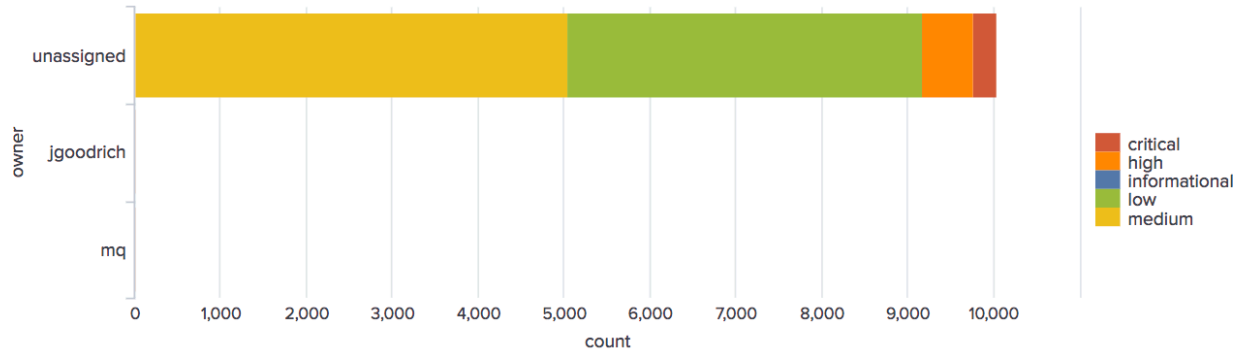
reviewer_realname	sparkline	count	firstTime	lastTime
Brian Heffernan		46	05/14/2018 19:08:44	06/04/2018 20:24:08
Eduardo Almeida		45	06/20/2018 19:13:43	09/04/2018 15:04:32
Beau Morgan		28	06/28/2018 14:41:40	06/28/2018 14:41:40
Grzegorz Flak		20	08/28/2018 09:02:54	08/28/2018 09:02:54
Jim Goodrich		20	09/07/2018 16:38:58	09/07/2018 16:38:58
Igor Gifrin		11	06/22/2018 05:14:14	07/12/2018 19:24:39
jklumpp		10	08/01/2018 10:56:22	08/10/2018 19:35:20
Jason Merry		6	05/18/2018 13:32:41	08/02/2018 13:41:36
jgattis		6	06/05/2018 18:13:00	07/11/2018 18:19:33
Michael Polisky		5	06/22/2018 16:10:41	08/20/2018 17:49:58

« prev 1 2 3 4 5 6 next »

