



# Advanced Threat Hunting and Anomaly Detection with Splunk UBA

Tom Smit  
Staff Sales Engineer | Splunk

# 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. © 2019 Splunk Inc. All rights reserved.

# #whoami

## Tom Smit

[smitty@splunk.com](mailto:smitty@splunk.com)

Staff Sales Engineer

@tsmit – Twitter

@tsmit5050 – IG

- ▶ Working at Splunk for almost 5 years
- ▶ Security and UBA SME
- ▶ BOTS v3 and v4 content creator / UBA overlord
- ▶ Previous life at Core Security, Mimecast, Symantec, and Raytheon
  
- ▶ #2hourstobeer OR #ivebeendrinkingsincebreakfast

# Sooooo.....

Everyone knows what UBA is, right?

- ▶ Yes, I know I used this meme last year
- ▶ UBA is an amazing piece of technology
- ▶ It's exceptional at finding all the things that you forgot to look for
- ▶ It can find the things you want to look for
- ▶ It is not great at finding Bob logging into your server for the first time (actually, it really is good at that, but you did pay money for this tool, don't you want it to do what it's supposed to do?)



# Based on BOTS!

- ▶ But wait... what is BOTS?
- ▶ Ohhh... let me tell you a story...







# How Big Was BOTS?

811

335

56

Players that  
Answered a  
Question

Teams  
Played

Questions  
Attempted  
per Minute

# Question Stats!

17548

Question  
Attempts

10601

Correct  
Answers

6947

Incorrect  
Answers

3873

Hints  
Purchased

# A Little Something Extra ...

The screenshot shows a dark-themed web interface for the "splunk> BOSS of the SOC" challenge. At the top, it says "Results for Question 100". Below that, a green "Correct!" message is displayed. A table shows "Base Points Earned" as 50 and "Speed Bonus Points Earned" as 25. A note below states: "Note: Regardless of the result shown above, your team will not be awarded points for answering the same question correctly multiple times." A text input field contains the instruction: "Nice work! For 5 bonus points, please enter the most helpful Splunk search you ran (or a brief description of any other site or technique you used) to answer this question." A "Submit" button is next to the input field. At the bottom left, there are links: "Attempt this question again", "Return to Question List", and "View Response Details". A large pink callout bubble points from the text input area to the following text:

Enter your Splunk search for a few bonus points.

# HEY THAT EXAMPLE WAS THE ANSWER YOU TRICKSTERS

bacon

Guessing rot13 beacuse its always [REDACTED] king rot13

I used my finger to click the left mouse button

That song rock my sox  
That was a [REDACTED] question.  
That was [REDACTED].

help idk what i'm doing

The dudes standing behind me were right

i know this song  
i like cake  
i like this uba thing

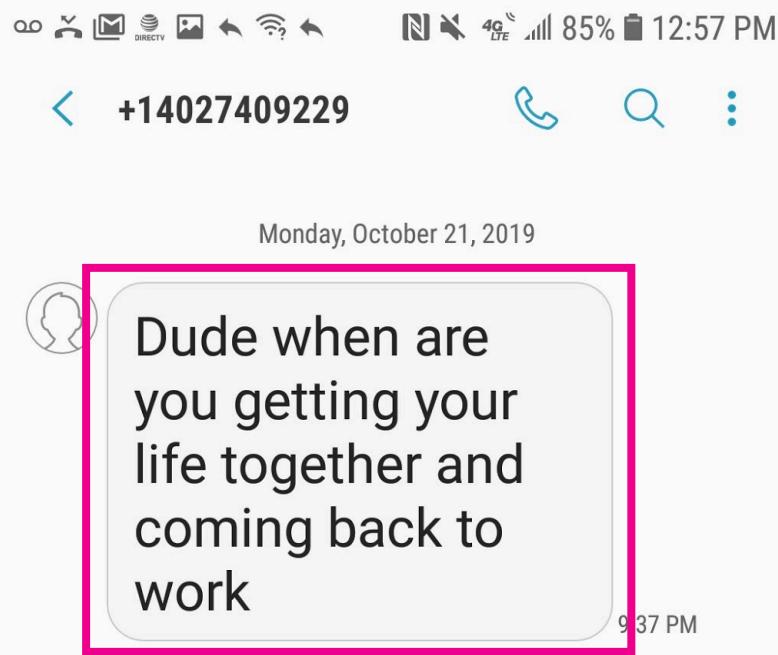
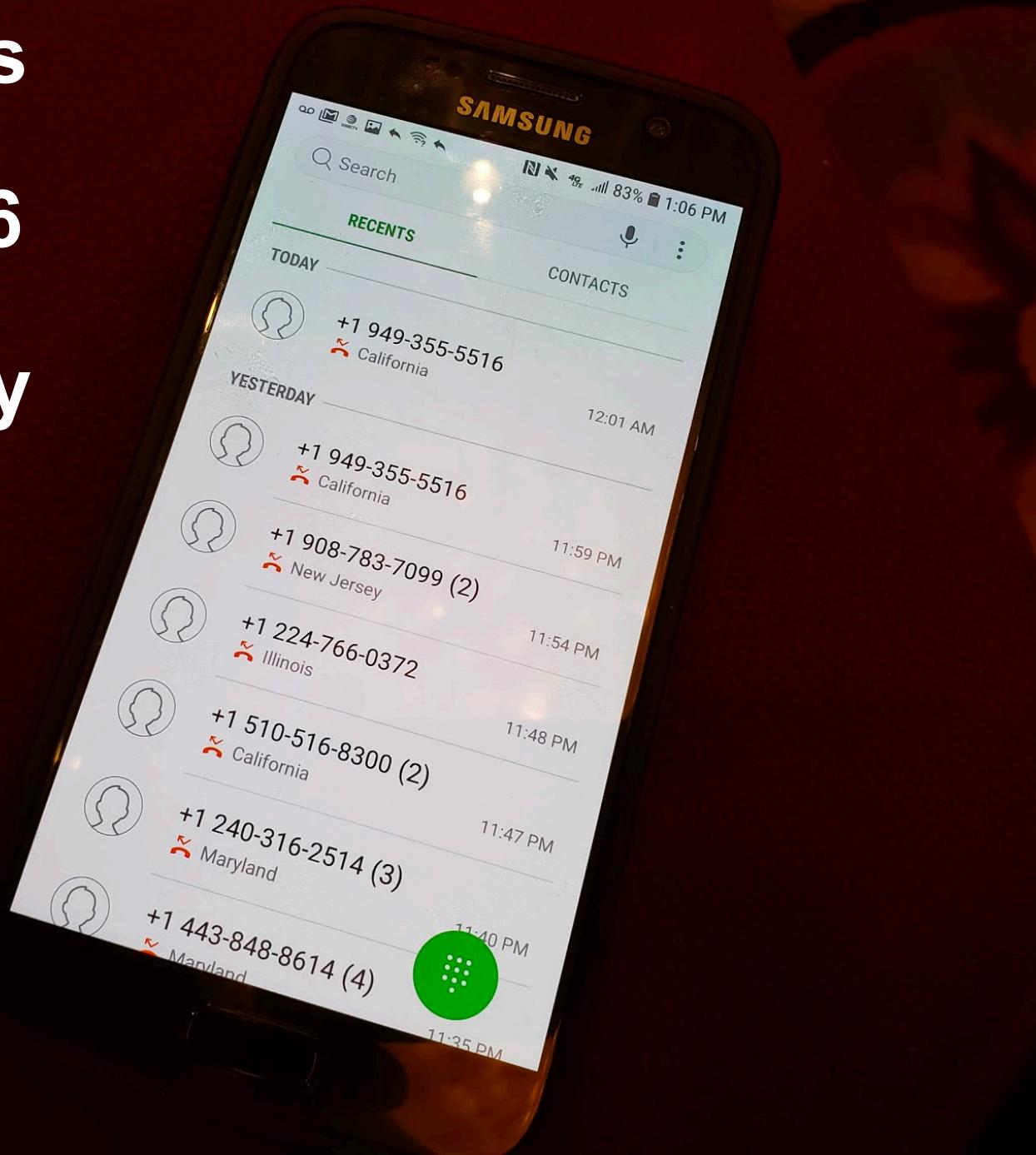
christ alive this question is nebulous

ridiculous

man that was rough

wow...this is hard...lol...more beer

# Mateo's phone rang 86 times Monday night!



Hey....sorry I am WFH today. My Vespa is in the shop. I will return to brew anew 10/24/19 because that's when the parts come back from Italy. Ciao!



