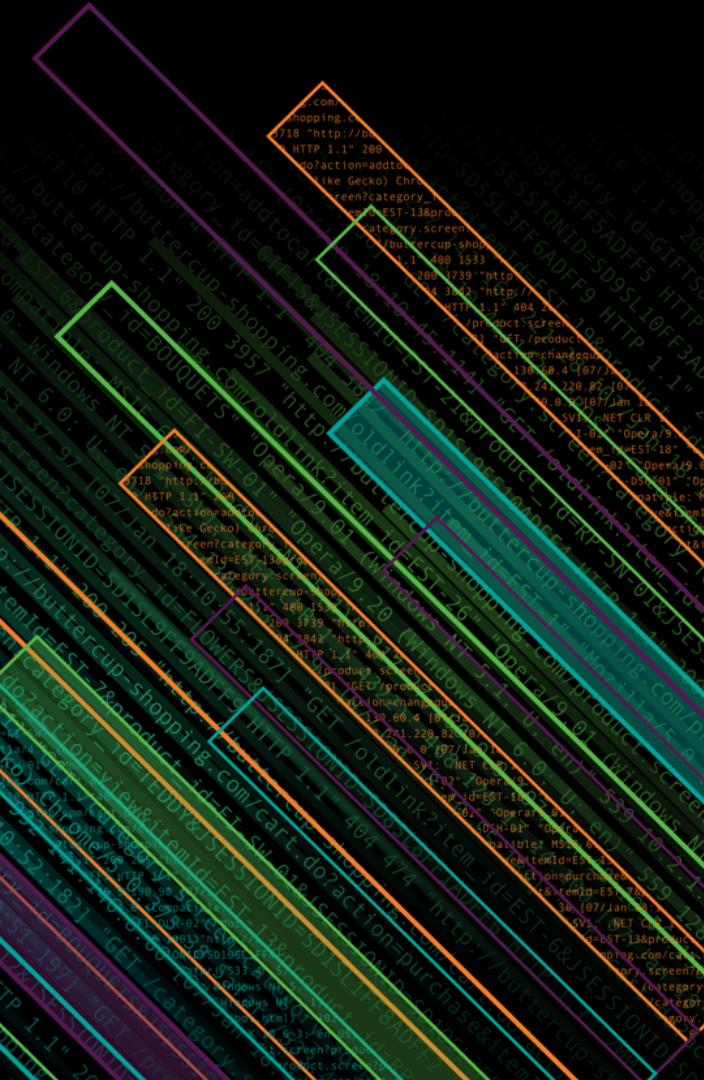




splunk>

Addressing Alert Fatigue

David Dorsey | Sr. Manager Security Research



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. © 2018 Splunk Inc. All rights reserved.

Who's This Guy?

- ▶ A coy 'lil security minx
- ▶ Splunk Security Research Team
- ▶ Been around for 15ish years now, mainly on the defensive side
- ▶ RE, IR, File Analysis, Network Analysis, Machine Learning
- ▶ Loves
 - BBQ
 - Pie
- ▶ Dislikes
 - Pants
 - Socks

Level Setting

Words matter



Alert Fatigue

Occurs when one is exposed to a **large number of frequent alerts** and consequently becomes desensitized to them.

Desensitization can lead to longer response times or to missing important alarms.

Alerts Should Provide Value

i	Time	Security Domain	Title	Urgency	Status	Owner	Actions
>	28/18 9:54:05.000 PM	Endpoint	Registry Key Associated With Persistence Modified on winterfell	Low	New	unassigned	▼
>	8/28/18 9:54:05.000 PM	Endpoint	Registry Key Associated With Persistence Modified on winterfell	Low	New	unassigned	▼
>	8/28/18 9:53:11.000 PM	Endpoint	Failed backup attempt by thenorth	Medium	New	unassigned	▼
>	8/28/18 9:52:07.000 PM	Endpoint	Failed backup attempt by thenorth	Medium	New	unassigned	▼
>	8/28/18 9:52:05.000 PM	Endpoint	Failed backup attempt by winterfell	Medium	New	unassigned	▼
>	8/28/18 9:52:05.000 PM	Endpoint	Failed backup attempt by winterfell	Medium	New	unassigned	▼
>	8/28/18 9:52:05.000 PM	Endpoint	Registry Key Associated With Persistence Modified on winterfell	Low	New	unassigned	▼
> ▾	8/28/18 9:52:05.000 PM	Endpoint	Failed backup attempt by winterfell	Medium	New	unassigned	▼

Description:
The system winterfell attempted a backup but encountered an error.