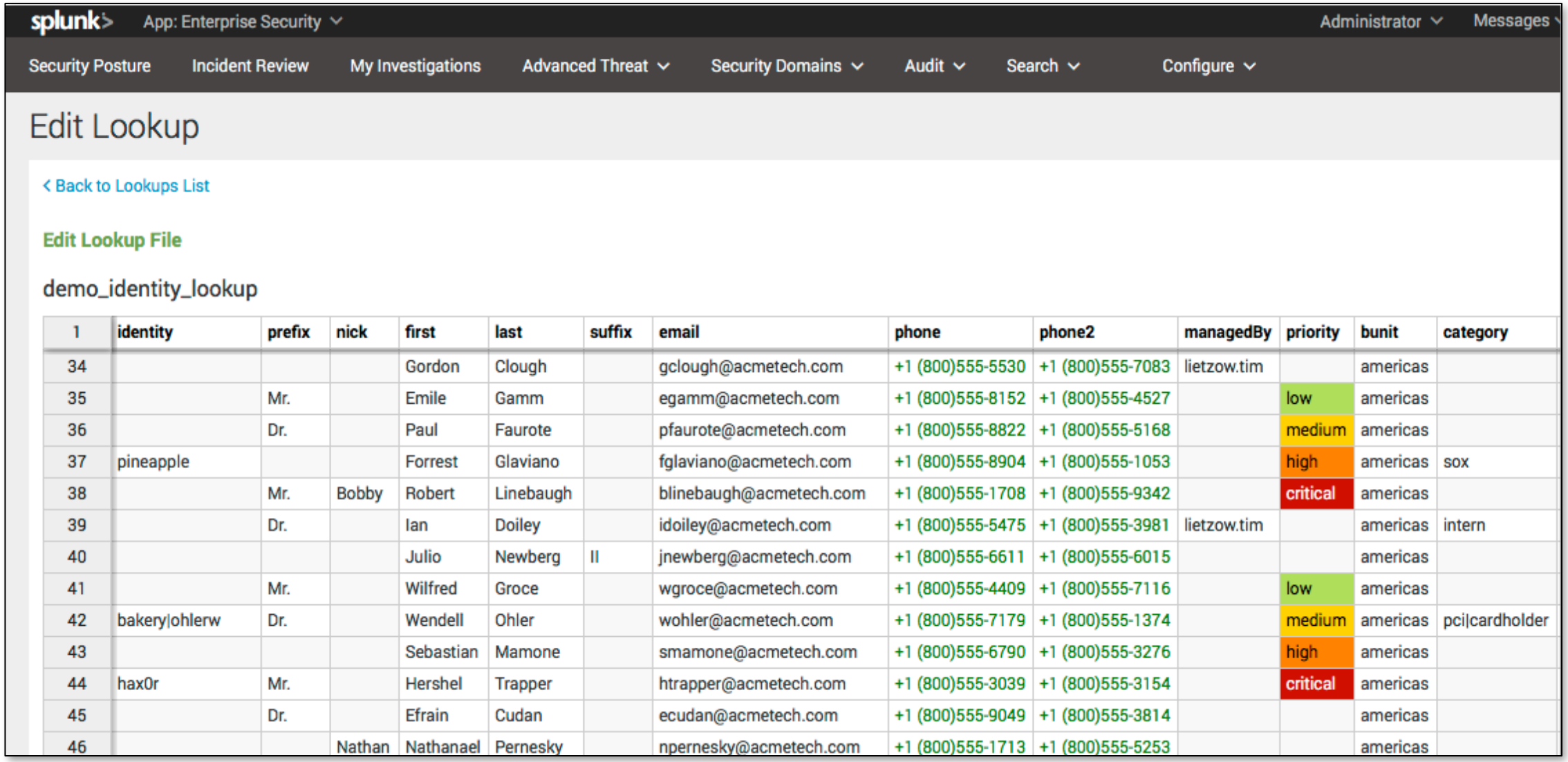
Notable Events By Status - Last 48 Hours