Enter message

+

Send

Speaker



RENDER.COM

-M11 100%  
-V1.1  
-V1.2

RENDER.COM

15:40:01

# Advanced Threat Detection

---

UBA IS  
AWESOME!



splunk> User Behavior Analytics

Explore ▾   Analytics ▾   Manage ▾   System ▾

 THREATS <b>11</b>	 ANOMALIES <b>210</b>	 USERS 26 Anomalous 12 All Known 38 All Unknown	 DEVICES 24 Anomalous 43 All Internal 10 All External	 APPS 54 Anomalous 54 All Apps
--	---	---	---	---



## Threats Table

≡ Actions ▾

Any Score ▾

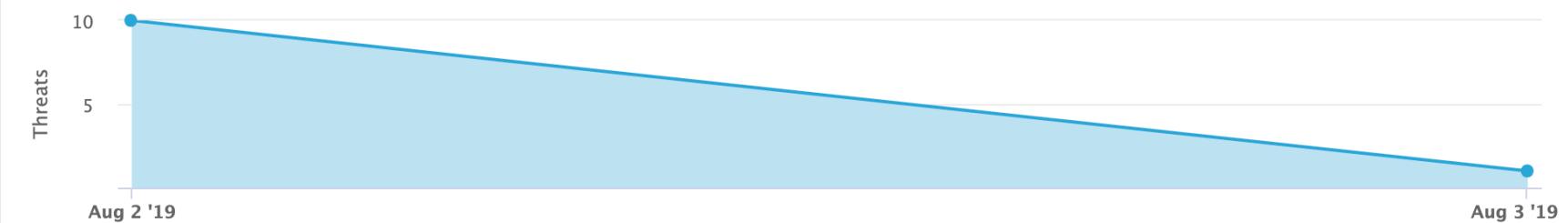
Add Filter ▾

Threats (11)

Search

Group by: Threat Type	
All Threats	11 ▾
Malware	3
Possible Froth.ly Compromised Account	3
Process Initiated from Suspicious Directory	3
Privilege Escalation after Powershell Activity	1
Malware Activity	1

Threats Trend



THREAT TYPE	THREAT CATEGORIES	PARTICIPANTS	LAST ANOMALY DATE	SCORE	⋮
Privilege Escalation after Powershell Activity	Custom	bstoll umfd-6 gravity	Aug 2, 2019 12:00 AM	8	⋮



# Threats Table

Actions ▾
Any Score ▾
Add Filter ▾
**Threats (11)**
Search
Group by: Threat Type ▾

All Threats 11 ▾

Malware 3

Possible Froth.ly Compromised Account 3

**Process Initiated from Suspicious Directory 3**

Privilege Escalation after Powershell Activity 1

Malware Activity 1

Compromised Account 0

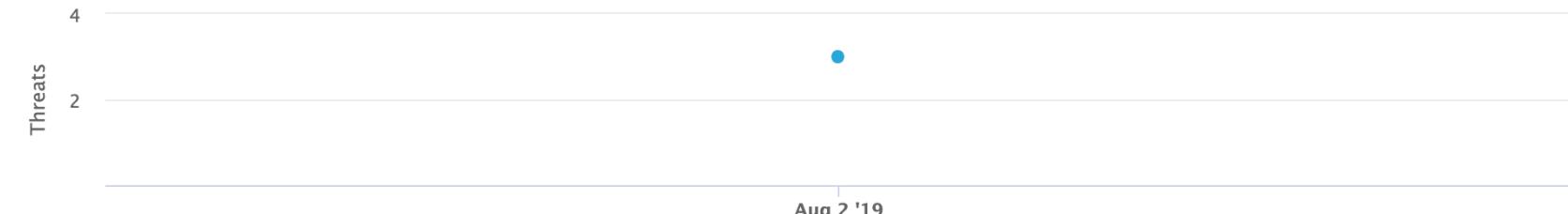
Compromised Web Server 0

Data Exfiltration 0

Data Exfiltration after Account Takeover 0

Data Exfiltration by Compromised 0

## Threats Trend



THREAT TYPE	THREAT CATEGORIES	PARTICIPANTS	LAST ANOMALY DATE	SCORE
Process Initiated from Suspicious Directory	Custom Internal	AudreyGrady agrady-l rdutil.exe sd.exe	Aug 2, 2019 12:00 AM	7
Process Initiated from Suspicious Directory	Custom Internal	frothly_helpdesk agrady-l passkey.exe	Aug 2, 2019 12:00 AM	7
Process Initiated from Suspicious Directory	Custom Internal	svc_print jwotoski-l rdutil.exe	Aug 2, 2019 12:00 AM	7

## Process Initiated from Suspicious Directory 7 »

 Detection Date Sep 20, 2019 1:10 PM Actions

Watchlists Custom Internal

Categories Custom Internal

A process has been executed from a suspicious directory. This could be a temp directory or another unusual location.

<span>Timeline</span>  <b>First Anomaly</b> 12:00 AM Aug 2, 2019  <b>Last Anomaly</b> 12:00 AM Aug 2, 2019	<span>Anomalies (1)</span>  Unusual Windows Security Event (1) <span>3</span>	<span>Users (1)</span>  frothly_helpdesk <span>5</span>	<span>Devices (1)</span>  Internal <span>5</span> agrady-l	<span>Apps (1)</span>  passkey.exe <span>1</span>
--	---	---	---	---

Home / Apps Table / App Details

  passkey.exe   
Last Update Sep 19, 2019 2:21 AM  
Watchlists 

 App Facts

THREATS ANOMALIES  
1 2

Home / Apps Table / App Details

  **passkey.exe**   
**Last Update** Sep 19, 2019 2:21 AM  
Watchlists 

 **App Anomalies**

 **Anomalies (2)**  
 **Unusual Windows Security Event (2)** 

 **Users in Anomalies (1)**  
**frothly\_helpdesk** 

 **Devices in Anomalies (1)**  
**Internal**  
**agrady-l** 

**App Anomalies Timeline**

 **agrady-l (2)**    **frothly\_helpdesk (1)**

Anomaly Types  
Unusual Windows Security Event

 Aug 2 '19

## App Anomalies (2)

Group by: Anomaly Type

All Anomalies	2
Unusual Windows Security Event	2

## Anomalies Trend



ANOMALY TYPE	PARTICIPANTS	SUMMARY	START DATE	SCORE
Unusual Windows Security Event	frothly_helpdesk agrady-l passkey.exe	Found 1 rare value(s) over a period of 30 days. Process.	Aug 2, 2019 12:00 AM	3
Unusual Windows Security Event	agrady-l passkey.exe	Found 1 rare value(s) over a period of 30 days. Process.	Aug 2, 2019 12:00 AM	3



## Unusual Windows Security Event

3

[Actions ▾](#)

Users with unusual Windows Security events.

**Anomaly Creation Time** Sep 20, 2019 2:18 AM

**Last Scored Time** Sep 20, 2019 2:18 AM

**Last Scored by** AnomalyScoringRules

**Event Start Time** Aug 2, 2019 12:00 AM

**Event End Time** Aug 3, 2019 12:00 AM

**Watchlists**



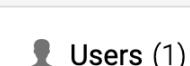
**Categories**

[Active Directory Data](#)[Behavior](#)[Infection](#)[Internal](#)

Found 1 rare value(s) over a period of 30 days.

1. Process [passkey.exe] is uncommon in this environment -- 2 occurrence(s) out of 7.5M. Most commonly observed values (up to top 3) are:

- [taskhostw.exe] occurs 3M time(s) out of 7.5M (**40.3%**)
- [tiworker.exe] occurs 2.3M time(s) out of 7.5M (**30.4%**)
- [svchost.exe] occurs 376K time(s) out of 7.5M (**5.0%**)



Users (1)

frothly\_helpdesk

5



Devices (1)

Internal

agrady-l

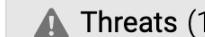
5



Apps (1)

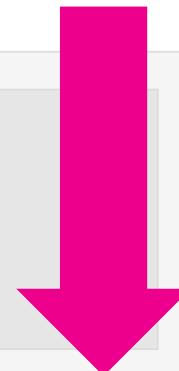
passkey.exe

5



Threats (1)

Process Initiated from Suspicious  
Directory (1)



## Anomaly Details (1)

TARGET ACCOUNT	SOURCE DEVICE	TARGET DEVICE	PROCESS	PROCESS PATH	EVENT DESCRIPTION	RETURN CODE	LOGIN TYPE	EVENT TIME
agrady-l	agrady-l	agrady-l	passkey.exe	c:\windows\system32\printdrv	A new process has been created.			Aug 2, 2019 12:00 AM

## Users That Have the Same Combination of Rare Values Over a Period of 30 Days (1)

This table shows users that have the same combination of rare values.

 frothly\_helpdesk

## Devices That Have the Same Combination of Rare Values Over a Period of 30 Days (1)

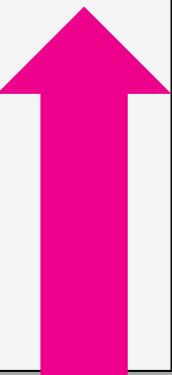
This table shows devices that have the same combination of rare values.

 agrady-l

## Days That Have the Same Combination of Rare Values Over a Period of 30 Days (1)

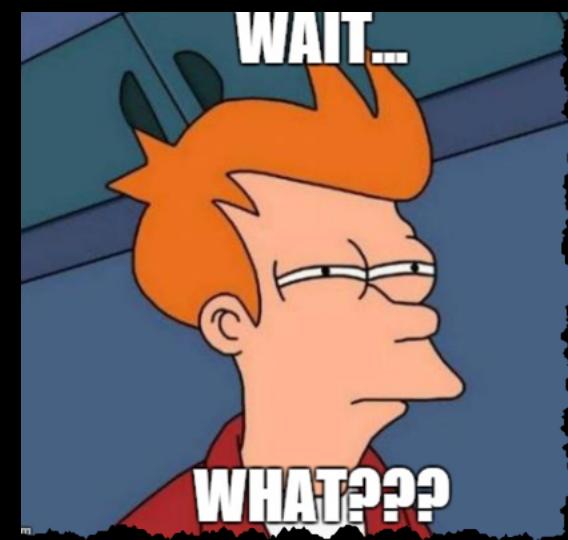
This table shows days that have the same combination of rare values.