Additional Fields	Value	Action	Correlation Search:
Destination	winterfell 159470	▼	ESCU - Unsuccessful Netbackup backups - Rule
Destination Expected	false	▼	
Destination PCI Domain	untrust	▼	
Destination Requires Antivirus	false	▼	
Destination Should Time Synchronize	false	▼	
Destination Should Update	false	▼	
Signature	An error occurred, failed to backup.	▼	

Related Investigations:
Currently not investigated.

History:
[View all review activity for this Notable Event](#)

Adaptive Responses: [▼](#)

Response	Mode	Time	User	Status
Notable	saved	2018-08-28T21:40:27+0000	admin	✓ success
Risk Analysis	saved	2018-08-28T21:40:27+0000	admin	✓ success

[View Adaptive Response Invocations](#)

Next Steps:

Recommended following steps:

- ESCU-Contextualize:** Based on ESCU context gathering recommendations:
 - ESCU - Get Notable History
 - ESCU - Get Risk Modifiers For Endpoint
 - ESCU - Get Risk Modifiers For User
- ESCU-Investigate:** Based on ESCU investigate recommendations:
 - ESCU - All backup logs for host

Event Details:

event_id	15BD9F07-38CF-44EA-89C8-8E7225712C77@@@notable@@@c110ce12b182ff1ceec81d1d1132c010	▼
event_hash	c110ce12b182ff1ceec81d1d1132c010	▼
eventtype	modnotable_results	▼
notable		▼
Short ID	Create Short ID	

>	8/28/18 9:52:05.000 PM	Endpoint	Failed backup attempt by winterfell	Medium	New	unassigned	▼
>	8/28/18 9:52:05.000 PM	Endpoint	Failed backup attempt by winterfell	Medium	New	unassigned	▼

Alerts Should Be Meaningful

Suspicious Network Connection 7

Detected an unusual network connection or one with possible security implications.

Start Date Aug 26, 2018 3:48 PM **End Date** Aug 26, 2018 3:58 PM

Watchlists ★

Categories Allowed Exfiltration Outgoing Suspicious Pattern Unusual Network Connection

DNS (Domain Name System) is protocol that follows a request/response model. This connection, however, is consistent with an acknowledged data transfer. This is especially suspicious because this connection is UDP. The source, Internal host acme-48140652, uploaded data to External host 54.190.62.152. UDP 53 is generally open on external firewalls, so this is likely an attempt to exfiltrate data without being detected.

Relevant Features:

- Connection contained a High number of bytes
- Transfer over UDP
- Data uploaded to external address

Event Details:

event_id	15BD9F07-38CF-44EA-89C9-8E7225712C
event_hash	c110ce12b182ff10eef1d1d1132c010
eventtype	modtable_results
notable	notable
Short ID	Create Short ID

Users (1)
Beau Struthers

Devices (2)
Internal
acme-48140652
External
54.190.62.152

Apps (1)
dns

Threats (1)
Data Exfiltration by Suspicious User or Device (1)

Anomaly Relations

```

graph LR
    BeauStruthers[Beau Struthers] --- NetworkConn[Suspicious Network Connection]
    acme48140652[acme-48140652] --- NetworkConn
    dns[dns] --- NetworkConn
    54_190_62_152[54.190.62.152] --- NetworkConn
  