Notable Events By Owner - Last 48 Hours

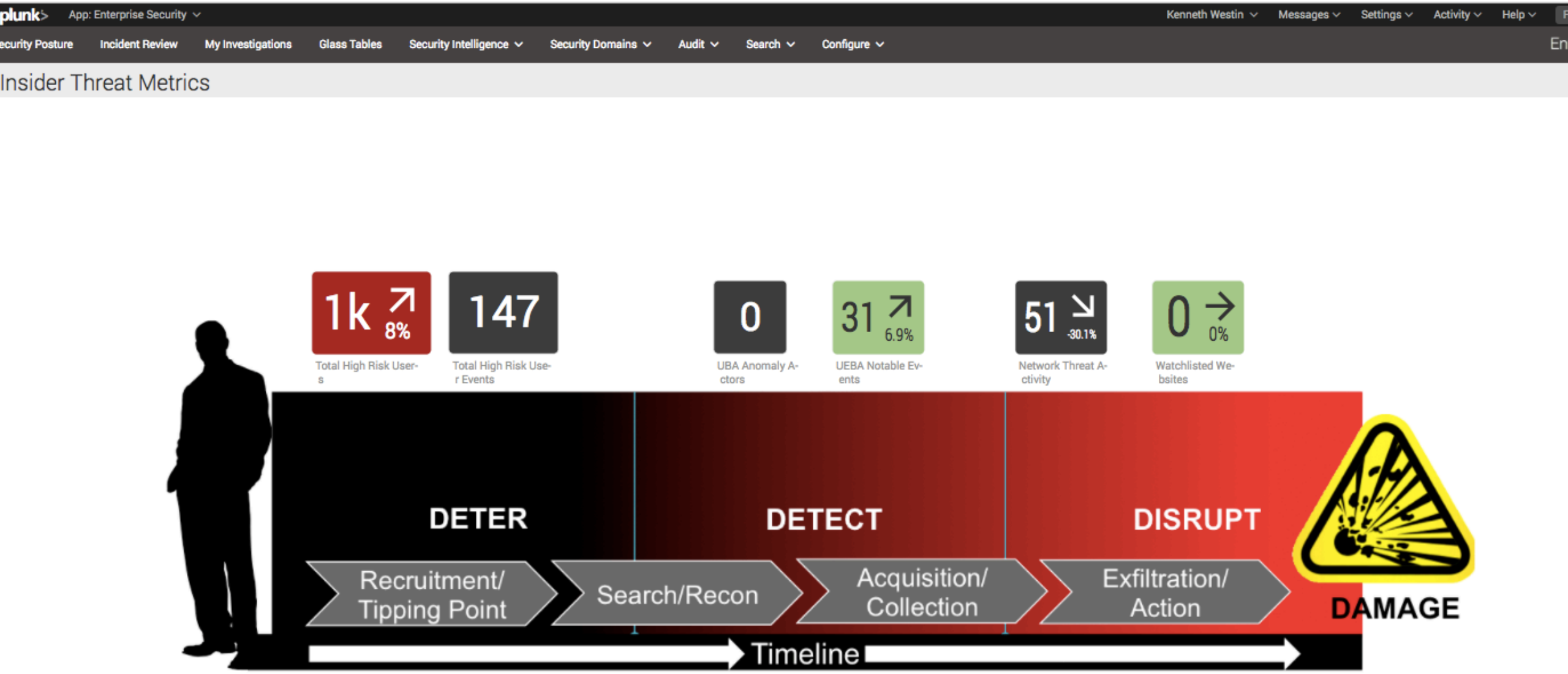


Asset and Identity Correlation



1	identity	prefix	nick	first	last	suffix	email	phone	phone2	managedBy	priority	bunit	category
34				Gordon	Clough		gclough@acmetech.com	+1 (800)555-5530	+1 (800)555-7083	lietzow.tim		americas	
35		Mr.		Emile	Gamm		egamm@acmetech.com	+1 (800)555-8152	+1 (800)555-4527		low	americas	
36		Dr.		Paul	Faurote		pfaurote@acmetech.com	+1 (800)555-8822	+1 (800)555-5168		medium	americas	
37	pineapple			Forrest	Glaviano		fglaviano@acmetech.com	+1 (800)555-8904	+1 (800)555-1053		high	americas	sox
38		Mr.	Bobby	Robert	Linebaugh		blinebaugh@acmetech.com	+1 (800)555-1708	+1 (800)555-9342		critical	americas	
39		Dr.		Ian	Doiley		idoiley@acmetech.com	+1 (800)555-5475	+1 (800)555-3981	lietzow.tim		americas	intern
40				Julio	Newberg	II	jnewberg@acmetech.com	+1 (800)555-6611	+1 (800)555-6015			americas	
41		Mr.		Wilfred	Groce		wgroce@acmetech.com	+1 (800)555-4409	+1 (800)555-7116		low	americas	
42	bakery|ohlerw	Dr.		Wendell	Ohler		wohler@acmetech.com	+1 (800)555-7179	+1 (800)555-1374		medium	americas	pci|cardholder
43				Sebastian	Mamone		smamone@acmetech.com	+1 (800)555-6790	+1 (800)555-3276		high	americas	
44	hax0r	Mr.		Hershel	Trapper		htrapper@acmetech.com	+1 (800)555-3039	+1 (800)555-3154		critical	americas	
45		Dr.		Efrain	Cudan		ecudan@acmetech.com	+1 (800)555-9049	+1 (800)555-3814			americas	
46			Nathan	Nathanael	Pernesky		npernesky@acmetech.com	+1 (800)555-1713	+1 (800)555-5253			americas	

