Advanced Threat Hunting and Anomaly Detection with Splunk UBA

Tom Smit
Staff Sales Engineer | Splunk

splunk> .conf19

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.

#whoami

Tom Smit

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…

.conf19

splunk>

BOSS of the SOC

Premium

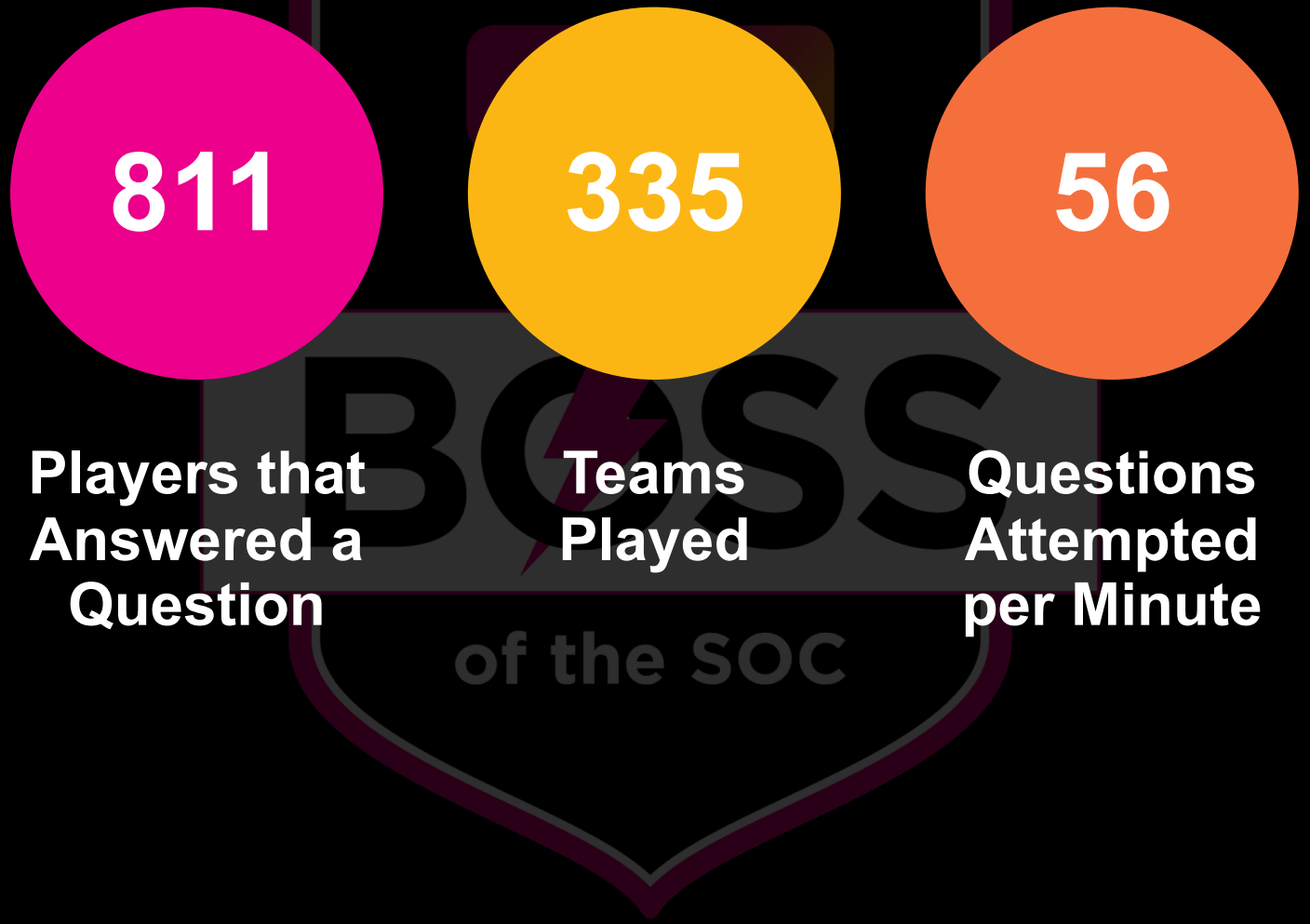
FROTHLY

Quality

Thirsty Berner Brewery


splunk>
splunk>
splunk>
13
12

How Big Was BOTS?



Question Stats!

