Addressing Alert Fatigue

David Dorsey | Sr. Manager Security Research

Forward-Looking Statements

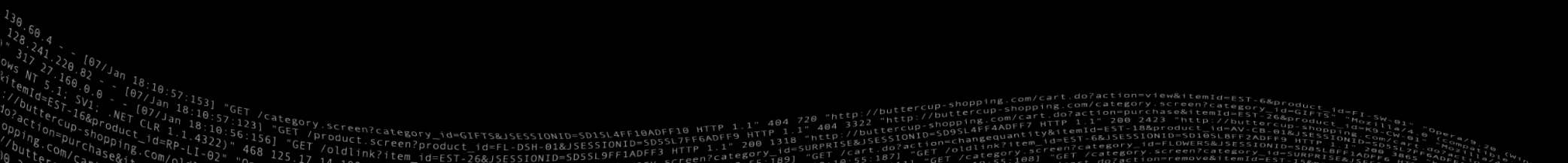
During the course of this presentation, we may make forward-looking statements regarding future events or the expected performance of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results 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> .conf18

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



Agenda

- Level Setting
- Grouping Anomalies
- Event Sequencing
- Automation

Level Setting

Words matter

splunk> .conf18

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
>	SelectAll 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	
v	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
Destination	winterfell 159470	
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.

Correlation Search:

ESCU - Unsuccessful Netbackup backups - Rule

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:

1. ESCU-Contextualize: Based on ESCU context gathering recommendations:
- ESCU - Get Notable History
- ESCU - Get Risk Modifiers For Endpoint
- ESCU - Get Risk Modifiers For User

2. ESCU-Investigate: Based on ESCU investigate recommendations:
- ESCU - All backup logs for host

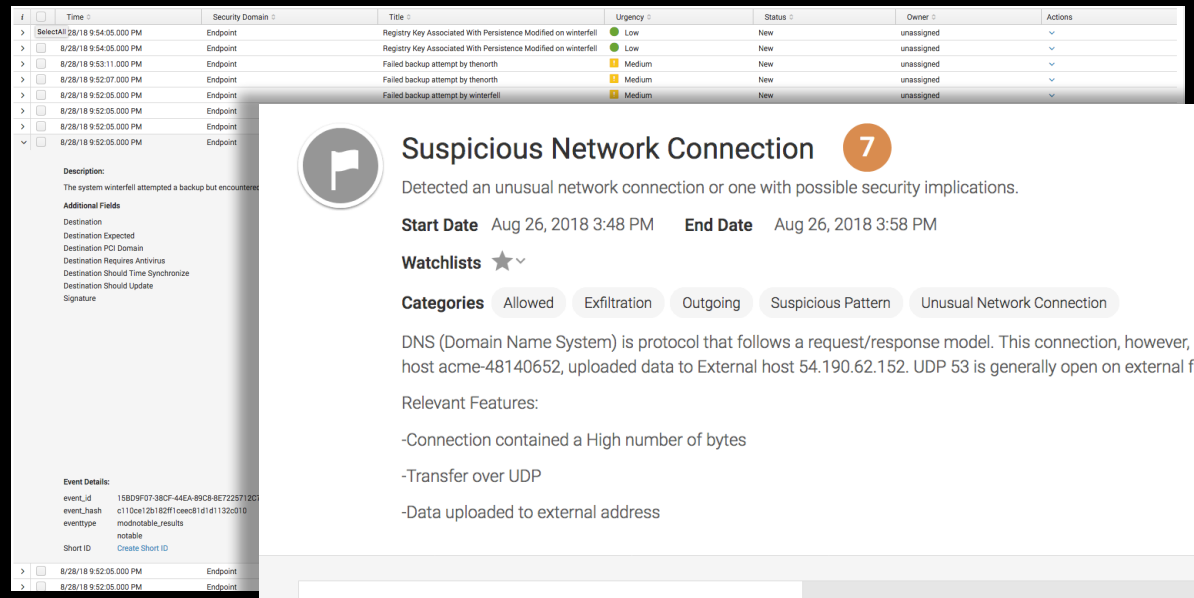
Event Details:

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	

splunk> .conf18

Alerts Should Be Meaningful



Suspicious Network Connection 7

Actions

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:

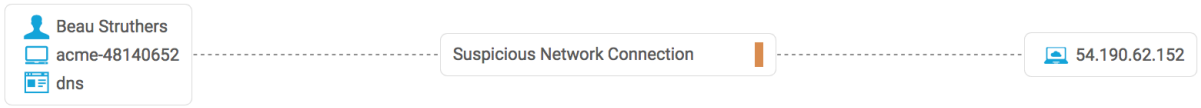
-Connection contained a High number of bytes