Enterprise Security Insider Threat Glass Table



Machine Learning for Insider Threat

splunk> .conf18

Evolution of Security Correlation, Advanced Analytics & ML

Complexity

Splunk User Behavior Analytics™

N-Dimensional Advanced – Data Science

- Shift from heavy manual tagging and rule building alone,
- Machine learning and data science for UEBA
- Enhances analyst capabilities to identify **unknown** threats
- Monitor and measure aggregated risk of users and assets

Splunk Enterprise Security™

Multi-Dimensional – Analytics

- Hybrid model developed as adversaries circumvent basic correlation
- Goal to reduce false positives
- Thresholds and combinations of rules developed.
- Behavioral models, statistics and patterns not signatures alone

splunk> essentials for Security

Two-Dimensional – Correlation

- Regex/pattern-matching for strings
- Used in anti-malware, IDS/IPS, DLP and basic/legacy SIEM
- Use of string matching to search a binary file to identify type of threat
- Enhanced capability to identify **previously known** threats and host enumeration

One-Dimensional – Correlation

- Fast and efficient basic matching e.g.. domains IP addresses, user-agent, MD5 file hashes
- Boolean operators to identify if signature is on a black/white list.
- Common usage in most firewall and IDS tools

Data Volume & Velocity

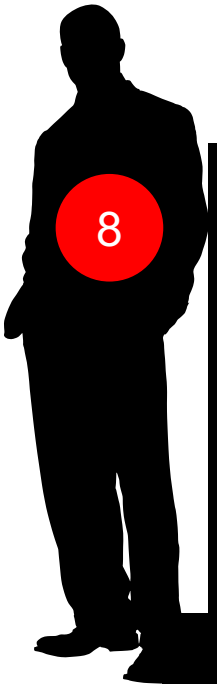
splunk> .conf18

Insider Threat Kill Chain: Sequencing

1. User added to watchlist
2. User attempts to access new business application
3. User accesses high volume of job sites during work hours
4. User accesses critical file share
5. User copies files to USB flash drive

1 Month

Non-Technical Indicators



DETER

DETECT

DISRUPT

Recruitment/ Tipping Point

Search/Recon

Acquisition/ Collection

Exfiltration/ Action

DAMAGE

Timeline

Technical Indicators

splunk> .conf18

Insider: Suspicious Behavior

There are signs of unusual user activity by user Pablo Ramirez

Multiple instances of unusual internal (intranet) user activity that could be a sign that this is a rogue user

Watchlists

TIMELINE

Start Date
5
May, 2016

Last Update
19
May, 2016

Duration
14d

ANOMALIES (3)

- Blacklisted IP Address (1) — 9
- Domain Name Anomaly (1) — 9
- Unusual Geolocation of Communication Destination (1) — 9

USERS (1)

- Pablo Ramirez — 9

DEVICES (4)

Internal

- 10.229.243.213 — 9
- 10.50.10.5 — 9

External

- 37.53.69.177 — 9
- 53.123.1.12 — 9

DOMAINS (2)

- www.nxavanullotn10k67fvp42.net
- www.orrswuwbumwcbypceofnjsg.co.jp

Types of Fancy Machine Learnin’

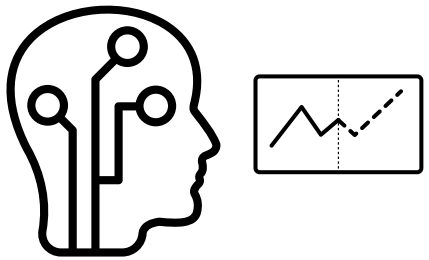
Supervised Machine Learning

Requires labeled data and requires care and feeding to teach the model so it identifies relationship between a known set of outputs and their related inputs. Once established it is used to predict output for a new set of inputs.

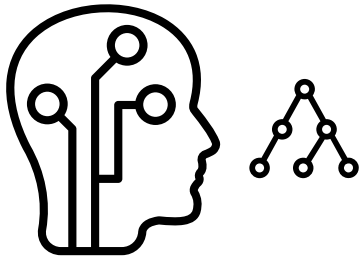
Unsupervised Machine Learning

Requires no prior training of models, analyzes sets of data and identifies groups with similar attributes and establishes baselines that identify anomalous behavior.