```

Alerts Should Be Actionable

Splunk User Behavior Analytics

Anomalies Table / Anomaly Details

Suspicious Powershell Activity 4

Detected an attack with possible powershell usage

Start Date Aug 25, 2018 12:00 AM **End Date** Aug 26, 2018 12:00 AM

Event Details:

event_id	15BD9F07380F-4
event_hash	c110ce12b182ff1
eventtype	modnable_result
	notable
Short ID	Create Short ID

Watchlists ★

Categories Lateral Movement, Suspicious Pattern

Behavioral analysis of PowerShell activity for acme-91156372 has identified certain patterns that can indicate malicious intent. The suspicious behaviors detected can be summarized as follow:

- * Bigram Average: Powershell command detected with significant proportion of random sequences in character strings
- * Encoding Analysis: Boolean value indicating high likelihood of character encoding
- * High Risk Command Count: Large number of risky commands detected in powershell log.
- * Entropy Analysis: Powershell command detected with high entropy in character strings

Devices (1)
Internal
acme-91156372 2

Threats (1)
Malware (1) 6

Suspicious Network Connection 7

Detected an unusual network connection or one with possible security implications.

Start Date Aug 26, 2018 3:48 PM **End Date** Aug 26, 2018 3:58 PM

Watchlists ★

Categories Allowed, Exfiltration, Outgoing, Suspicious Pattern, Unusual Network Connection

DNS (Domain Name System) is protocol that follows a request/response model. This connection, however, is consistent with an acknowledged data transfer. This is especially suspicious because this connection is UDP. The source, Internal

Actions

All Alerts Are Not Created Equal

Suspicious Network Connection 7

Detected an unusual network connection or one with possible security implications.

Start Date: Aug 26, 2018 3:48 PM End Date: Aug 26, 2018 3:58 PM

Watchlists: ★

Categories: Allowed, Exfiltration, Outgoing, Suspicious Pattern, Unusual Network Connection

i	Time	Urgency	Security Domain	Title
>	8/29/18 3:50:39.000 AM	Low	Network	Abnormally High Number of HTTP GET Request Events By 10.186.85.250
>	8/29/18 3:50:36.000 AM	Low	Network	Abnormally High Number of HTTP GET Request Events By 10.186.217.239
>	8/29/18 3:50:36.000 AM	Low	Network	Abnormally High Number of HTTP GET Request Events By 10.185.148.20
>	8/29/18 3:50:36.000 AM	Low	Network	Abnormally High Number of HTTP GET Request Events By 10.184.171.56
>	8/29/18 3:50:36.000 AM	Low	Network	Abnormally High Number of HTTP GET Request Events By 10.176.185.54
>	8/29/18 3:50:36.000 AM	Low	Network	Abnormally High Number of HTTP GET Request Events By 10.174.96.92
>	8/29/18 3:50:36.000 AM	Low	Network	Abnormally High Number of HTTP GET Request Events By 10.169.15.7
>	8/29/18 3:50:36.000 AM	Low	Network	Abnormally High Number of HTTP GET Request Events By 10.163.243.2
>	8/29/18 3:50:36.000 AM	Low	Network	Abnormally High Number of HTTP GET Request Events By 10.153.60.212
>	8/29/18 3:50:36.000 AM	Low	Network	Abnormally High Number of HTTP GET Request Events By 10.149.197.224
>	8/29/18 3:50:36.000 AM	Low	Network	Abnormally High Number of HTTP GET Request Events By 10.148.36.75
>	8/29/18 3:50:36.000 AM	Low	Network	Abnormally High Number of HTTP GET Request Events By 10.145.145.57
>	8/29/18 3:50:36.000 AM	Low	Network	Abnormally High Number of HTTP GET Request Events By 10.145.141.224

Suspicious Po

Detected an attack with

Start Date: Aug 25, 2018

Watchlists: ★

Categories: Lateral Move

Behavioral analysis of P

- * Bigram Average: Power
- * Ecoding Analysis: Boc
- * High Risk Command C
- * Entropy Analysis: Pow