Aug 2, 2019 12:00 AM



# What is this suspicious directory?

PROCESS PATH	EVENT DESCRIPTION
c:\windows\system32\printdrv	A new process has been created.





## Unusual Windows Security Event

3

≡ Actions ▾

Users with unusual Windows Security events.

**Anomaly Creation Time** Sep 20, 2019 2:18 AM

**Last Scored Time** Sep 20, 2019 2:18 AM

**Last Scored by** AnomalyScoringRules

**Event Start Time** Aug 2, 2019 12:00 AM

**Event End Time** Aug 3, 2019 12:00 AM

**Watchlists**



**Categories**

Active Directory Data

Behavior

Infection

Internal

Found 1 rare value(s) over a period of 30 days.

1. Process [passkey.exe] is uncommon in this environment -- 2 occurrence(s) out of 7.5M. Most commonly observed values (up to top 3) are:

- [taskhostw.exe] occurs 3M time(s) out of 7.5M (**40.3%**)
- [tiworker.exe] occurs 2.3M time(s) out of 7.5M (**30.4%**)
- [svchost.exe] occurs 376K time(s) out of 7.5M (**5.0%**)

<p><b>Users (1)</b></p> <p>frothly_helpdesk</p> <p>5</p>	<p><b>Devices (1)</b></p> <p>Internal</p> <p>agrady-l</p> <p>5</p>	<p><b>Apps (1)</b></p> <p>passkey.exe</p> <p>5</p>	<p><b>Threats (1)</b></p> <p>Process Initiated from Suspicious Directory (1)</p> <p>7</p>
--	--	--	---

Home / Threats Table / Threat Details / passkey.exe / Anomaly Details / agrady-l

 agrady-l 

Last Update Aug 2, 2019 10:22 PM

Watchlists 

Device Resolution Resolved

## Device Facts

THREATS	ANOMALIES
5	35

IP ADDRESS 10.1.1.100

DEVICE SCOPE Internal

DEVICE TYPE Unknown

IS EXPECTED No

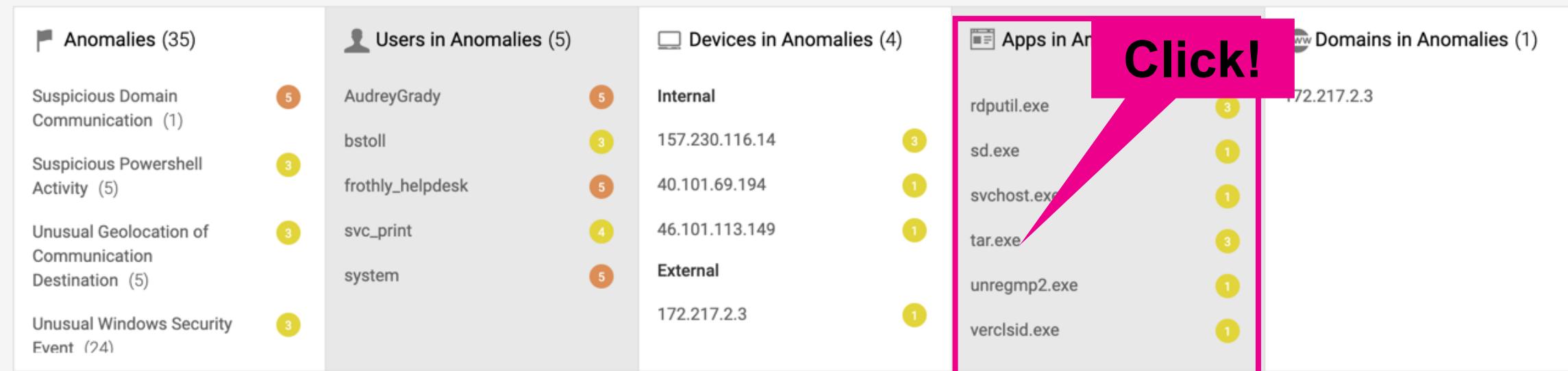
 agrady-l 5  
Last Update Aug 2, 2019 10:22 PM  
Watchlists ★▼  
Device Resolution Resolved

## Device Anomalies

Anomalies (35)	Users in Anomalies (5)	Devices in Anomalies (4)	Apps in Anomalies (14)	Domains in Anomalies (1)
Suspicious Domain Communication (1) <span style="border: 1px solid orange; border-radius: 50%; padding: 2px 5px;">5</span>	AudreyGrady <span style="border: 1px solid orange; border-radius: 50%; padding: 2px 5px;">5</span>	Internal 157.230.116.14 <span style="border: 1px solid yellow; border-radius: 50%; padding: 2px 5px;">3</span>	cmd.exe <span style="border: 1px solid yellow; border-radius: 50%; padding: 2px 5px;">1</span>	172.217.2.3
Suspicious Powershell Activity (5) <span style="border: 1px solid yellow; border-radius: 50%; padding: 2px 5px;">3</span>	bstoll <span style="border: 1px solid yellow; border-radius: 50%; padding: 2px 5px;">3</span>	40.101.69.194 <span style="border: 1px solid yellow; border-radius: 50%; padding: 2px 5px;">1</span>	dccw.exe <span style="border: 1px solid yellow; border-radius: 50%; padding: 2px 5px;">1</span>	
Unusual Geolocation of Communication Destination (5) <span style="border: 1px solid yellow; border-radius: 50%; padding: 2px 5px;">3</span>	frothly_helpdesk <span style="border: 1px solid orange; border-radius: 50%; padding: 2px 5px;">5</span>	46.101.113.149 <span style="border: 1px solid yellow; border-radius: 50%; padding: 2px 5px;">1</span>	fsquirt.exe <span style="border: 1px solid yellow; border-radius: 50%; padding: 2px 5px;">1</span>	
Unusual Windows Security Event (24) <span style="border: 1px solid yellow; border-radius: 50%; padding: 2px 5px;">3</span>	svc_print <span style="border: 1px solid yellow; border-radius: 50%; padding: 2px 5px;">4</span>	External 172.217.2.3 <span style="border: 1px solid yellow; border-radius: 50%; padding: 2px 5px;">1</span>	hostname.exe <span style="border: 1px solid yellow; border-radius: 50%; padding: 2px 5px;">1</span>	
	system <span style="border: 1px solid orange; border-radius: 50%; padding: 2px 5px;">5</span>		locationnotification.exe <span style="border: 1px solid yellow; border-radius: 50%; padding: 2px 5px;">1</span>	
			lsass.exe <span style="border: 1px solid yellow; border-radius: 50%; padding: 2px 5px;">1</span>	

splunk> .conf19

## Device Anomalies



Device Anomalies Relations

# Click!

Home / Threat Table / Threat Details / passkey.exe / Anomaly Details / agrady-l / tar.exe

**tar.exe** 3

Last Update Sep 19, 2019 2:21 AM

Watchlists ★

**App Facts**

THREATS	ANOMALIES
<b>3</b>	<b>4</b>

**App Score Trend**

Date	Score
Sep 19 '19	1
Sep 20 '19	3

Home / Threats Table / Threat Details / passkey.exe / Anomaly Details / agrady-l / tar.exe

**tar.exe** 3

Last Update Sep 19, 2019 2:21 AM

Watchlists ★▼

App Threats

App Threats Timeline

Possible Froth.ly Compromised Account

Threat Types

Aug 2 '19

App Threats (3)

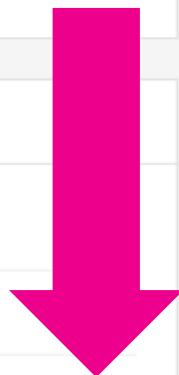
Group by: Threat Type

All Threats 3

Possible Froth.ly Compromised Account 3

Threats Trend

Threats



App Threats (3)