-Transfer over UDP

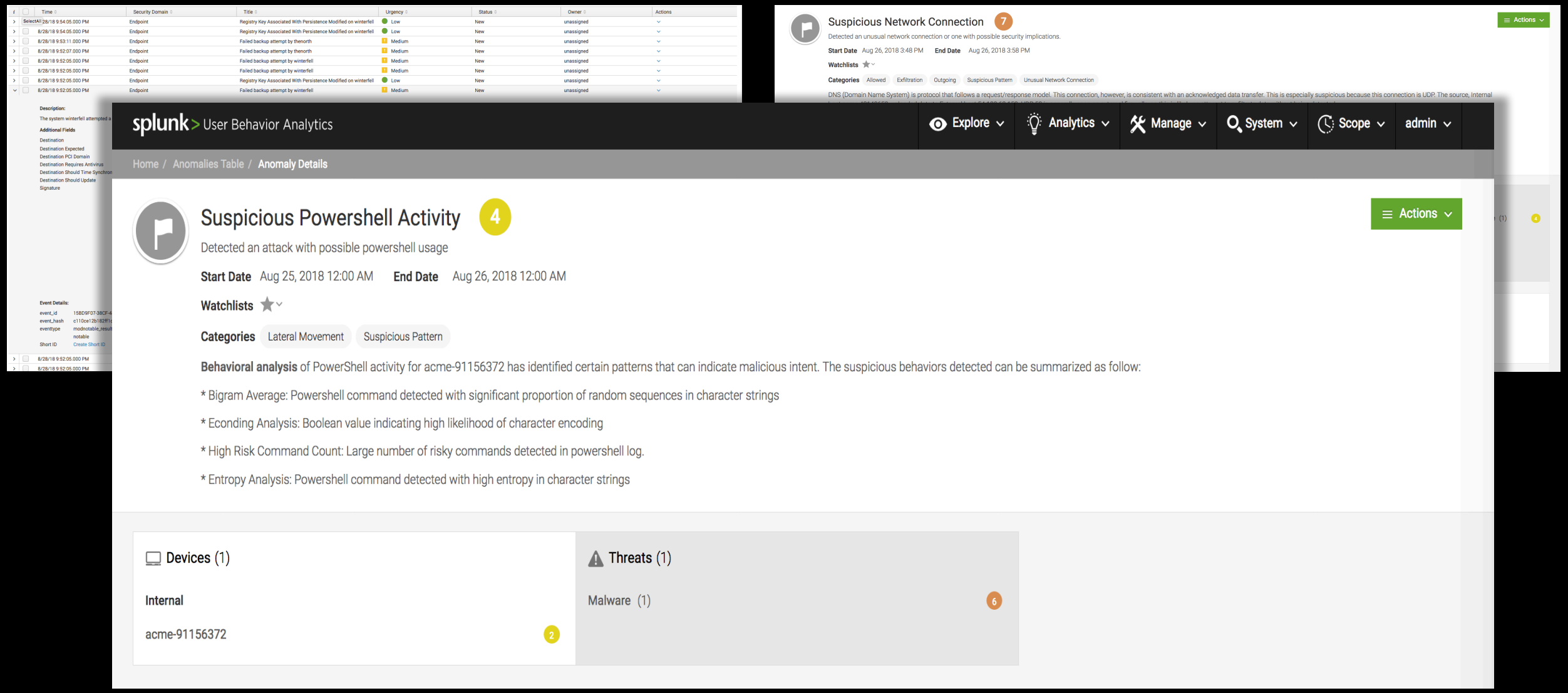
-Data uploaded to external address

Users (1)	Devices (2)	Apps (1)	Threats (1)
Beau Struthers 3	**Internal**	dns 3	Data Exfiltration by Suspicious User or Device (1) 4
	acme-48140652 1		
	External		
	54.190.62.152 1		