Devices (1)
Internal
acme-91156372

Threats (1)
Malware (1) 6

splunk> .conf18

Some Alerts Are Straightforward

Time	Security Domain	Title	Urgency	Status	Owner	Actions
> SelectAll 28/18 9:54:00.000 PM	Endpoint	Registry Key Associated With Persistence Modified on winterfell	Low	New	unassigned	
> 8/28/18 9:54:00.000 PM	Endpoint	Registry Key Associated With Persistence Modified on winterfell	Low	New	unassigned	
> 8/28/18 9:53:11.000 PM	Endpoint	Failed backup attempt by thenorth	Medium	New	unassigned	
> 8/28/18 9:52:01.000 PM	Endpoint	Failed backup attempt by thenorth	Medium	New	unassigned	
> 8/28/18 9:52:05.000 PM	Endpoint	Failed backup attempt by winterfell	Medium	New	unassigned	
> 8/28/18 9:52:05.000 PM	Endpoint	Failed backup attempt by winterfell	Low	New	unassigned	
> 8/28/18 9:52:05.000 PM	Endpoint	Registry Key Associated With Persistence Modified on winterfell	Low	New	unassigned	

▼ 8/29/18 3:50:20.000 AM High Endpoint

Suspicious Network Connection 7

Detected an unusual network connection or one with possible security implications.

Start Date: Aug 26, 2018 3:48 PM **End Date:** Aug 26, 2018 3:58 PM

Watchlists:

Categories: Allowed, Exfiltration, Outgoing, Suspicious Pattern, Unusual Network Connection

Actions

Host With Multiple Infections (212.27.63.151)

New

Description:

The device 212.27.63.151 was detected with multiple (2) infections.

Additional Fields

	Value
Destination	212.27.63.151 560
Destination Expected	false
Destination PCI Domain	untrust
Destination Requires Antivirus	false
Destination Should Time Synchronize	false
Destination Should Update	false
Tag	modaction_result

Action

Correlation Search:

[Endpoint - Host With Multiple Infections - Rule](#)

History:

[View all review activity for this Notable Event](#)

Contributing Events:

[View all infection events associated with device 212.27.63.151](#)

Adaptive Responses:

Response	Mode	Time	User	Status
Notable	saved	2018-08-29T03:50:17+0000	admin	success
Risk Analysis	saved	2018-08-29T03:50:17+0000	admin	success

[View Adaptive Response Invocations](#)

Devices (1)

Internal

acme-91156372

> 8/29/18 3:50:36.000 AM	Low	Network	Abnormally High Number of HTTP GET Request Events By 10.145.145.57
> 8/29/18 3:50:36.000 AM	Low	Network	Abnormally High Number of HTTP GET Request Events By 10.145.141.224

2

But it's Easy to get Lost

This isn't right



There Are Better Ways!



Grouping Anomalies With UBA

Unusual Geolocation

splunk> User Behavior Analytics

Home / Threats Table / Threat Details / Anomaly Details

Unusual VPN Login Geolocation 3

VPN Login Activity from unusual/rare geographic locations that do not match the profile of the user.

Start Date Aug 20, 2018 12:00 AM **End Date** Aug 21, 2018 12:00 AM

Watchlists ★▼

Categories Account Takeover Incoming Unusual Activity

Found 1 rare value(s) over a period of 3043 days.

1. **Geo Location [KR]** is uncommon in this environment -- **1 occurrence(s)** out of 3.2K. Most commonly observed values (up to top 3) are:

- [US] occurs 3.2K time(s) out of 3.2K (**99.9%**)
- [RU] occurs 2 time(s) out of 3.2K (**0.1%**)
- [CN] occurs 1 time(s) out of 3.2K (**0.0%**)



Scanning Activity



Scanning Activity

5

Detected a possible horizontal or vertical scan over the network.

Start Date Aug 22, 2018 12:00 AM **End Date** Aug 23, 2018 12:00 AM

Watchlists ★▼

Categories Lateral Movement Unusual Activity

Device acme-70231045 scanned multiple hosts looking for 1 particular service over the course of 7 days.