17548

Question Attempts

10601

Correct Answers

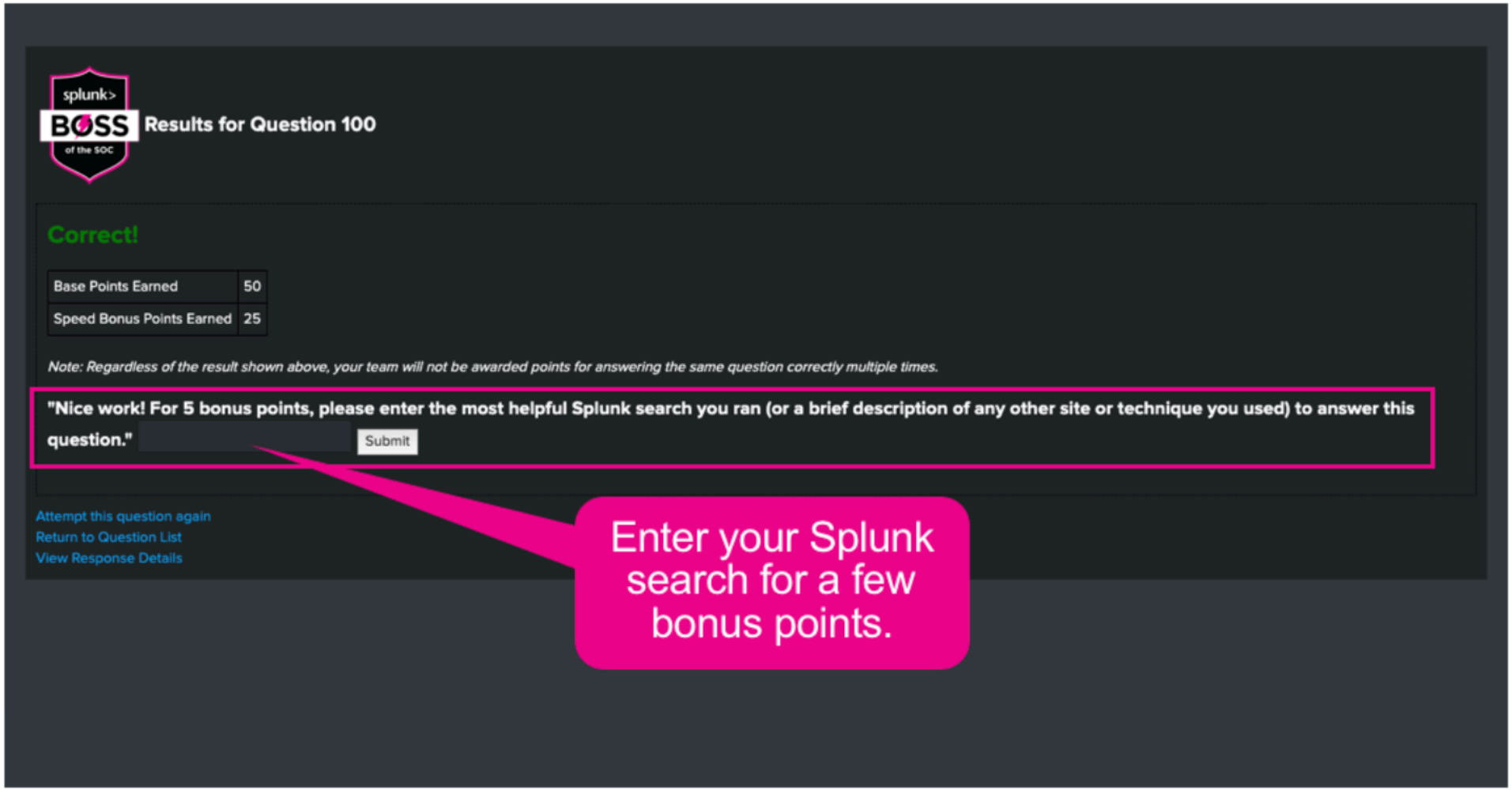
6947

Incorrect Answers

3873

Hints Purchased

A Little Something Extra …



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

christ alive this question is nebulous

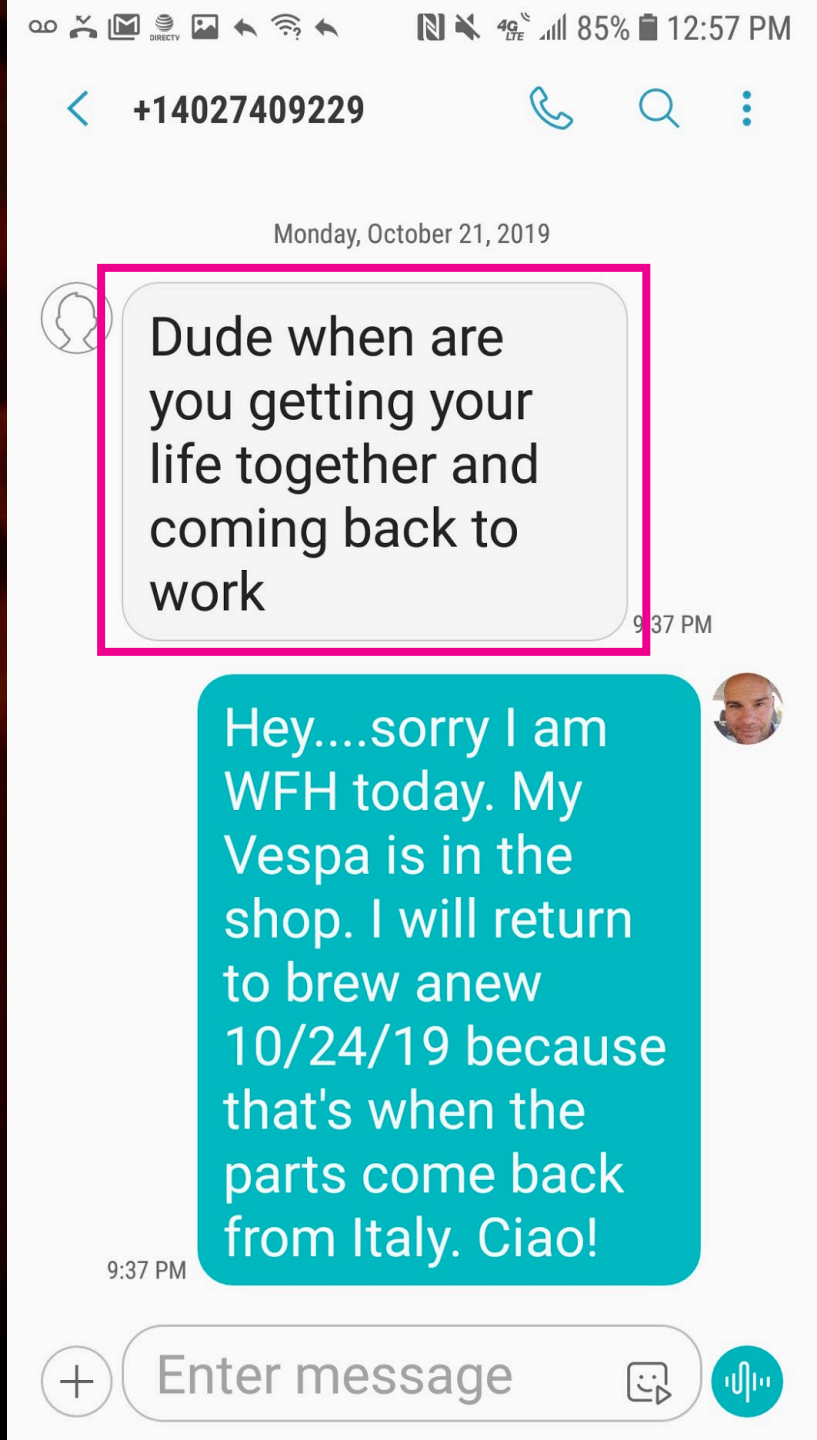
i know this song
i like cake
i like this uba thing