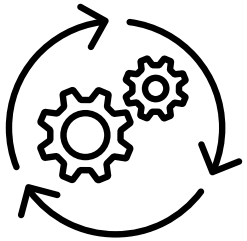
Machine Learning for UEBA



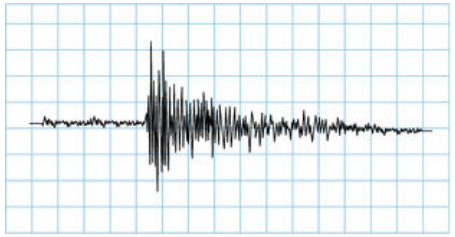
Supervised Machine Learning



Unsupervised Machine Learning



Model



Baseline

Use Cases, Models, Kill Chains & Data Sources

Use Case	Kill Chain	Model Types	Detection	Training Data	Data Sources
Abnormal Server Access	Lateral Movement	K Means	Anomaly (unknown threat)	Unlabeled (Unsupervised)	Active Directory Windows Logs
Malicious Download	Command & Control, Infection	Naïve Bayes, Logistic Regression	Maliciousness (Known Threat)	Labeled (Supervised)	Email Logs Windows Logs Anti-Malware

Mapping Anomalies to Data Sources in Splunk UBA

Anomaly	UBA Model	Type of Model	Data Source	Fields	Model Readiness
Suspicious Network Exploration	User Info Exploration	Batch	Windows Event Log	EventId, Target Entity Id, Source Entity Id, Event Time	7 Days
Unusual USB Activity	USB Activity	Batch	Client Data	Client IP, username, operation, target info	7 Days
Suspicious Account Activity	Feature-Based Peer Grouping	Batch	Multiple	Multiple	7 Days

Connecting Insider Threat Dots With Machine Learning

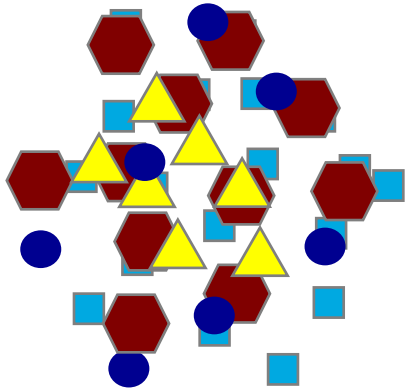
RAW SECURITY EVENTS

ANOMALIES

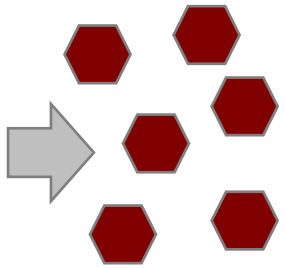
Anomalies graph
Entity relationship graph

ANOMALY CHAINS (THREATS)

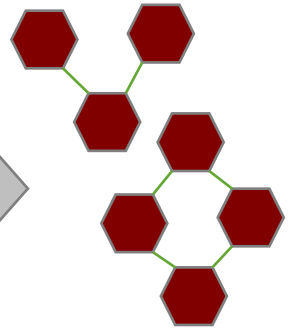
Lateral Movement
Beaconing
Land-Speed Violation



MACHINE LEARNING



GRAPH MINING



THREAT MODELS

Kill chain sequence
Forensic artifacts
Threat/Risk scoring

VISUALIZATION & ANALYTICS

FEEDBACK

Insider: Suspicious Behavior

There are signs of unusual user activity by user Pablo Ramirez

Multiple instances of unusual internal (intranet) user activity that could be a sign that this is a rogue user

Watchlists

TIMELINE

Start Date
5
May, 2016

Last Update
19
May, 2016

Duration
14d

ANOMALIES (3)

- Blacklisted IP Address (1) — 9
- Domain Name Anomaly (1) — 9
- Unusual Geolocation of Communication Destination (1) — 9

USERS (1)

- Pablo Ramirez — 9

DEVICES (4)