It is likely that an attacker is attempting to locate a specific service or type of host on the network while avoiding detection with a long-running scan. A stealth service scan like this usually indicates that an attacker has an exploit for a service and is looking for available hosts to exploit.

Device acme-70231045 looked for 5 distinct destinations, sending 6 probes. 3 probes were acknowledged.

Device acme-70231045 scan behavior shows regularity in the number of service scanned per day, but variations in the destinations scanned.

The tables below show details about each service scanned. For each service scanned we show maximum 50 destinations.

Scanned Destinations for Service: tcp on port 3389 (1)

Group By: Service: tcp on port 3389 ▾

This scan took more than one day to complete: total 7 days. Out of 6 probes, 3 were acknowledged. This scan may provide an interactive command environment: rdp.

SERVICE: TCP ON PORT 3389	DESTINATION	# PROBES	# ACKNOWLEDGED PROBES	# EVENTS OTHER THAN PROBES
	acme-54698001	1	1	0
	acme-51945572	2	2	0
	acme-88415989	1	0	0
	acme-60980983	1	0	0
	acme-94126743	1	0	0

Excessive Data Transmission

[Home](#) / [Threats Table](#) / [Threat Details](#) / [Anomaly Details](#)



Excessive Data Transmission

5

Users transmitting an excessive amount of data.

Start Date Aug 28, 2018 12:00 AM

End Date Aug 29, 2018 12:00 AM

Watchlists ★

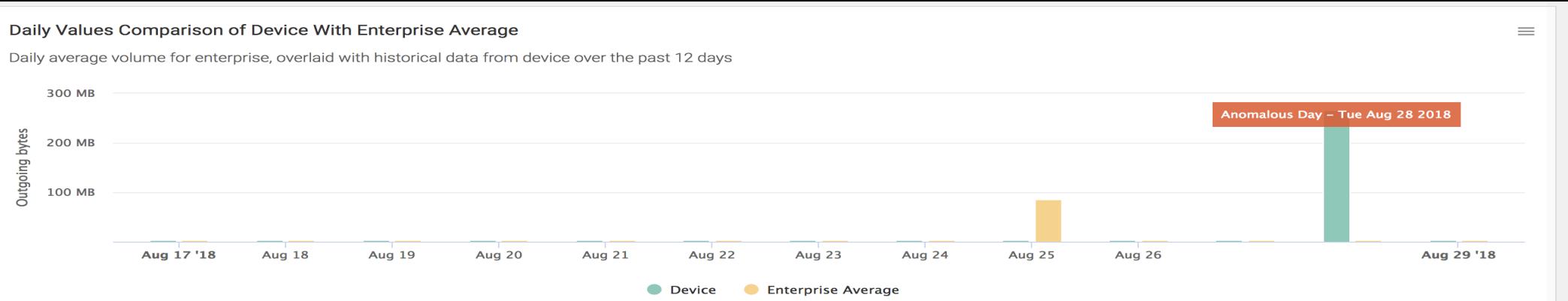
Categories

Exfiltration

Outgoing

Unusual Activity

The volume of data transmitted over the network by device shows abnormal temporal patterns. Anomalous value is 253.5 MB in a daily window. Device average is 628.9 KB.



Breakdown by External Destination (254 MB)

Group By: External Destination ▾

Breakdown of volume of data transmitted over the network by external destination on day 2018-08-28.

EXTERNAL DESTINATION	VOLUME	PERCENTAGE
162.125.248.24	253 MB	99.6%
104.40.17.172	414 KB	0.16%

Together, Those Anomalies Constitute a Problem

splunk> User Behavior Analytics

Home / Threats Table / Threat Details

Data Exfiltration by Compromised Account 5 »

Users are moving large amounts of data out of the network after multiple login anomalies.