Group by: Threat Type

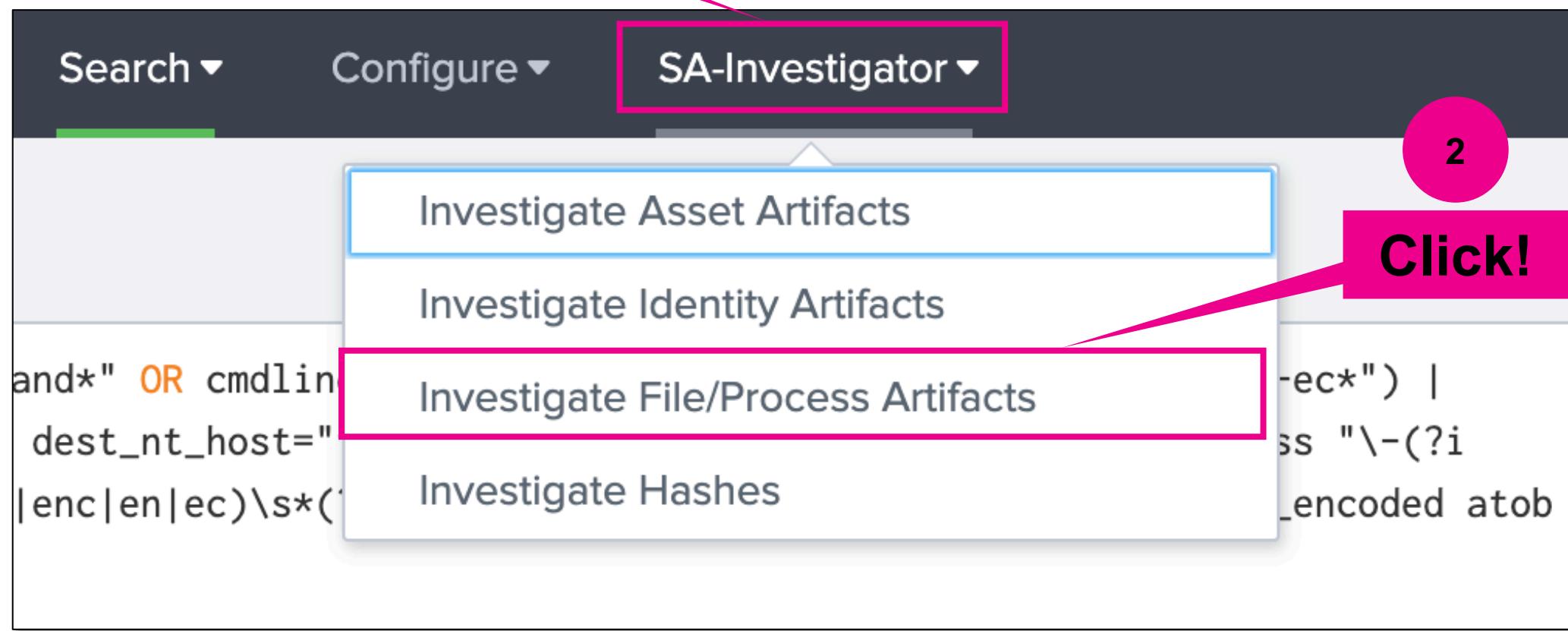
All Threats 3

Possible Froth.ly Compromised Account 3

### Threats Trend

Aug 2 '19

THREAT TYPE	THREAT CATEGORIES	PARTICIPANTS	LAST ANOMALY DATE	SCORE
Possible Froth.ly Compromised Account	Custom Internal	svc_print jwortsaki-l tar.exe	Aug 2, 2019 12:00 AM	7
Possible Froth.ly Compromised Account	Custom Internal	frothly_helpdesk agradyl hostname.exe tar.exe	Aug 2, 2019 12:00 AM	7
Possible Froth.ly Compromised Account	Custom Internal	AudreyGrady agradyl tar.exe	Aug 2, 2019 12:00 AM	7



# Back in ES Asset Investigator

1

2

3

Click!

Click!

Investigations /Process Artifacts

Enter a filename or process name. Index needs to be set for the Details and Search tabs ONLY.

File/Process Name: tar.exe

Destination Host:

User:

Index: main

Time: All time

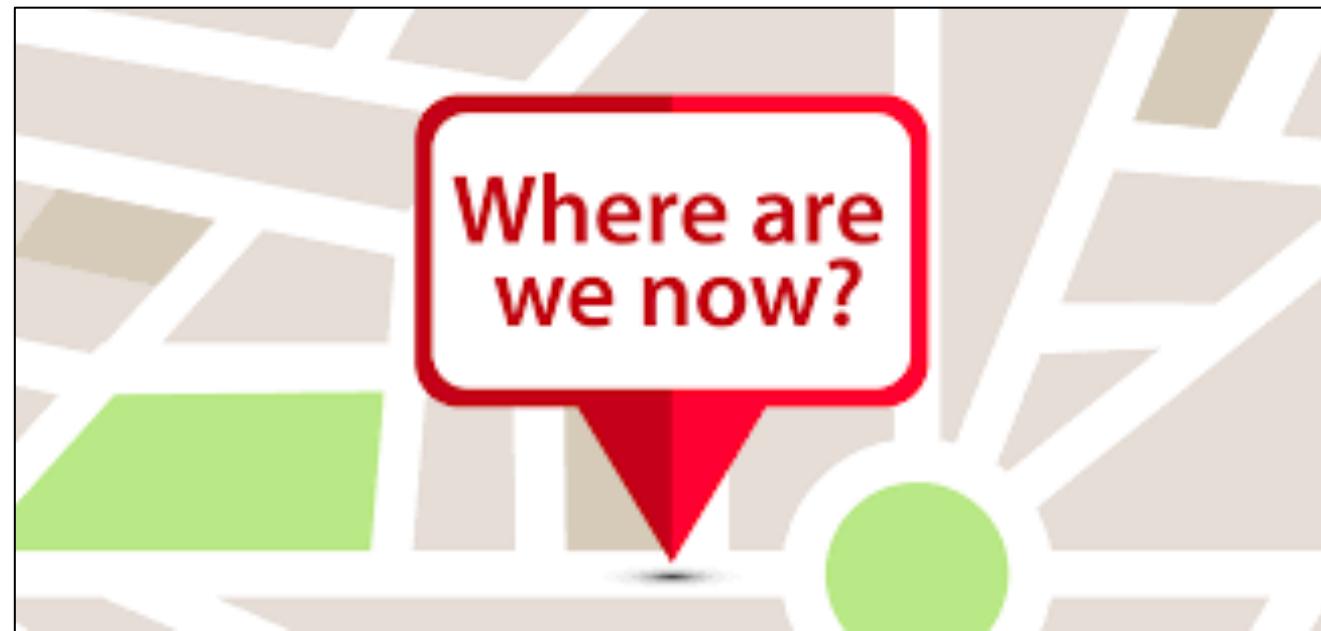
Submit Hide Filters

Details Endpoint Malware Email Threat Indicators Web Windows Process Starts (Event Code 4688) Search

Windows Event Code 4688 Search

_time	host	user	dest	Account_Name	Process	Command Line
2019-08-02 09:00:07	AGRADY-L	-	AGRADY-L.froth.ly	AGRADY-L\$		"c:\windows\system32\tar.exe" -xf printdrv.tar
2019-08-02 09:23:49	JWORTOSKI-L	-	JWORTOSKI-L.froth.ly	JWORTOSKI-L\$		"c:\windows\system32\tar.exe" -xf printdrv.tar
2019-08-02 09:53:11	AGRADY-L	-	AGRADY-L.froth.ly	AGRADY-L\$		tar -czvf leckereien.tar.gz *
2019-08-02 11:23:38	AGRADY-L	-	AGRADY-L.froth.ly	AGRADY-L\$		tar -czvf kennwort.tar.gz *

- ▶ The exe passkey triggered in UBA
- ▶ Threat associated with it due to suspicious location of process (c:\windows\system32\printdrv)
  - agrady-l is the associated workstation
  - frothly\_helpdesk is the associated user
- ▶ Looking further into agrady-l, we see previous IOCs of tar.exe and hostname.exe
- ▶ tar.exe has been used to extract printdrv.tar and create kennwort.tar.gz and leckereien.tar.gz
- ▶ A Google search of kennwort shows it's German for "password"
- ▶ A Google search for leckereien shows it translates to "goodies"