Anomaly Relations

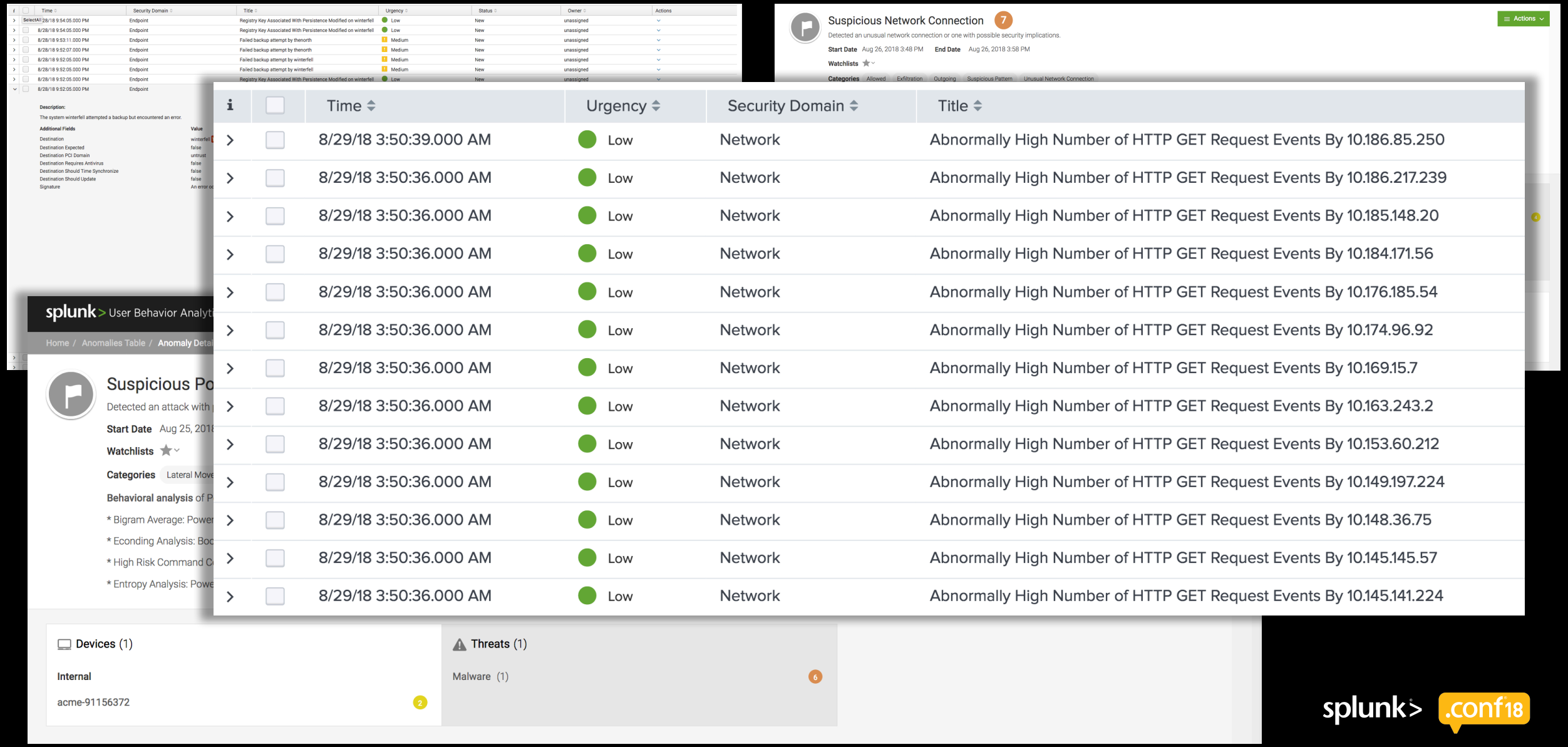


Alerts Should Be Actionable



splunk> .conf18

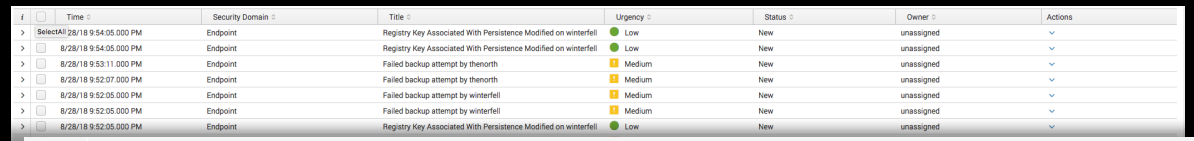
All Alerts Are Not Created Equal

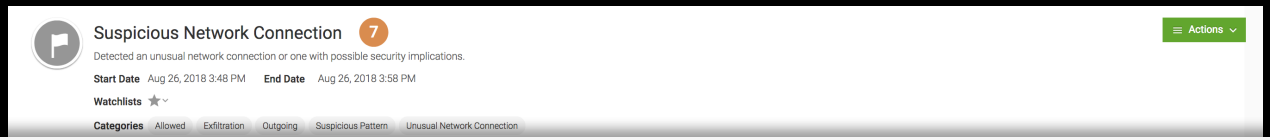


Time	Urgency	Security Domain	Title
8/29/18 3:50:39.000 AM	Low	Network	Abnormally High Number of HTTP GET Request Events By 10.186.85.250
8/29/18 3:50:36.000 AM	Low	Network	Abnormally High Number of HTTP GET Request Events By 10.186.217.239
8/29/18 3:50:36.000 AM	Low	Network	Abnormally High Number of 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

splunk> .conf18

Some Alerts Are Straightforward





8/29/18 3:50:20.000 AM | High | Endpoint | 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	Action
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	

Related Investigations:

Currently not investigated.

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

splunk> .conf18

But it's Easy to get Lost

This isn't right

There Are Better Ways!