ridiculous

man that was rough

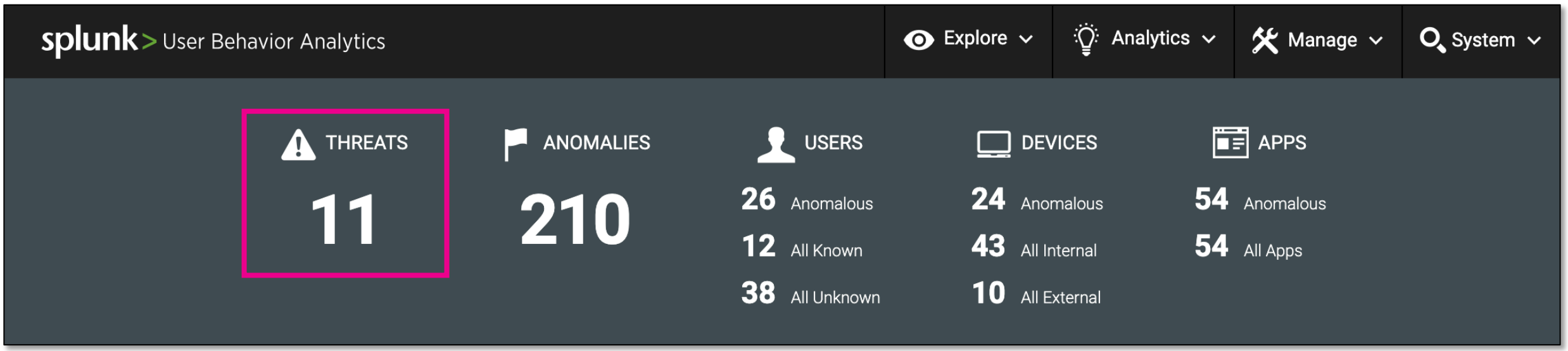
wow...this is hard...lol...more beer

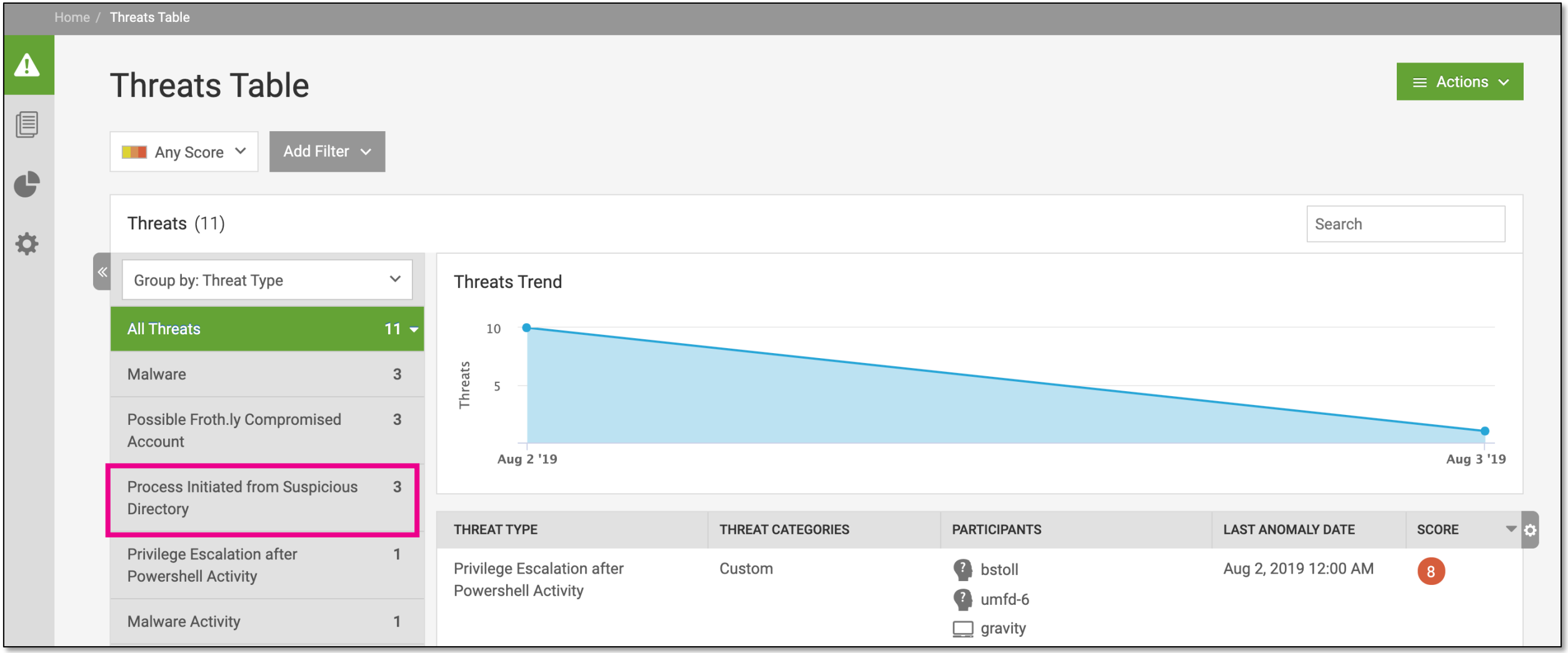
Mateo's phone rang 86 times Monday night!



Advanced Threat Detection

.conf19
splunk>





Threats Table

Actions

Any Score | Add Filter

Threats (11)