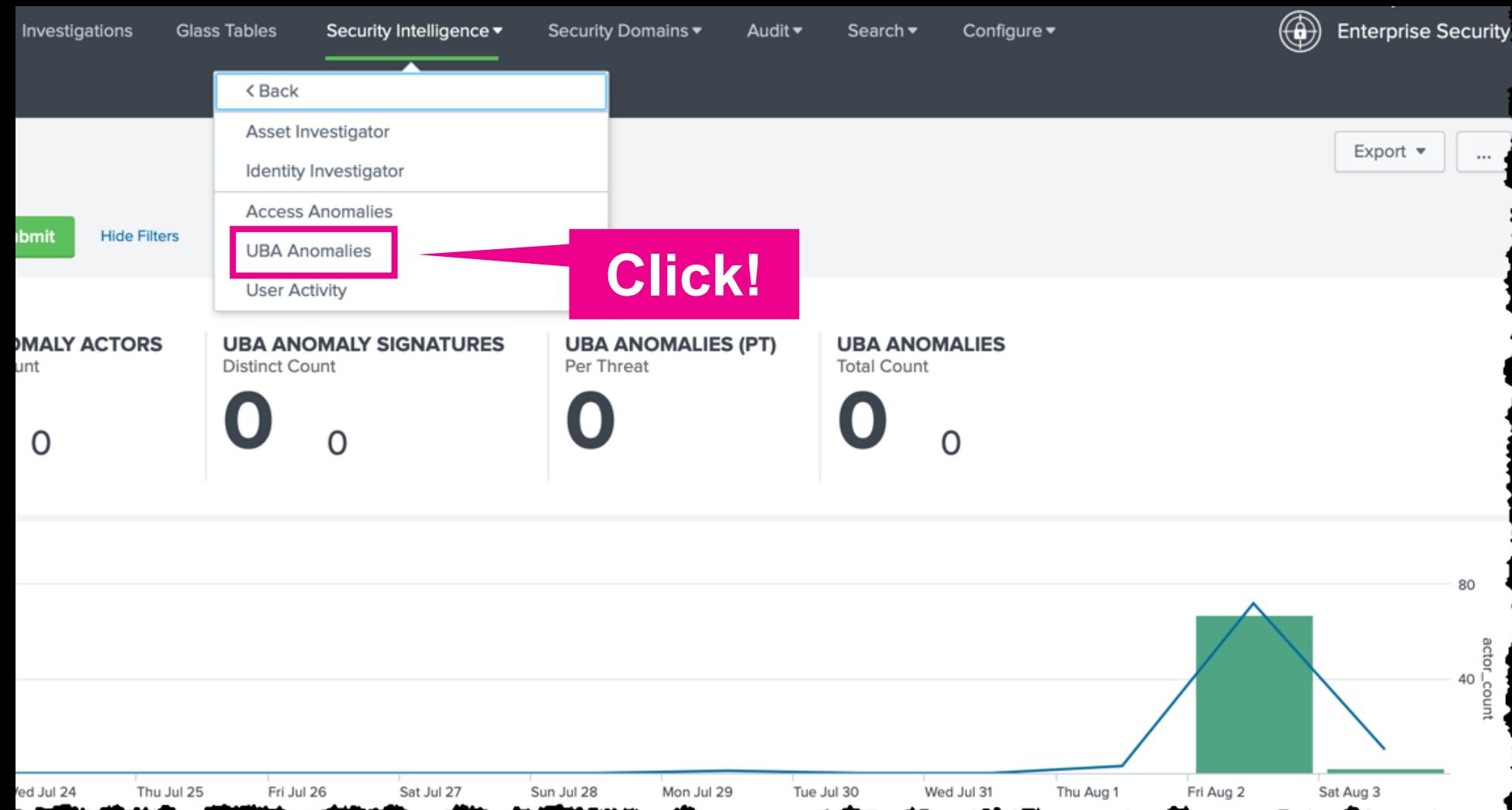
# Anomaly Hunting

---

.conf19  
splunk>



# Start inside Enterprise Security



# How about we find a weird one?

Recent UBA Anomalies								
_time	signature	category	severity	app	dvc	url	user	
2019-08-02		Internal Infection	low	verclsid.exe			mkraeuse-n-1	
2019-08-02		Internal Infection	low	hostname.exe			agraday-1	frothly_helpdesk
2019-08-02		Internal Infection	low	tar.exe			agraday-1	frothly_helpdesk
2019-08-02		Internal Infection	low	sd.exe			agraday-1	AudreyGrady
2019-08-02		Internal Infection	low	prl_vshadow.exe			jwortoski-1	dwm-1
2019-08-02		Internal Infection	low	am_delta_patch_1.299.805.0.exe			fmaltek Esko-1	
2019-08-02		Internal Infection	low	microsoftpdfreader.exe			mvalitus-1	MateoValitus
2019-08-02		Internal	low	cmd.exe			jwortoski-1	JeremiahWortoski
2019-08-02		Internal Infection	low	peopleapp.exe			ghoppy-1	GraceHoppy
2019-08-02		Internal Infection	low	am_delta_patch_1.299.883.0.exe			fmaltek Esko-1	FyodorMalteskesko

< Prev 1 2 3 4 5 6 7 8 9 10

Click!

# Switch to UBA!

splunk > User Behavior Analytics

Explore ▾ Analytics ▾ Manage ▾ System ▾ Scope ▾ bots ▾

Threats Review

Users Review

Analytics Dashboard

THREATS	ANOMALIES	USERS	DEVICES	APPS
11	210	26 Anomalous 12 All Known 38 All Unknown	24 Anomalous 43 All Internal 10 All External	54 Anomalous 54 All Apps

Latest Threats

Malware Activity	Aug 3	4
Malware	Aug 2	7
Privilege Escalation after Powershell Activity	Aug 2	8
Possible Froth.ly Compromised Account	Aug 2	7
Process Initiated from Suspicious Directory	Aug 2	7
Possible Froth.ly Compromised Account	Aug 2	7

Showing all 11 threats

View Details

Threats Timeline (Last 7 Days)

No New Threats

There are no new threats in the last 7 days

Latest Anomalies

Machine Generated Beacon	Aug 3	4
--------------------------	-------	---

Anomalies Timeline (Last 7 Days)

# List those Anomalies!

**Anomalies Table**

Any Score ▾ Add Filter ▾

Anomalies (210)

Group by: Anomaly Type ▾

All Anomalies	210
Unusual Windows Security Event	124
Suspicious Powershell Activity	34
Suspicious Domain Communication	15
Unusual Geolocation of Communication Destination	14
Machine Generated Beacon	9
Unusual Box Activity	7
Excessive Data Transmission	3
Unusual Machine Access	3

**Anomalies Trend**

Apps ▾ sd.exe ▾

ANOMALY TYPE	PARTICIPANTS	SUMMARY	START DATE	SCORE
Unusual Windows Security Event	JeremiahWortoski jwortoski-l tor.exe	Found 1 rare value(s) over a period of 30 days. Process.	Aug 2, 2019 12:00 AM	9
Unusual Windows Security Event	svc_print umfd-1 jwortoski-l	Found 1 rare value(s) over a period of 30 days. Event Description.	Aug 2, 2019 12:00 AM	7
Machine Generated Beacon	PostConf	During 1 hour 26 min and 8 sec	Aug 2, 2019 10:00 PM	6

# SD Anomaly List

ANOMALY TYPE	PARTICIPANTS	SUMMARY	START DATE	SCORE
Unusual Windows Security Event	 agrady-l  sd.exe	Found 1 rare value(s) over a period of 30 days. Process.	Aug 2, 2019 12:00 AM	
Unusual Windows Security Event	 AudreyGrady  agrady-l  sd.exe	Found 1 rare value(s) over a period of 30 days. Process.	Aug 2, 2019 12:00 AM	

Click!

# SD.EXE Details

1. Process [sd.exe] is uncommon in this environment – 3 occurrence(s) out of 7.5M. Most commonly observed values (up to top 3) are:

- [taskhostw.exe] occurs 3M time(s) out of 7.5M (**40.5%**)
- [tiworker.exe] occurs 2.3M time(s) out of 7.5M (**30.6%**)
- [svchost.exe] occurs 368K time(s) out of 7.5M (**4.9%**)

# SD Threats

App Threats (1)

Group by: Threat Type

All Threats 1

Process Initiated from Suspicious Directory 1

Threats Trend

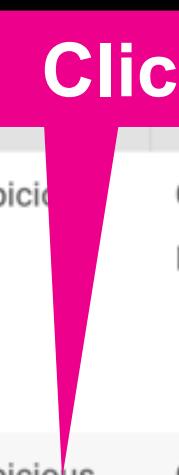
1

Aug 2 '19

Click!

THREAT TYPE	THREAT CATEGORIES	PARTICIPANTS	LAST ANOMALY DATE	SCORE
Process Initiated from Suspicious Directory	Custom Internal	 AudreyGrady  agrady-l  rdutil.exe  sd.exe	Aug 2, 2019 12:00 AM	7

# Rdputil Threats



THREAT TYPE	CATEGORIES	PARTICIPANTS	LAST ANOMALY DATE	SCORE
Process Initiated from Suspicious Directory	Custom Internal	 AudreyGrady  agrady-l  rdputil.exe  sd.exe	Aug 2, 2019 12:00 AM	
Process Initiated from Suspicious Directory	Custom Internal	 svc_print  jwortoski-l  rdputil.exe	Aug 2, 2019 12:00 AM	

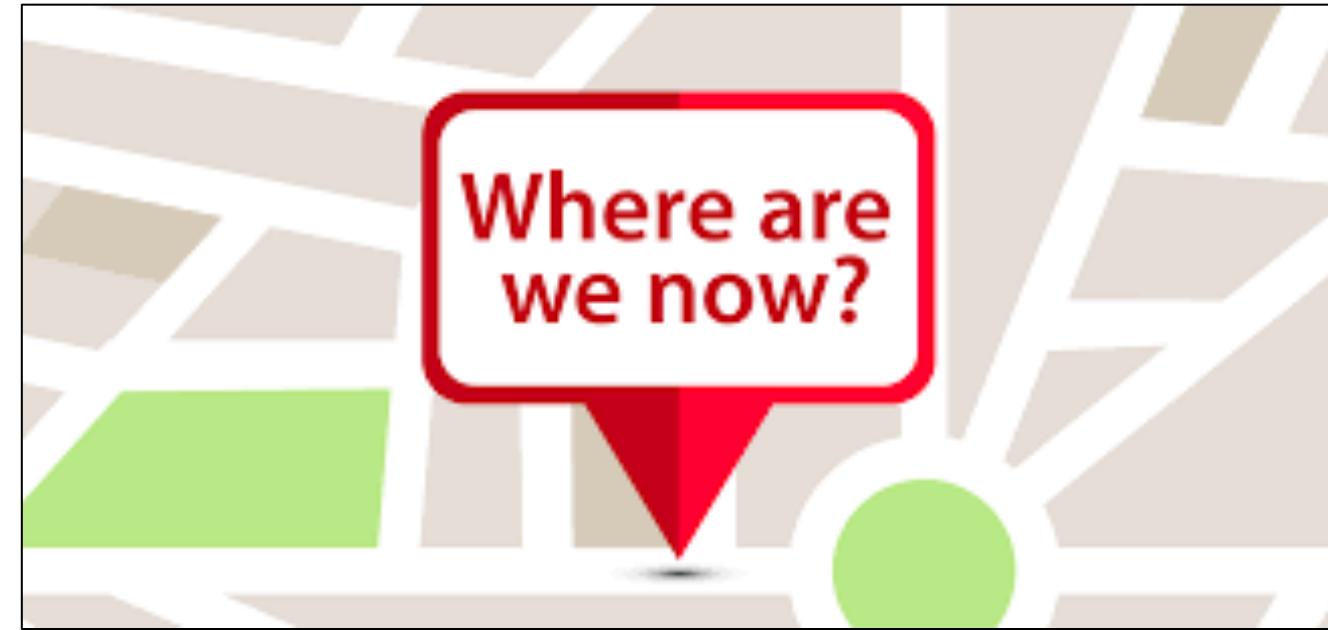
# Wait a second!!!