Internal

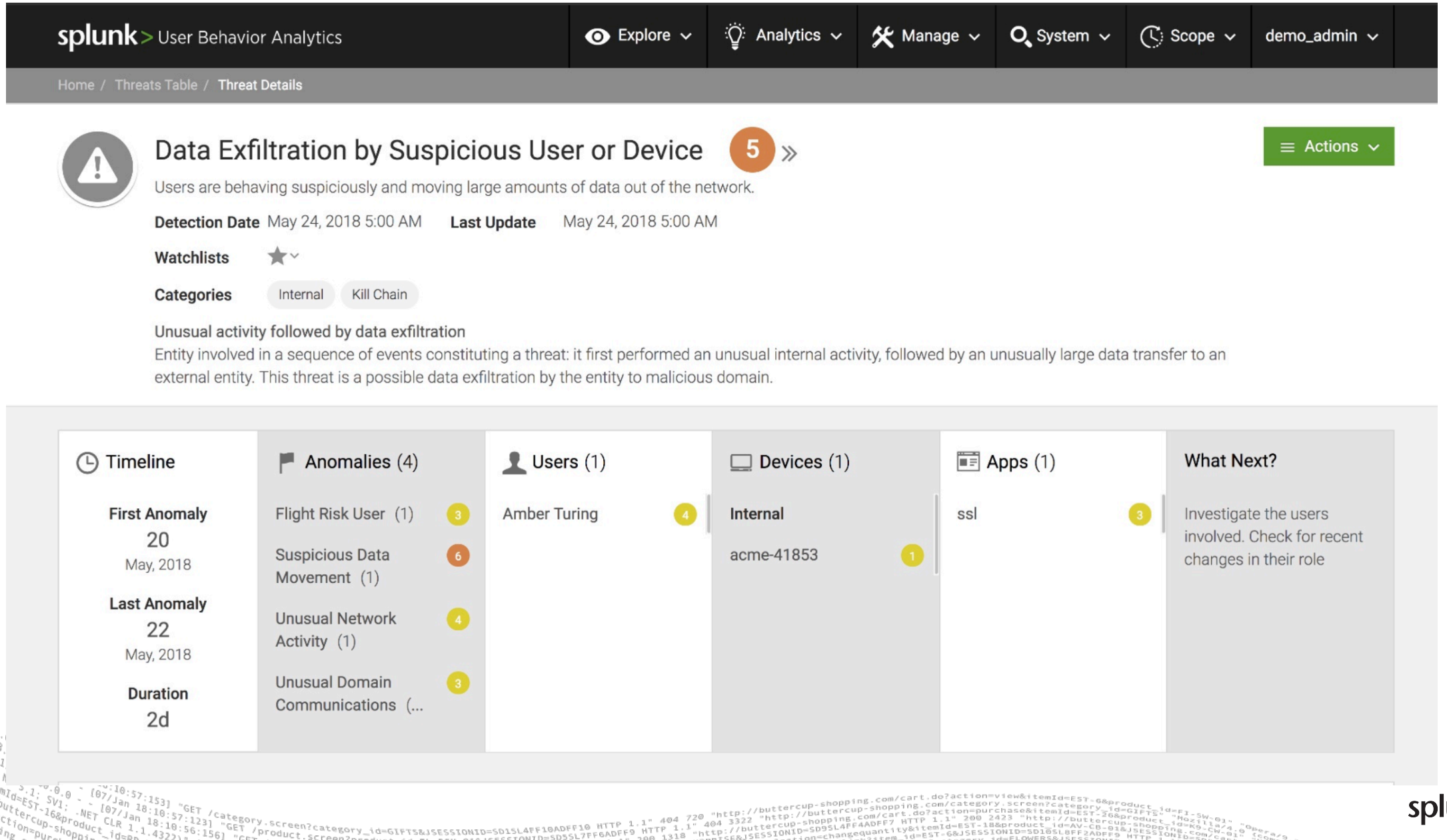
- 10.229.243.213 — 9
- 10.50.10.5 — 9

External