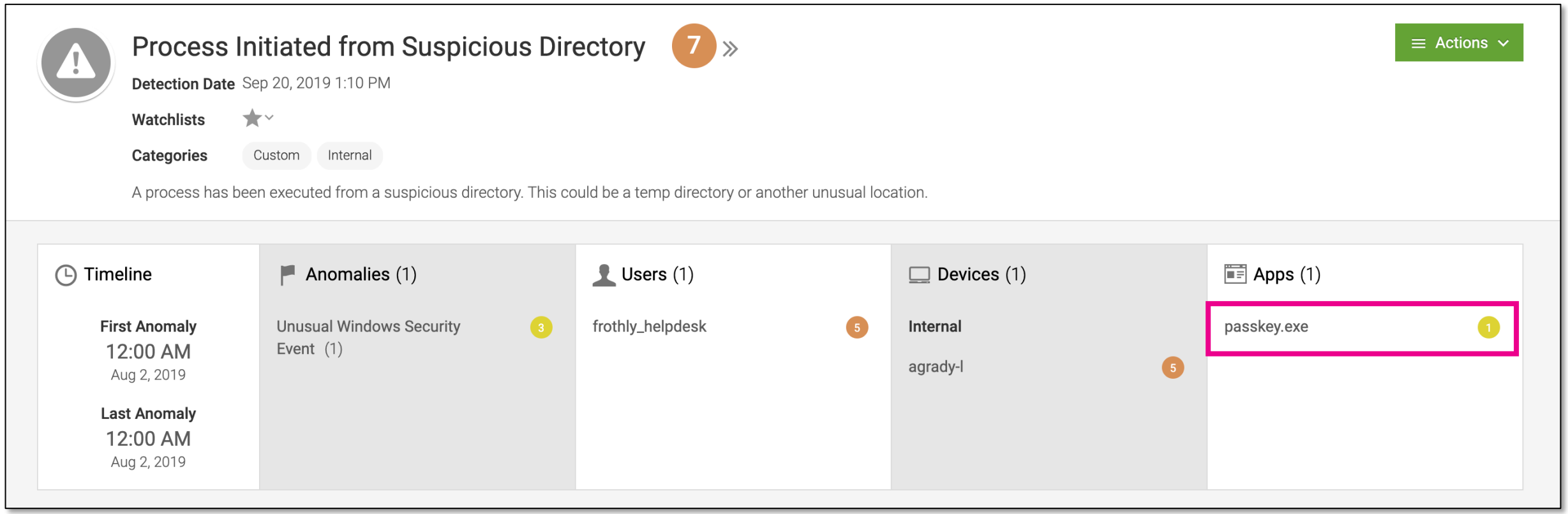
Search

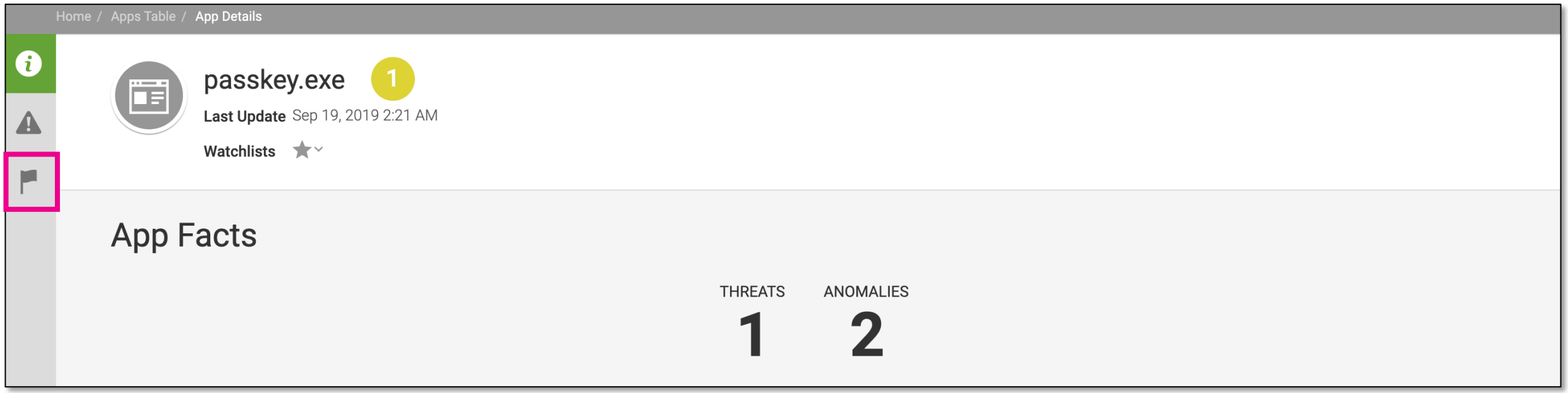
Group by: Threat Type

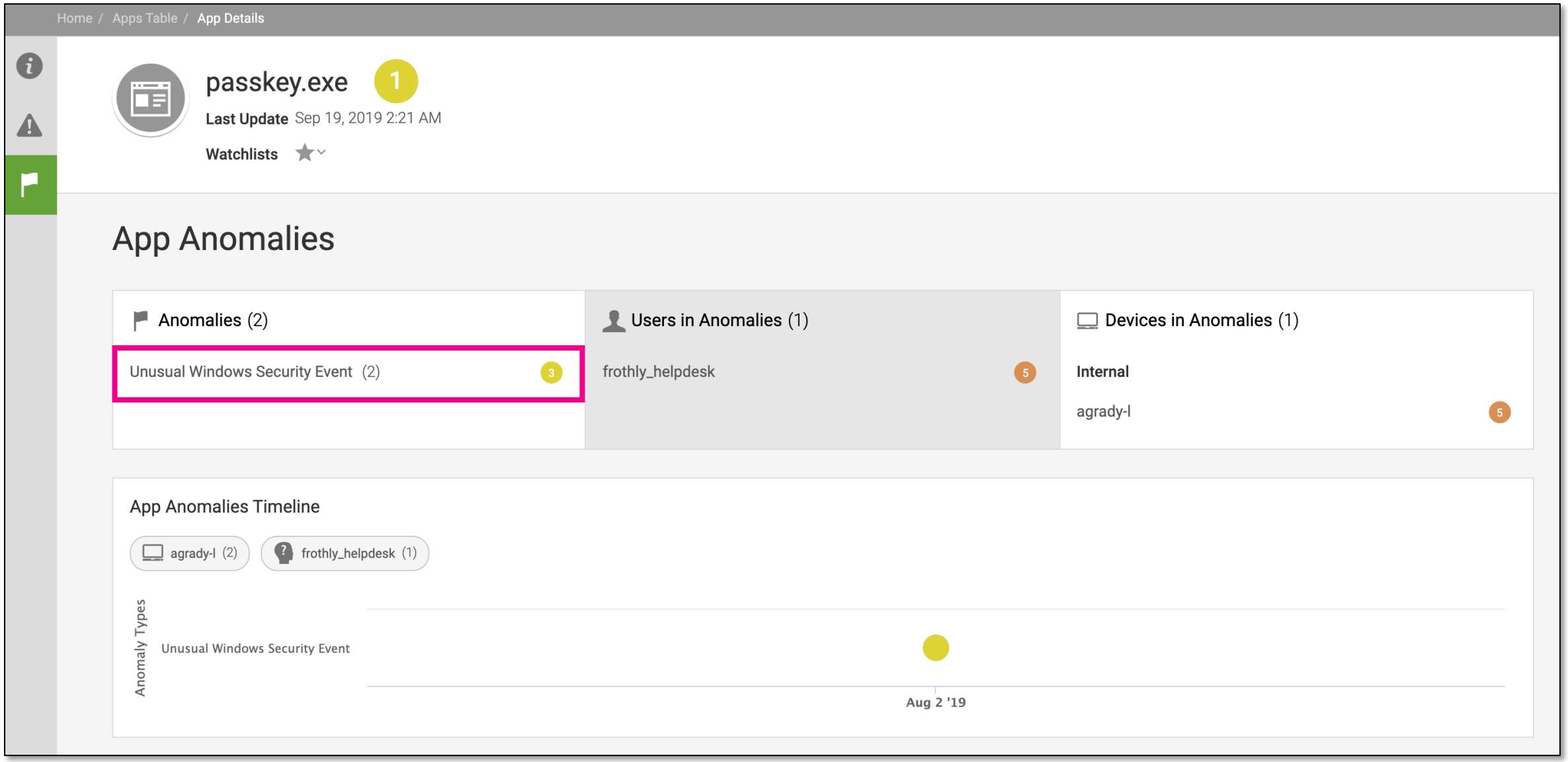
All Threats	11
Malware	3
Possible Froth.ly Compromised Account	3
Process Initiated from Suspicious Directory	3
Privilege Escalation after Powershell Activity	1
Malware Activity	1
Compromised Account	0
Compromised Web Server	0
Data Exfiltration	0
Data Exfiltration after Account Takeover	0
Data Exfiltration by Compromised	0