Detection Date Aug 28, 2018 10:50 AM

Watchlists ★

Categories External Kill Chain

Remote account takeover followed by unusual activity and data exfiltration

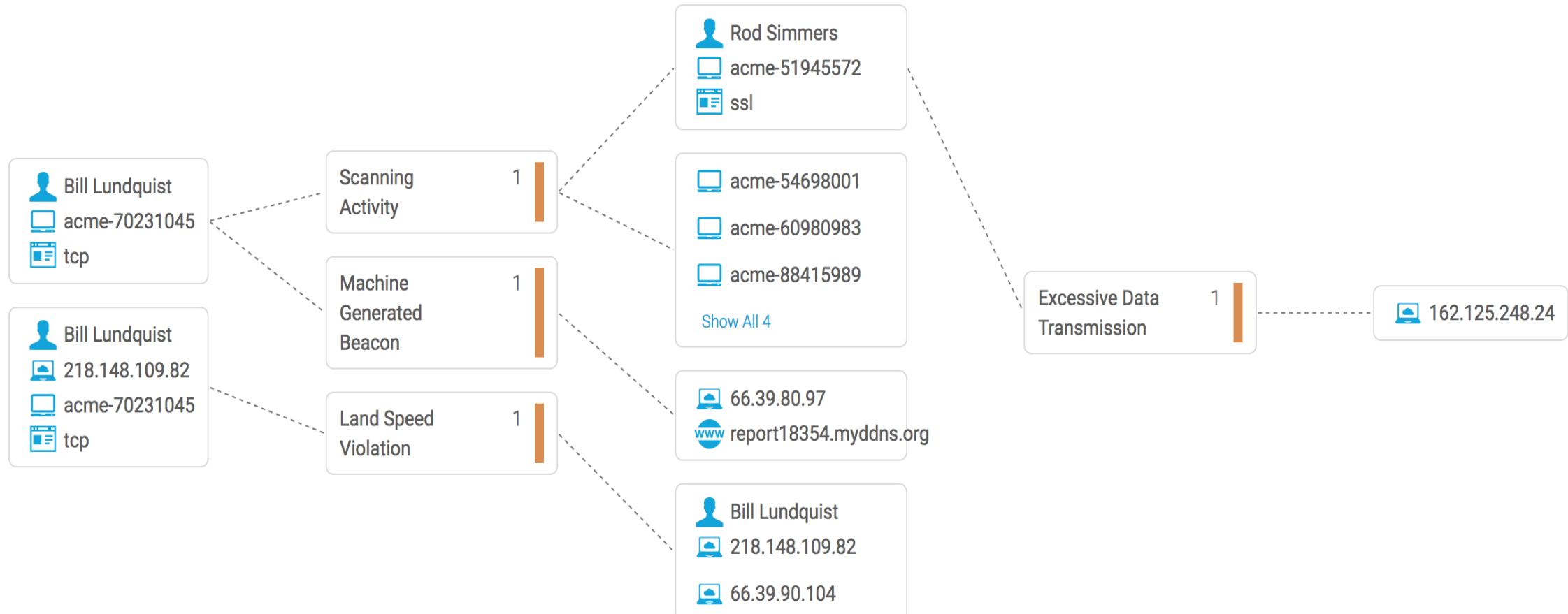
Entity involved in a sequence of events constituting a threat: it was first involved in unusual login activity and unusual internal activity, followed by an unusual data transfer to external destination. This threat should be investigated for possible user compromise followed by data exfiltration.

Timeline	Anomalies (5)	Users (2)	Devices (10)	Apps (2)	Domains (1)	What Next?
First Anomaly 18 Aug, 2018	Excessive Data Transmission (1) Land Speed Violation (1) Machine Generated Beacon (1) Scanning Activity (1) Unusual VPN Login Geolocation (1)	Bill Lundquist (3) Rod Simmers (3)	Internal (1) 66.39.90.104 (1) acme-14614411 (1) acme-35738865 (1) acme-52672270 (1) acme-70231045 (2)	ssl (5) tcp (4)	report18354.myddns.org (1)	Collect more information for the users involved and investigate their activities. Disable the account of the user.
Last Anomaly 26 Aug, 2018						
Duration 8d						