Grouping Anomalies With UBA

splunk> .conf18

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 th

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%**)

splunk> .conf18

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

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

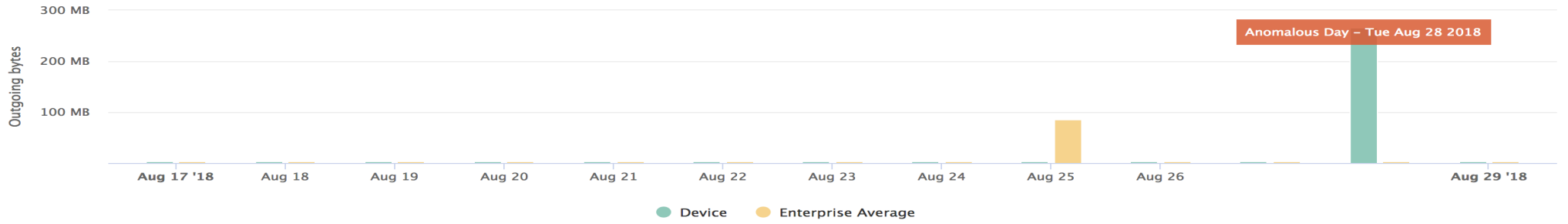
Watchlists

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.

Daily Values Comparison of Device With Enterprise Average

Daily average volume for enterprise, overlaid with historical data from device over the past 12 days



Breakdown by External Destination (254 MB)