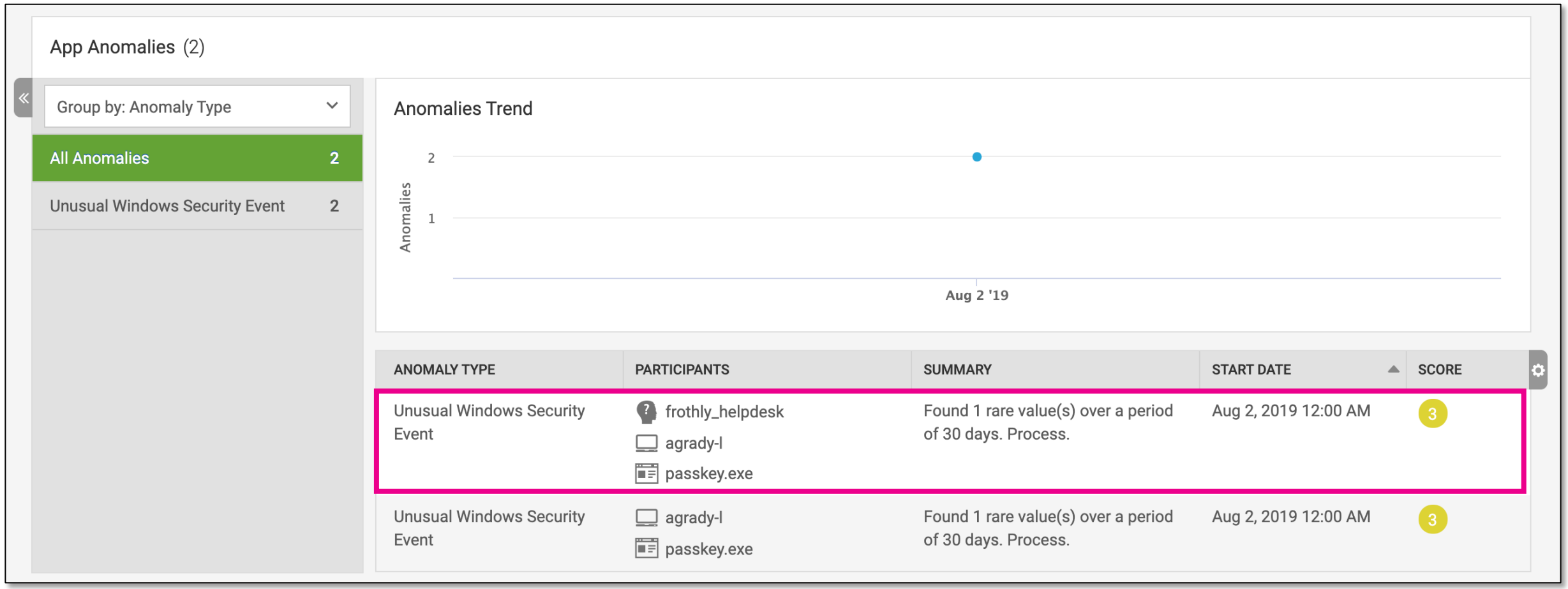
Threats Trend

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









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)	Devices (1)	Apps (1)	Threats (1)
frothly_helpdesk 5	**Internal**	passkey.exe 1	Process Initiated from Suspicious Directory (1)
	agrady-l 5		

Anomaly Details (1)

TARGET ACCOUNT	SOURCE DEVICE	TARGET DEVICE	PROCESS	PROCESS PATH	EVENT DESCRIPTION	RETURN CODE	LOGIN TYPE	EVENT TIME
	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)

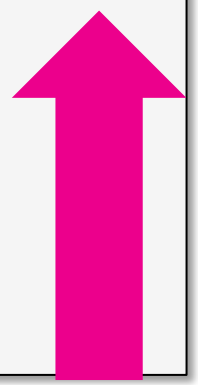
This table shows devices that have the same combination of rare values.