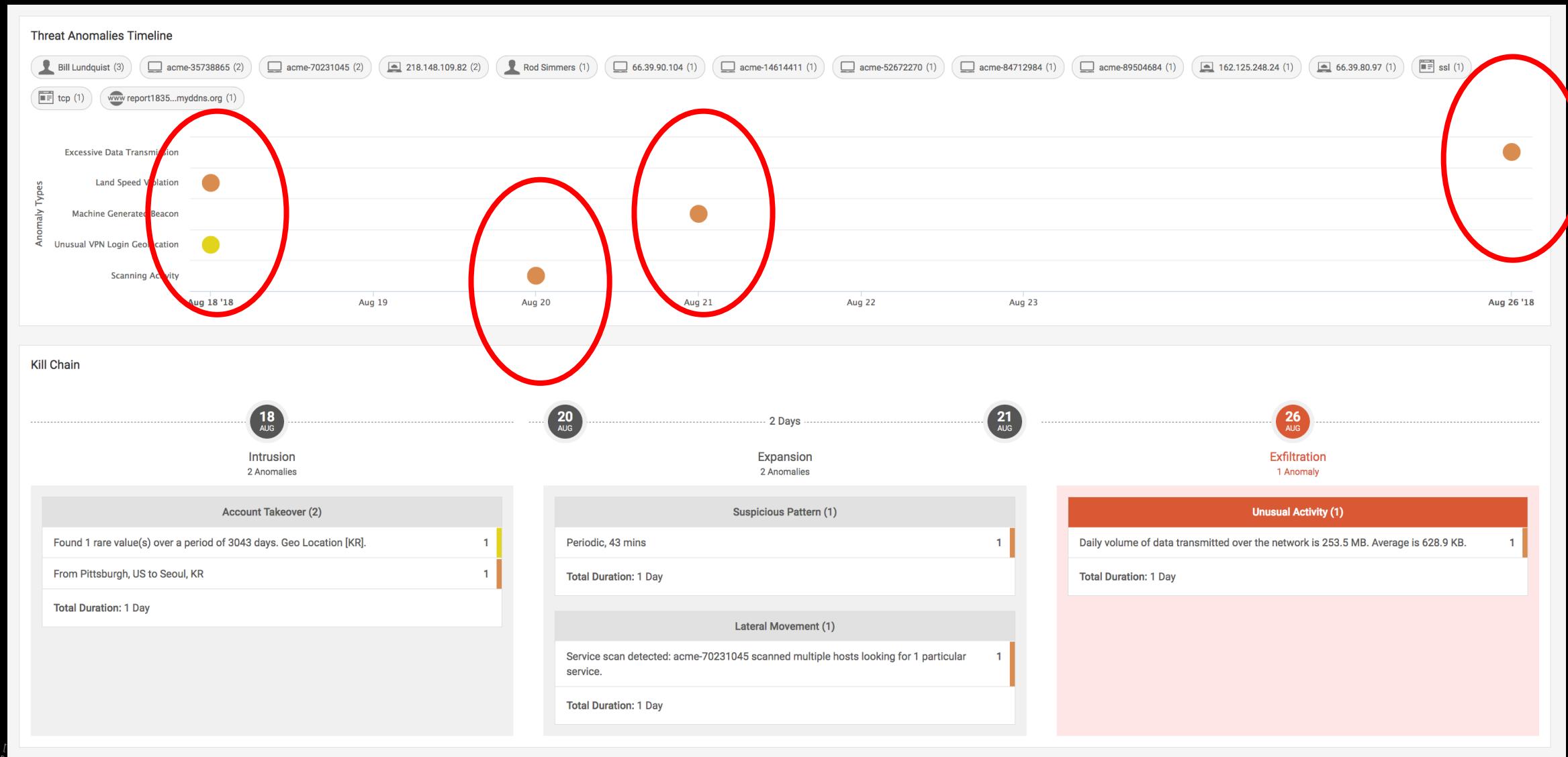
Threat Relations

Finding Complex Behaviors

Threat Relations



Actionable Threats



Event Sequencing



What is this Sorcery?