PROCESS PATH	EVENT DESCRIPTION
c:\windows\system32\printdrv	A new process has been created.



- ▶ sd.exe was executed (unknown executable)
- ▶ rdutil.exe was executed (unknown executable – MS is mstsc.exe)
- ▶ That suspicious directory is C:\Windows\system32\printdrv



Because “C:\Windows\System32\printdrv” is totally a place I would execute files from!!!!

# Rdputil Threats

THREAT TYPE	THREAT CATEGORIES	PARTICIPANTS	LAST ANOMALY DATE	SCORE
Process Initiated from Suspicious Directory	Custom Internal	 AudreyGrady  agrady-l  rdputil.exe  sd.exe	Aug 2, 2019 12:00 AM	7
Process Initiated from Suspicious Directory	Custom Internal	 svc_print  jwortoski-l  rdputil.exe	Aug 2, 2019 12:00 AM	7

Click!

# SVC\_PRINT User Threats



THREAT TYPE	THREAT CATEGORIES	PARTICIPANTS	LAST ANOMALY DATE	SCORE
Possible Froth.ly Compromised Account	Custom Internal	svc_print jwortoski-l tar.exe	Aug 2, 2019 12:00 AM	7
Malware	Custom	6 Users 5 Devices	Aug 2, 2019 12:00 AM	6
Process Initiated from Suspicious Directory	Custom Internal	svc_print jwortoski-l rdputil.exe	Aug 2, 2019 12:00 AM	7
Malware	Custom	4 Users 5 Devices 172.217.2.3	Aug 2, 2019 8:52 AM	7

# Malware Threat

**Malware** 7 »

**Detection Date** Sep 19, 2019 6:01 PM    **Last Update** Sep 20, 2019 1:07 PM

**Watchlists** ★▼

**Categories** Custom

A host on your network may have been compromised and is displaying suspicious activity consistent with a malware infection.

**Timeline**

**First Anomaly**  
12:00 AM  
Aug 2, 2019

**Last Anomaly**  
08:52 AM  
Aug 2, 2019

**Duration**  
8h 52m

**Anomalies (11)**

- Suspicious Domain Communication (1) 5
- Suspicious Powershell Activity (5) 3
- Unusual Geolocation of Communication Destination (5) 3

**Users (4)**

- AudreyGrady
- frothly\_helpdesk
- svc\_print
- system

**Devices (5)**

- 40.101.69.194
- 46.101.113.149
- agrady-l
- External

**Domains (1)**

- 172.217.2.3

Click!

**Threat Relations**

```

graph LR
    AG[AudreyGrady] --- SD[Suspicious Domain Communication]
    AG --- F[frothly_helpdesk]
    SD --- D1[172.217.2.3]
    SD --- D2[www 172.217.2.3]
    
```

splunk> .conf19

# Oh this isn't good...

ANOMALY TYPE	PARTICIPANTS	SUMMARY	START DATE	SCORE
Suspicious Powershell Activity	💻 agrady-l	Detected risky PowerShell behavior	Aug 2, 2019 12:00 AM	3
Suspicious Powershell Activity	👤 system 💻 agrady-l	Detected risky PowerShell behavior	Aug 2, 2019 12:00 AM	3
Suspicious Powershell Activity	👤 AudreyGrady 💻 agrady-l	Detected risky PowerShell behavior	Aug 2, 2019 12:00 AM	2
Suspicious Powershell Activity	👤 svc_print 💻 agrady-l	Detected risky PowerShell behavior	Aug 2, 2019 12:00 AM	3
Suspicious Powershell Activity	👤 frothly_helpdesk 💻 agrady-l	Detected risky PowerShell		

**Command Executed by the user (1)**

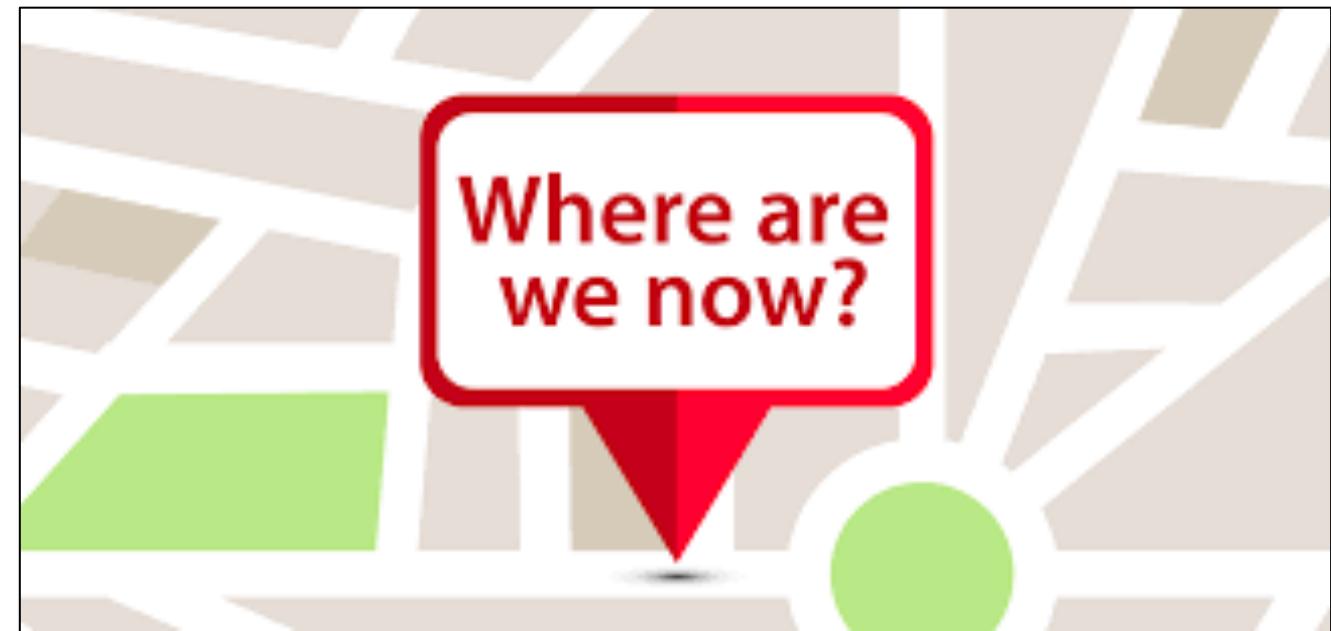
Command Executed by the user

```
powershell -ec
LgBcAHMAbQBiAC4AZQB4AGUAIABcAFwAdABpAHQAYQBuACAAwBtAGQAIAAvAGMAIABjADoAX
AB3AGkAbgBkAG8AdwBzAFwAcwB5AHMAdABIAG0AMwAyAFwAcwBjAGgAdAbhAHMAawBzACAA
LwBjAHIAZQBhAHQAZQAgAC8AcgB1ACAAJwBOAFQAIABBAFUAVABIAE8AUgBJAFQAWQBcAFMA
WQBTAFQARQBNACcAIAAvAHQAbgAgAE0AaQBjAHIAbwBzAG8AZgB0AFwAVwBpAG4AZABvAHcA
cwBcAFAAcgBpAG4AdABpAG4AZwBcAFAAcgBpAG4AdABEAHIAaQB2AGUAcgBVAHAAZABhAHQA
ZQAgAC8AcwBjACAAbwBuAGwAbwBnAG8AbgAgAC8AdAByACAAJwBwAG8AdwBIAHIAcwBoAGUA
bABsACAALQB3ACAAaAAGAEMA0gBcAFcAaQBuAGQAbwB3AHMAXABTAhkAcwB0AGUAbQAzADI
AXABwAHIAaQBuAHQAZAByAHYAXABwAHIAaQBuAHQAZAByAHYALgBwAHMAMQAnAA==
```

# Decrypted PS Commands

```
.\smb.exe \\titan cmd /c net group 'Domain Admins' daffligem /ADD /DOMAIN  
  
.\smb.exe \\titan cmd /c c:\windows\system32\schtasks /create /ru 'NT AUTHORITY\SYSTEM' /tn  
Microsoft\Windows\Printing\PrintDriverUpdate /sc onlogon /tr 'powershell -w h C:\Windows\System32\printdrv\printdrv.ps1'  
  
ntdsutil  
  
Stop-Service UmR*  
  
c:\windows\system32\schtasks /change /tn 'Microsoft\Windows\SharedPC\Account Cleanup' /enable /tr 'powershell  
c:\windows\system32\printdrv\msfont.ps1'
```