agrady-l

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

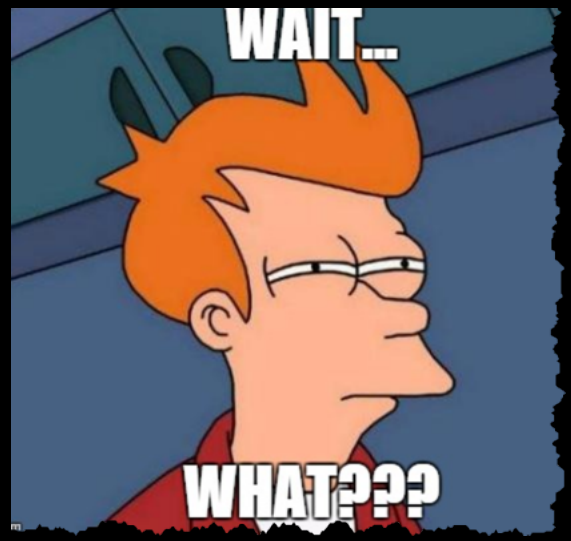
This table shows days that have the same combination of rare values.

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

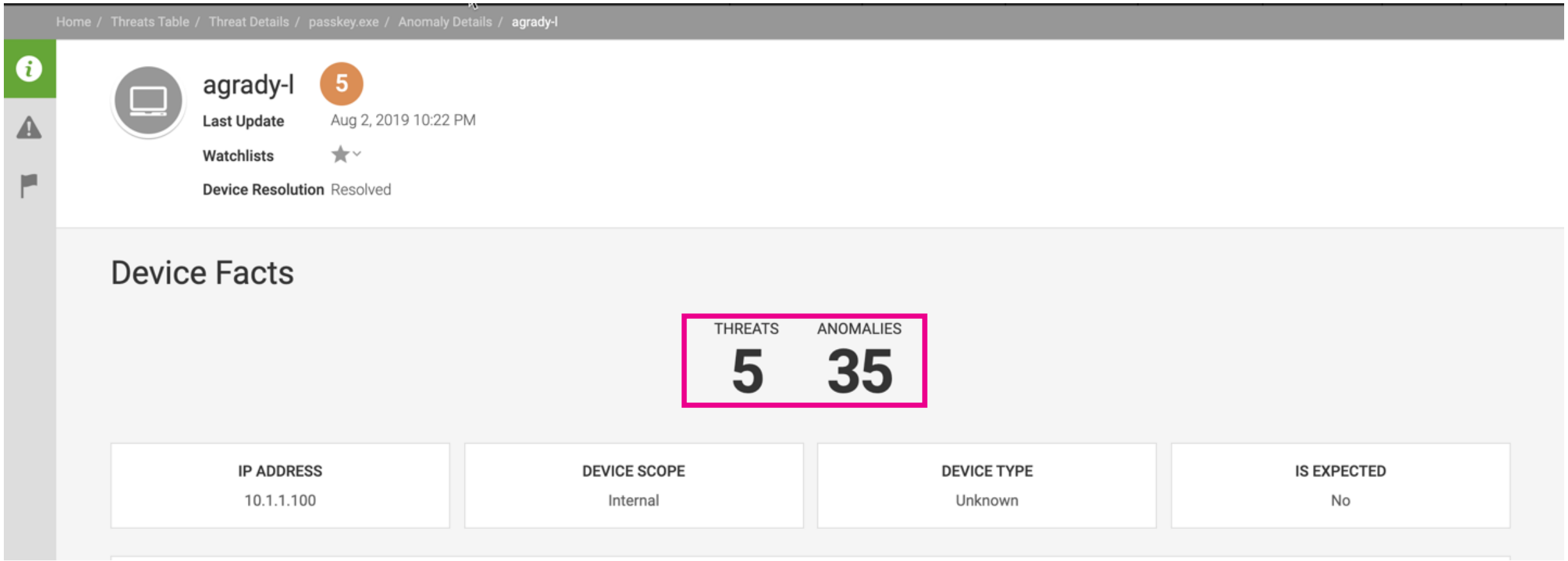