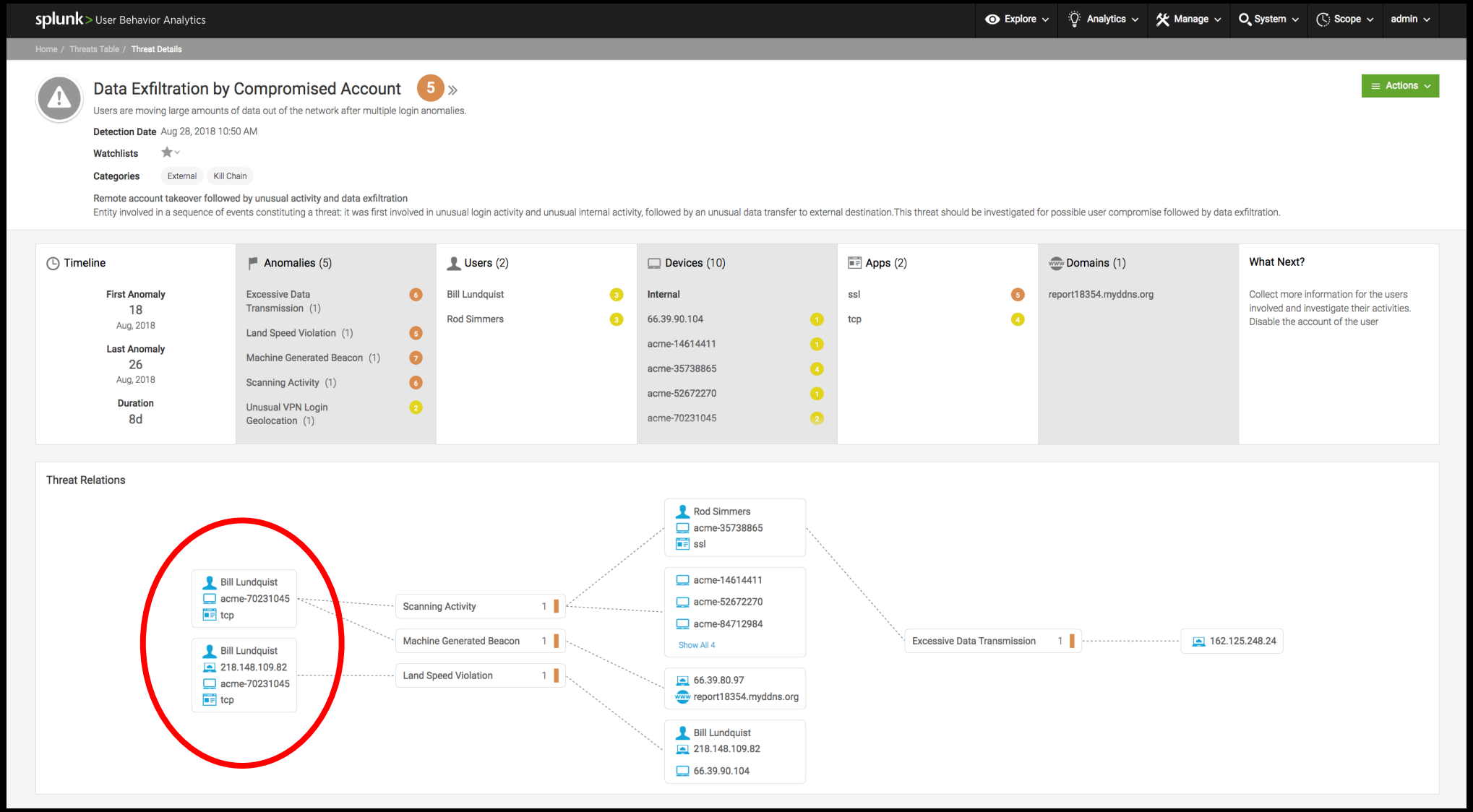
Group By: External Destination

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

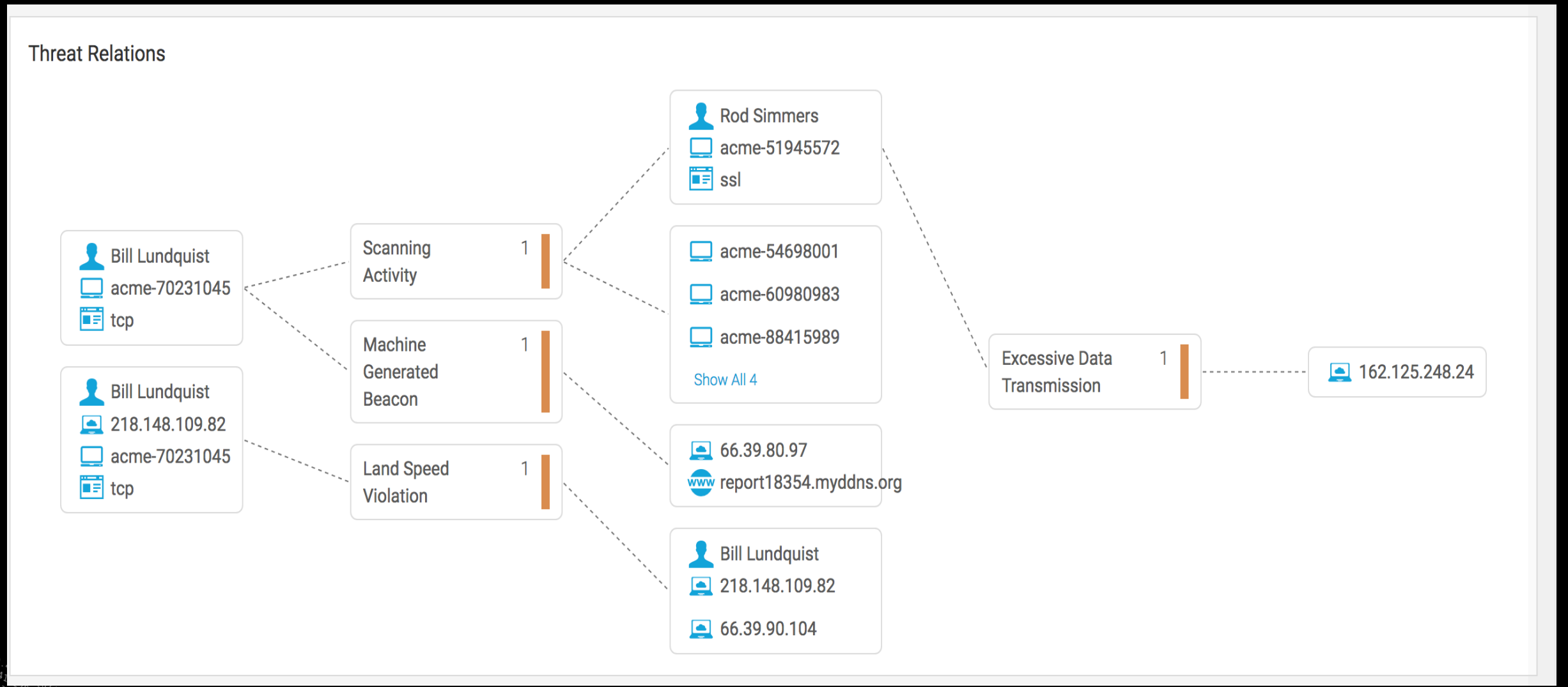
EXTERNAL DESTINATION	VOLUME	PERCENTAGE
162.125.248.24	253 MB	99.6%
104.40.17.172	414 KB	0.16%