- ▶ sd.exe was executed (unknown executable)
- ▶ rdutil.exe was executed (unknown executable – MS is mstsc.exe)
- ▶ That suspicious directory is C:\Windows\system32\printdrv
- ▶ **NEW**
- ▶ svc\_print user is involved in a bunch of threats/anomalies
- ▶ svc\_print apparently executed encrypted powershell commands
- ▶ Those encrypted PS commands were malicious and involved scheduled tasks



# Where do we go from here?

- ▶ svc\_print account should be disabled
- ▶ sd.exe should be removed
- ▶ rdputil.exe should be removed
- ▶ msfont.ps1 which was a scheduled task? Yah, that was meterpreter
- ▶ printdrv.ps1 is the beaconing software out to imperialstout.org

# Best/Worst Practices

---

NOT Mike Dupuis



# Quick Synopsis

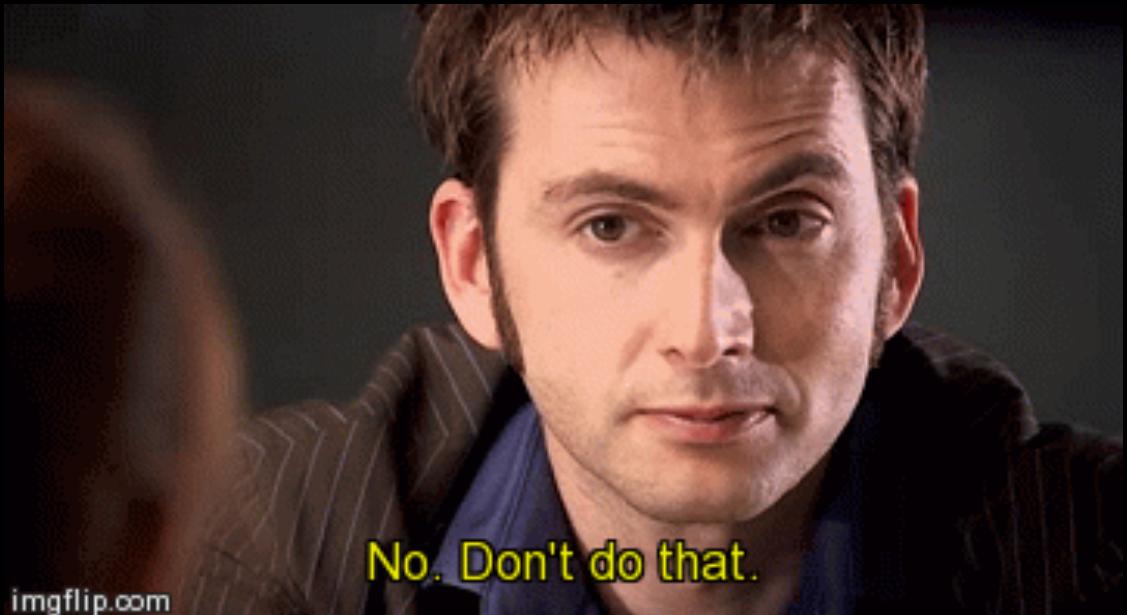
## ► Each Section Here

- First Slide: Bad things we've seen in the field
- Subsequent Slides: How to combat those things

1. Pre-everything!
2. Architecture
3. Usage

# Pre-Installation

These are things NOT to do...

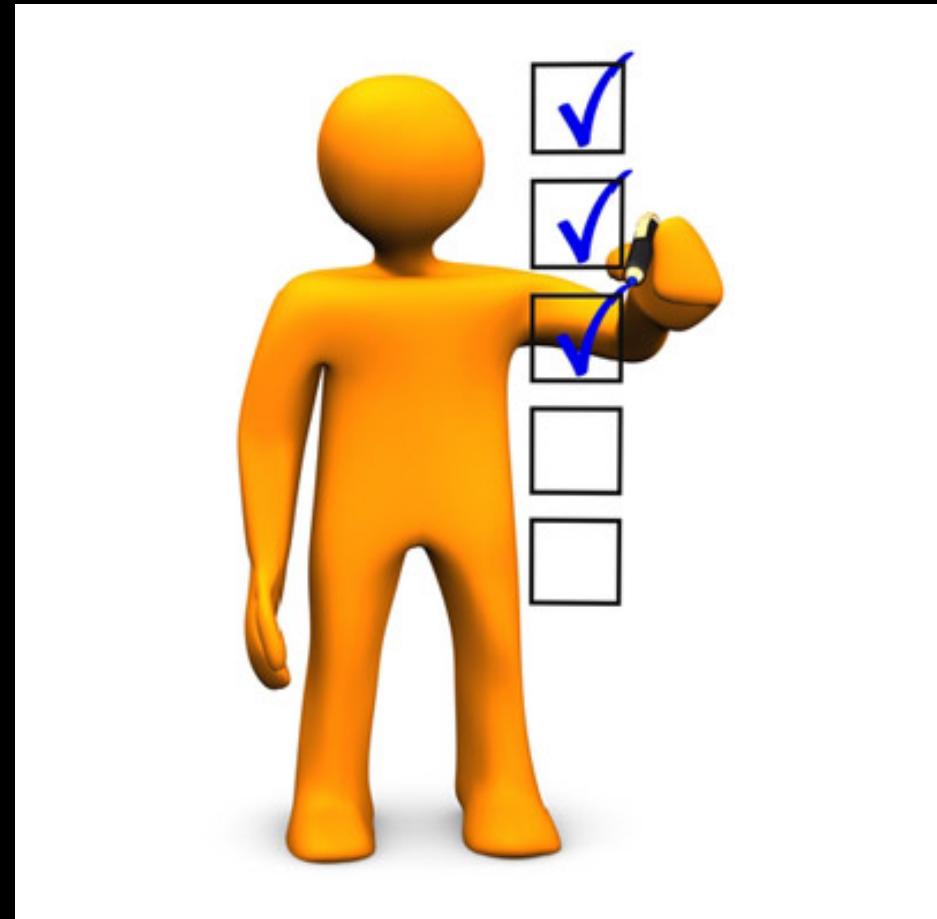


- ▶ Size UBA for 1000 accounts when there's 15,000 accounts
- ▶ Assure us all data is CIM compliant and on-boarded into Splunk
- ▶ IOPS of 800? No problem!
- ▶ Limit data or decrease logging
- ▶ Block basic networking ports (80/443)
  
- ▶ Need UBA because it's UBA!

# Best Practices

Meet all the pre-requisites

- ▶ Indexed Real Time Required
- ▶ DHCP, Windows Security Logs, Proxy, and Firewall required
- ▶ DNS is preferred
- ▶ Asset information
- ▶ IOPS at 1200+
- ▶ Network ports open
- ▶ Use cases well defined
- ▶ For more information:  
<https://docs.splunk.com/Documentation/UBA/latest/Install/Requirements>



# Architecture

What not to do!

- ▶ When sized at 10 servers, create 12
- ▶ Install on shared infrastructure (VM)
- ▶ Try to install on AIX, Windows, SELinux Kernel, or one of the other 20 different distributions that aren't supported
- ▶ Just add some extra servers for HA/DR
- ▶ Position your UBA cluster in a data center across the country from your Splunk installation



# Architecture



- ▶ Size appropriately! More on next slide
- ▶ Used dedicated resources (CPU and Memory)
- ▶ Install on approved and supported OSes
- ▶ Follow docs for HA/DR:  
<https://docs.splunk.com/Documentation/UBA/latest/Admin/WarmStandby>
- ▶ Try to place your UBA install as close to Splunk as Possible! Network latency is a thing!

# Best Practices

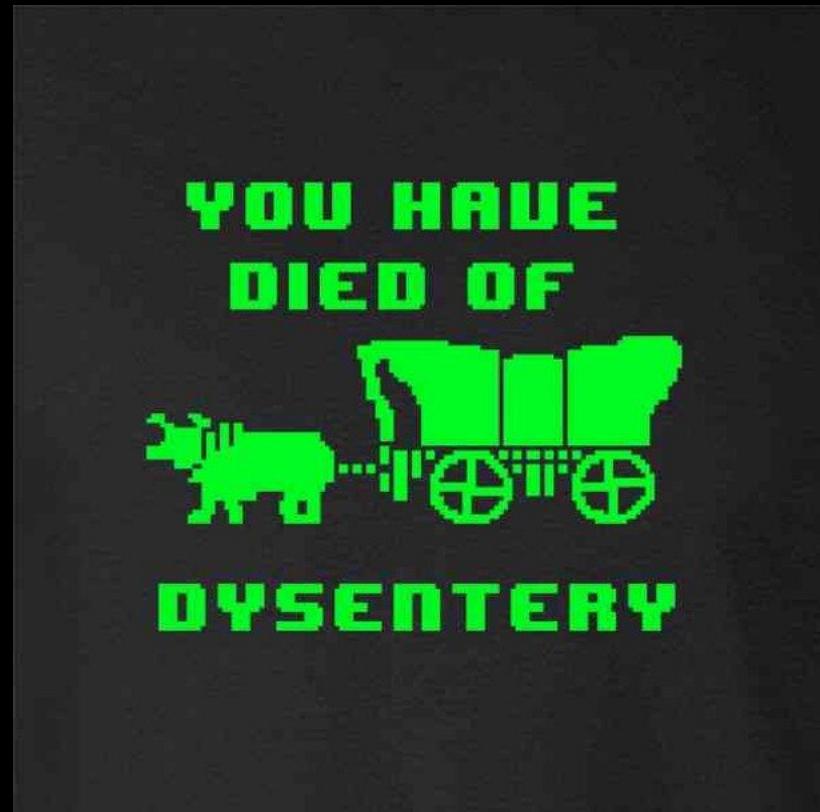
## Sizing and Configuration

Size of cluster	Max events per second capacity	Number of accounts	Number of devices
1	4K	up to 50K	up to 100K
3	12K	up to 50K	up to 200K
5	20K	up to 200K	up to 300K
7	28K	up to 350K	up to 500K
10	40K-45K	up to 350K	up to 500K
20	75K-80K	up to 750K	up to 1 Million