- 37.53.69.177 — 9
- 53.123.1.12 — 9

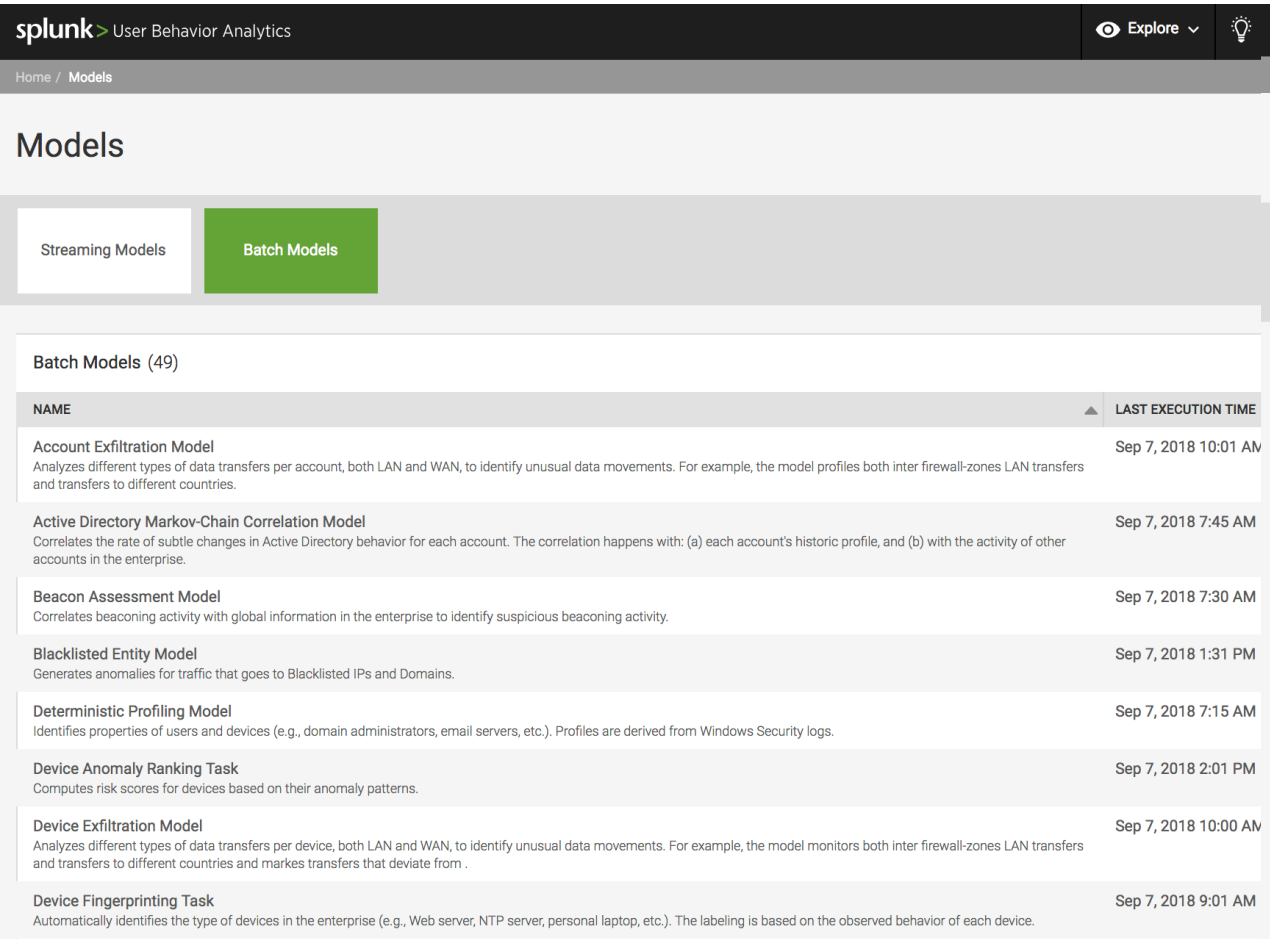
DOMAINS (2)