- ▶ The Event Sequencing Engine provides additional capabilities for threat detection by allowing you to **group correlation searches into clusters of events**, either in a specific sequence, by specific attributes, or both.
- ▶ You do this by defining a workflow to run correlation searches in an order of your choice, specifying what notables would need to occur in order to advance to the next step.
- ▶ The concept is similar to writing a script to automate the things that you might otherwise have to do manually when tracking a variety of notables and variables through a variety of correlation searches.

Basic Structure

- ▶ Define a starting event
- ▶ Define a set of transition events
 - Order can be enforced
- ▶ Define an ending event

General Malware Behavior

- ▶ Run a process never seen before
- ▶ Download an executable
- ▶ Visit a domain never visited before

138.60.4 ~ [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD15LAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST_6&product_id=EST_5&product_name=Buttercup Shopping" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17.14.10 ~ [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD55L7FF6ADFF9 HTTP 1.1" 404 332 "http://buttercup-shopping.com/cart.do?action=plusless&itemId=EST_26&product_id=EST_26&product_name=Buttercup Shopping" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17.14.10 ~ [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST_26&JSESSIONID=SD55L9FF1ADEF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST_18&product_id=EST_18&product_name=Buttercup Shopping" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17.14.10 ~ [07/Jan 18:10:55:187] "GET /oldlink?item_id=EST_68&JSESSIONID=SD85LBF2ADFF9 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST_18&product_id=EST_18&product_name=Buttercup Shopping" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17.14.10 ~ [07/Jan 18:10:55:187] "GET /oldlink?item_id=EST_68&JSESSIONID=SD85LBF2ADFF9 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST_18&product_id=EST_18&product_name=Buttercup Shopping" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17.14.10 ~ [07/Jan 18:10:55:187] "GET /category.screen?category_id=SURPRISE&JSESSIONID=SD85LBF2ADFF9 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST_68&product_id=EST_68&product_name=Buttercup Shopping" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17.14.10

Not Everything Qualifies as an Alert

- ▶ Run a process never seen before
 - Any time you install something new
- ▶ Download an executable from Internet
 - Happens all the time
- ▶ Visit a domain never visited before
 - Happens frequently

Event Sequencing Demo



Automation



I Don't Want to Deal with Alerts



imgflip.com

Continue Previous Example

- ▶ Those three events happening is very interesting*
- *Interesting != malicious
- ▶ What can we do next?

138.60.4 ~ [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD15LAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FZ-SW-04" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17.14.103
 128.241.220.82 ~ [07/Jan 18:10:57:153] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD55L7FF6ADFF9 HTTP 1.1" 404 332 "http://buttercup-shopping.com/cart.do?action=plus&itemId=EST-26&product_id=FZ-SW-04" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17.14.103
 317.27.160.0.0 ~ [07/Jan 18:10:57:153] "GET /oldlink?item_id=EST-26&JSESSIONID=SD55L9FF1ADEF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&productId=SD55L9FF1ADEF3" 2423 125.17.14.103
 ://buttercup-shopping.com/purchase&it... ://buttercup-shopping.com/cart.do?actio... ://buttercup-shopping.com/cart.do?actio... ://buttercup-shopping.com/cart.do?actio...

Where Automation Can Help

INVESTIGATE

- Grab a copy of the binary
- Detonate it
- If determine to be malicious, remediate

REMEDIATE

- Isolate Machine
- Deactivate Account
- Notify IT to restore from backup

ROOT CAUSE ANALYSIS

- Kick off Investigation
- Run Searches
- Create your own threat intel

Conclusion



Where do I go From Here?

- ▶ Talk to your Splunk account manager/sales engineer
- ▶ Splunk Enterprise Security: <http://docs.splunk.com/Documentation/ES/latest>
- ▶ Splunk UBA: <http://docs.splunk.com/Documentation/UBA>
- ▶ Phantom: https://www.splunk.com/en_us/software/splunk-security-orchestration-and-automation.html
- ▶ Event Sequencing Docs:
http://docs.splunk.com/Documentation/ES/5.2.0/Admin/Sequencecorrelation_searches

Thank You

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