splunk> .conf18

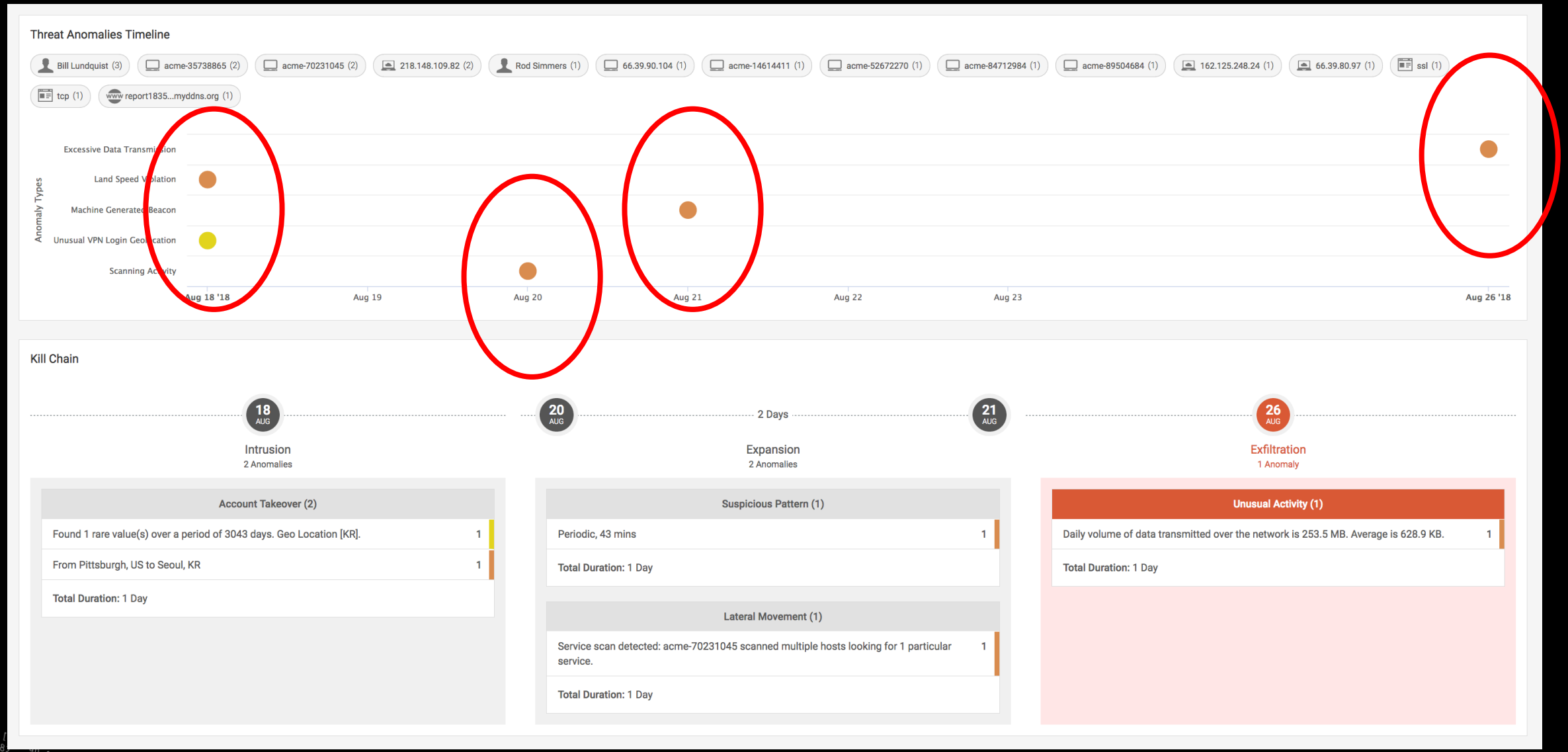
Together, Those Anomalies Constitute a Problem