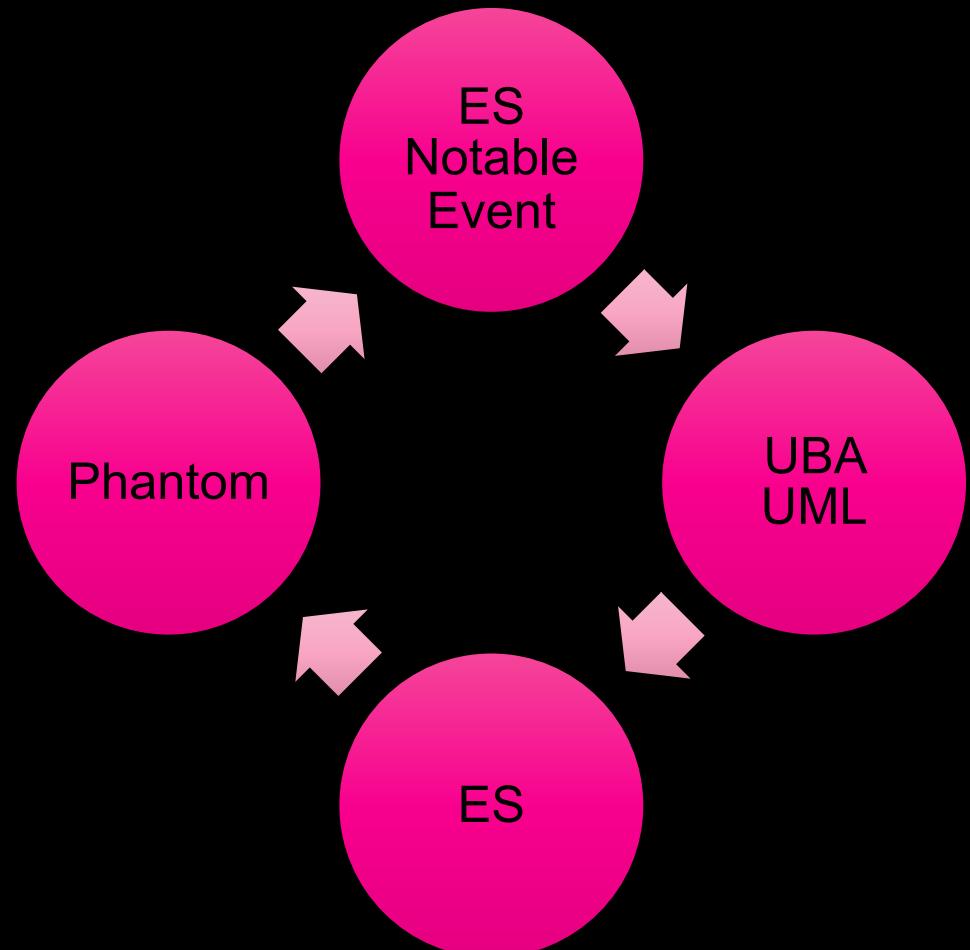
- ▶ Sizing exercise with your Splunk SME to verify data load
- ▶ 16 Core/64 RAM is set – throwing 96 cores at it will not affect data processing
- ▶ 50 GB/1 TB/1 TB drives are required – SSD preferred
- ▶ AMI and OVA are available

# Usage

- ▶ Try to replace ES and SSE with UBA
- ▶ Creating a bunch of basic rule searches inside of UBA
- ▶ Trying to integrate everything in UBA that you already have integrated in Splunk
- ▶ Treat UBA as a stand-alone platform in your environment



# Usage



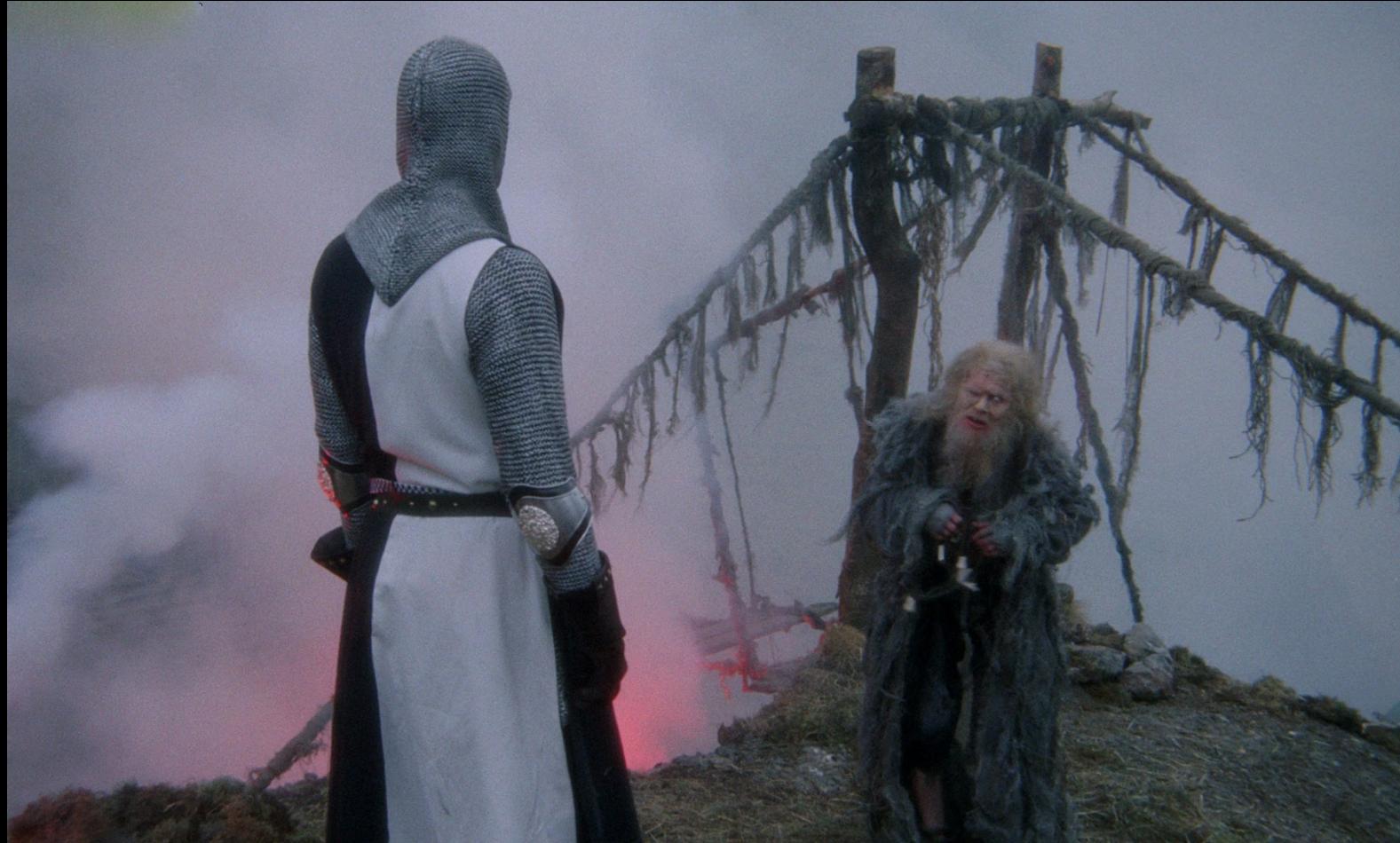
- ▶ Pull in correlation notable events from ES
- ▶ Send anomalies back to ES and the ES risk framework – see RBA deck for more!
- ▶ Send threats back to ES as notable events
- ▶ Reactions and responses to UBA data should be done through Splunk
- ▶ Take the online training!
- ▶ Use in conjunction with SSE, ES, and Phantom!

# Where to go from here?

- ▶ Product Page: [https://www.splunk.com/en\\_us/software/user-behavior-analytics.html](https://www.splunk.com/en_us/software/user-behavior-analytics.html)
- ▶ UBA White Papers
  - <https://www.splunk.com/pdfs/product-briefs/splunk-uba.pdf>
  - <https://www.splunk.com/pdfs/technical-briefs/using-splunk-uba-to-detect-cyber-attacks.pdf>
  - <https://www.splunk.com/pdfs/technical-briefs/using-splunk-uba-to-detect-insider-threats.pdf>
- ▶ UBA Demo – reach out to your Splunk rep!
- ▶ UBA Test Drive – reach out to your Splunk rep!
- ▶ Coming soon!!!! – Threat Hunting on UBA Workshop v4 (new year)

# Ask me anything!

Well, not anything, it should be about Splunk or UBA



.conf19<sup>®</sup>

splunk>

Thank  
You!

Go to the .conf19 mobile app to

**RATE THIS SESSION**