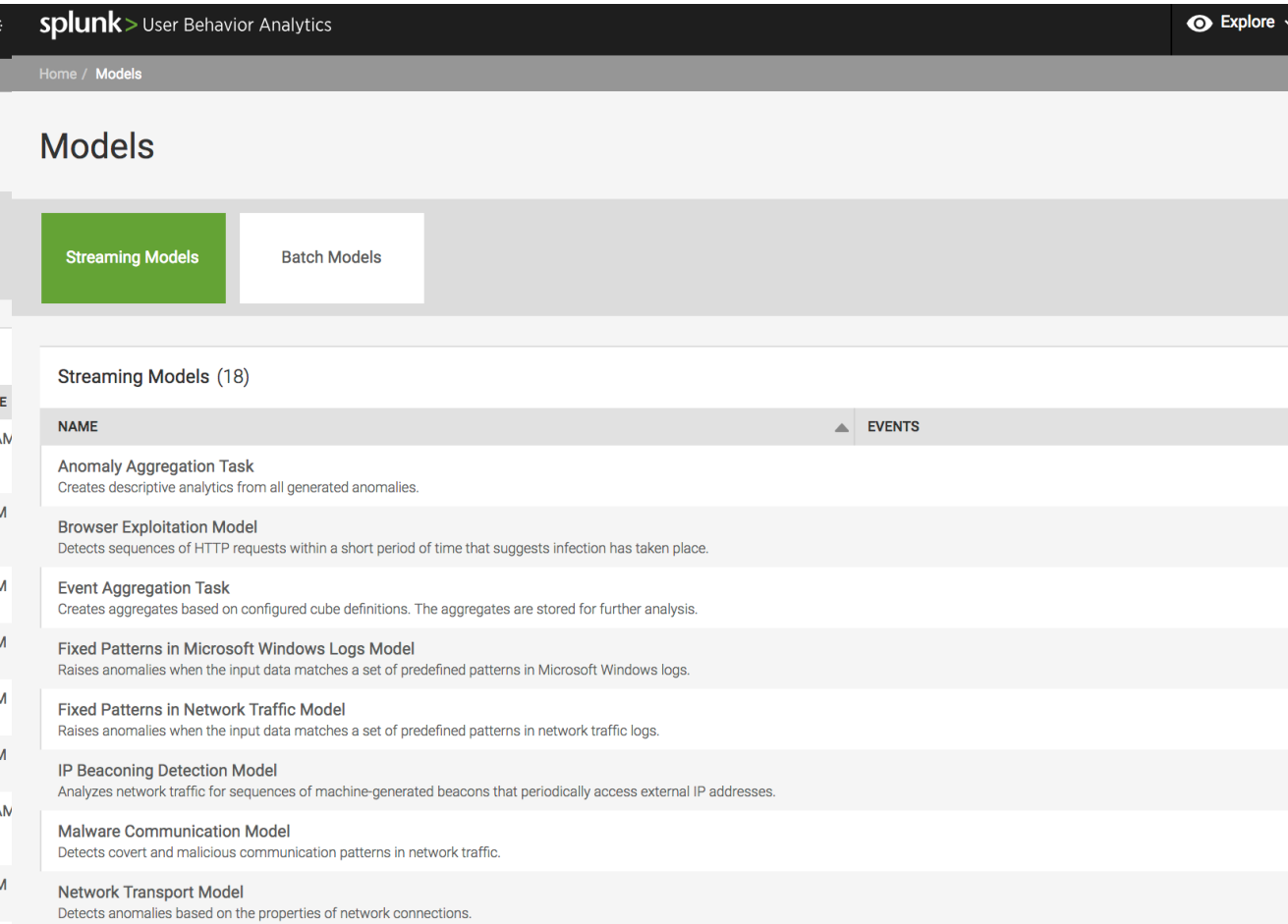
- www.nxavanullotn10k67fvp42.net
- www.orrswuwbumwcbypceofnjsg.co.jp



splunk> .conf18

49 Batch Models and 18 Streaming Models





splunk> .conf18

Specialist Workshops

- **Insider Threat Assessment and Hands-On Workshop**
- **Fraud Workshop**

kwestin@splunk.com

splunk> .conf18

Thank You!

splunk> .conf18