Finding Complex Behaviors



Actionable Threats



splunk> .conf18

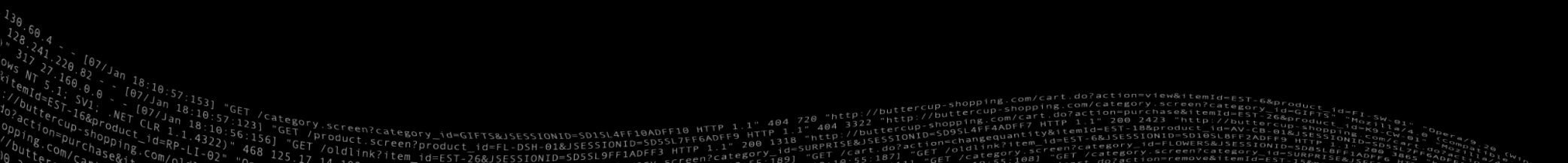
Event Sequencing

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



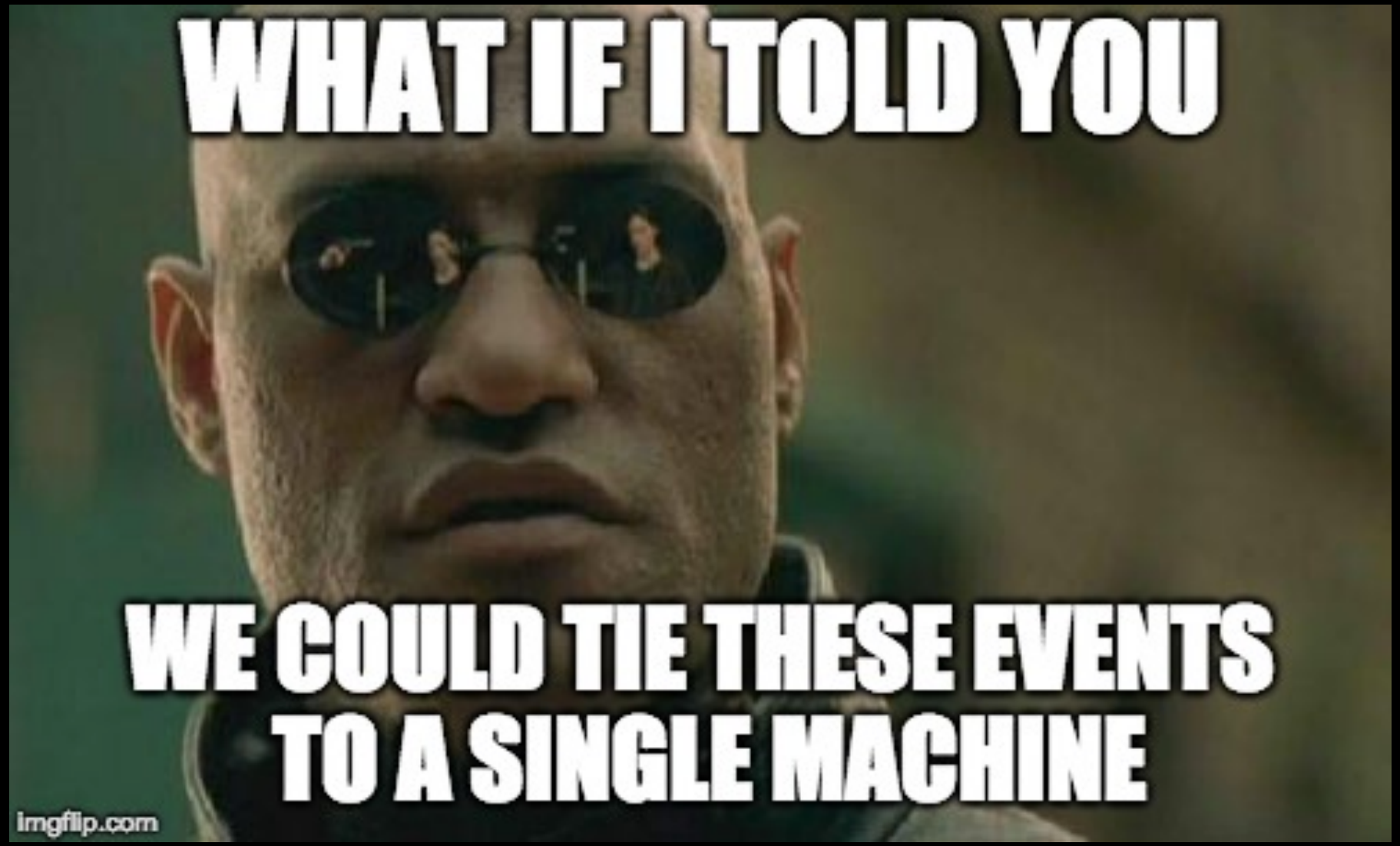
General Malware Behavior

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

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

What If?

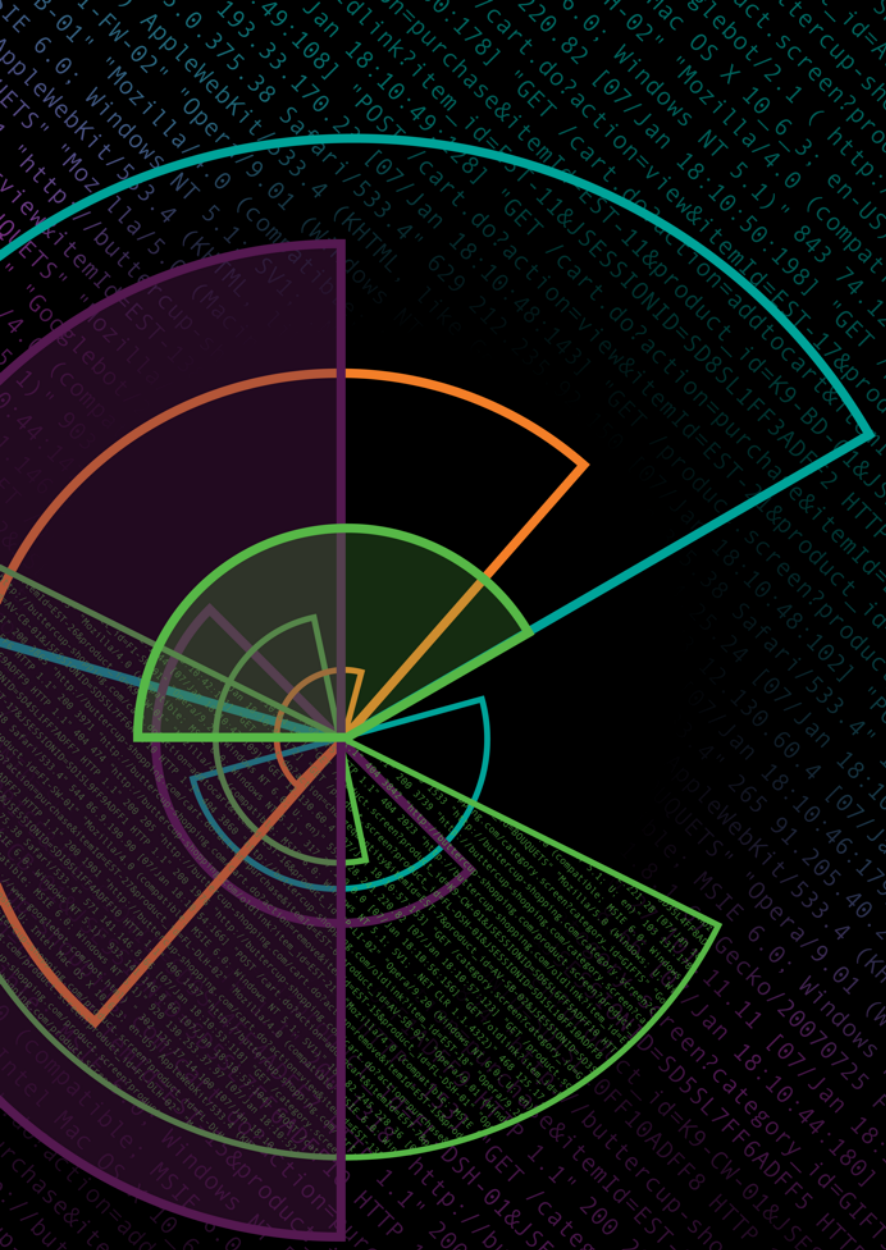


Event Sequencing Demo

Event Sequencing Demo

- An endpoint visited a domain it's never seen before
- Same endpoint downloaded an executable
- Same endpoint ran a process it's never seen before

splunk> .conf18

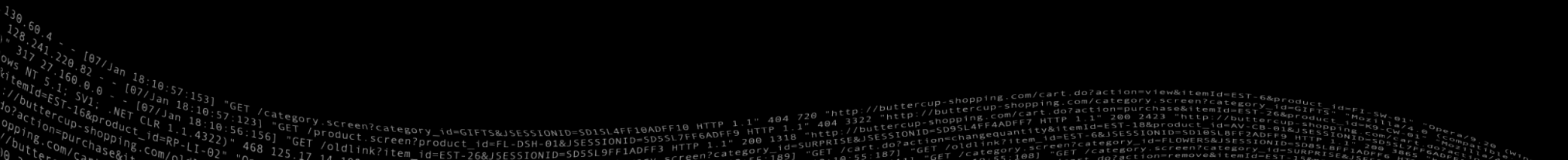


Automation

I Don’t Want to Deal with Alerts

Continue Previous Example

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



Where Automation Can Help

INVESTIGATE

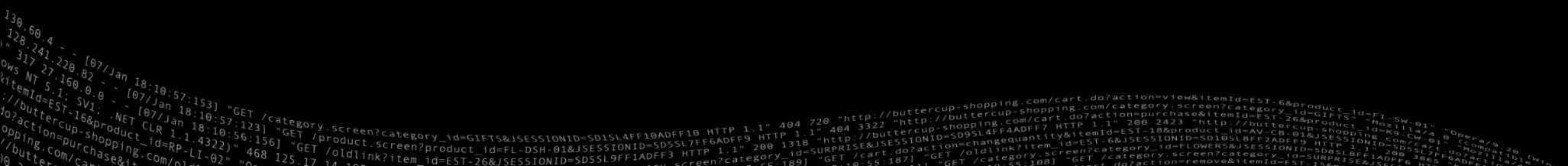
- Grab a copy of the binary
- Detonate it
- If determine to be malicious, remediate

REMEDIATE

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

ROOT CAUSE ANALYSIS

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



splunk> .conf18

Conclusion

What Just Happened?

- We can group individual events together
  - Event Sequencing
  - UBA
- Leverage Automation
  - Reduce investigation time
  - Assist with remediation
  - Root Cause Analysis

Where do I go From Here?

- Talk to your Splunk account manger/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/Sequencecorrelationsearches

Thank You

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