Watchlists

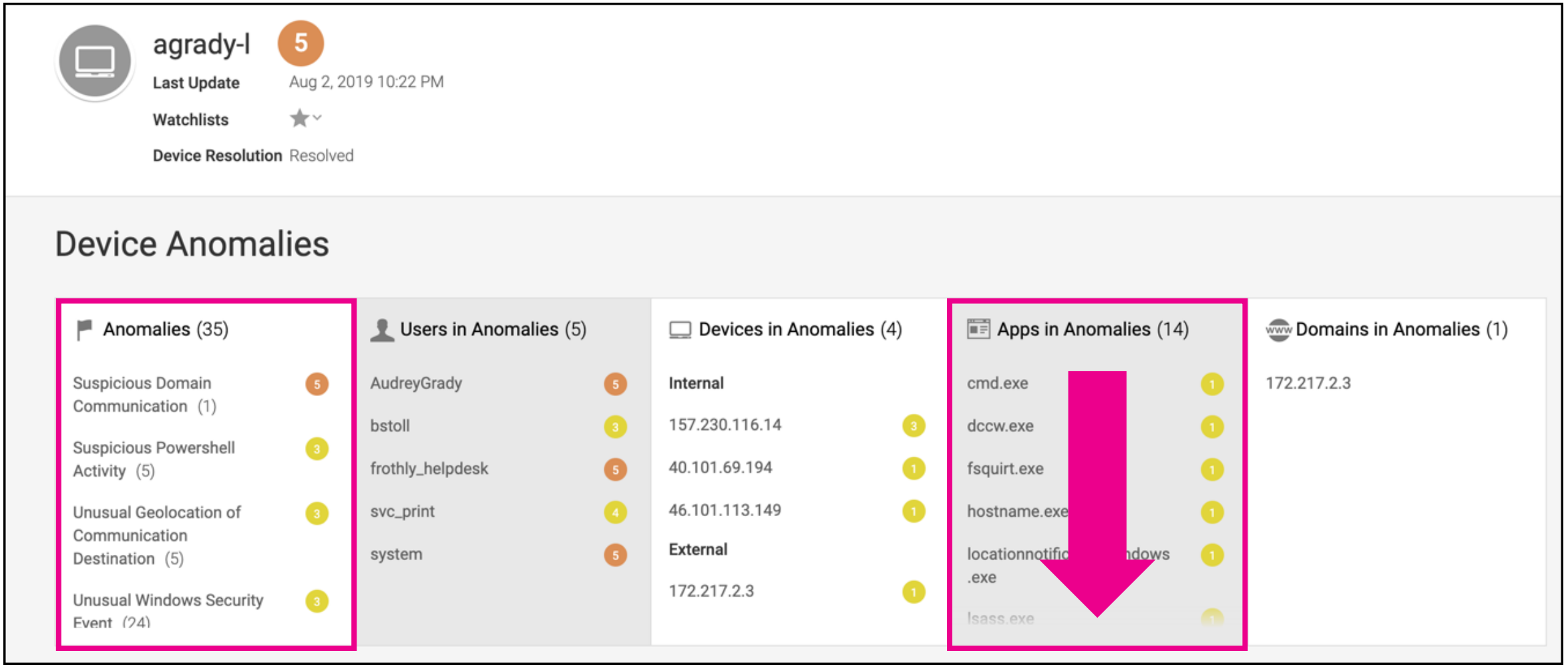
Categories Active Directory Data | Behavior | Infection | Internal

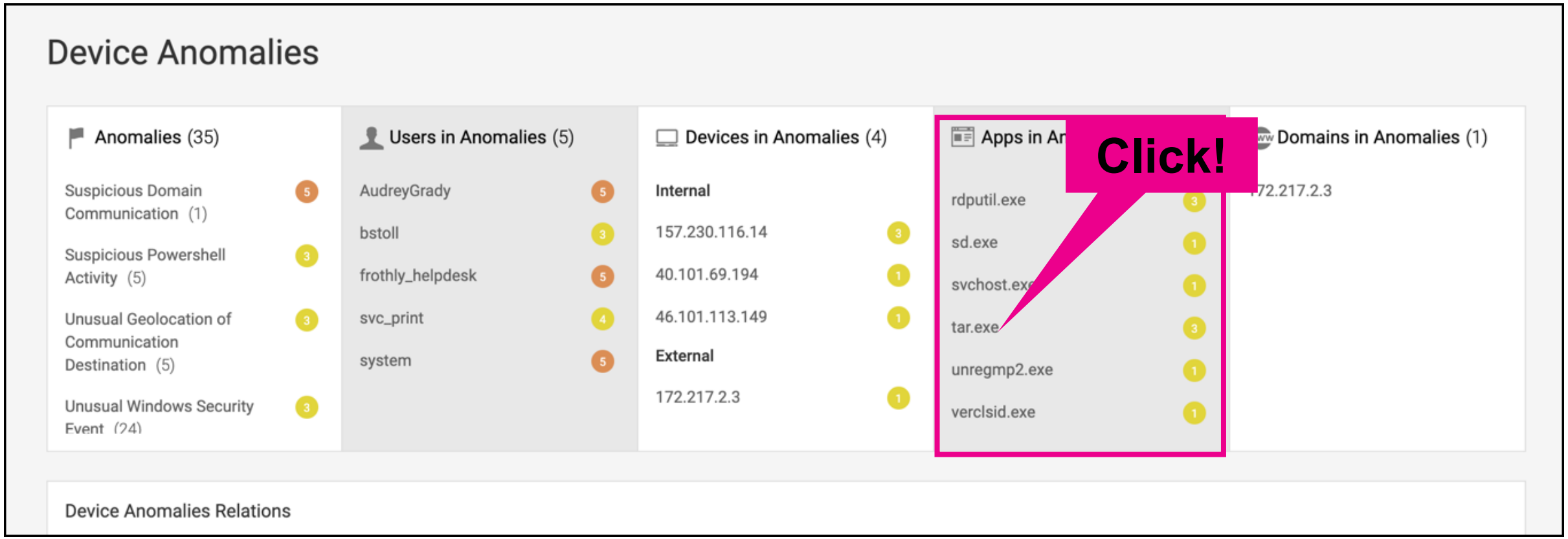
Found 1 rare value(s) over a period of 30 days.

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%**)

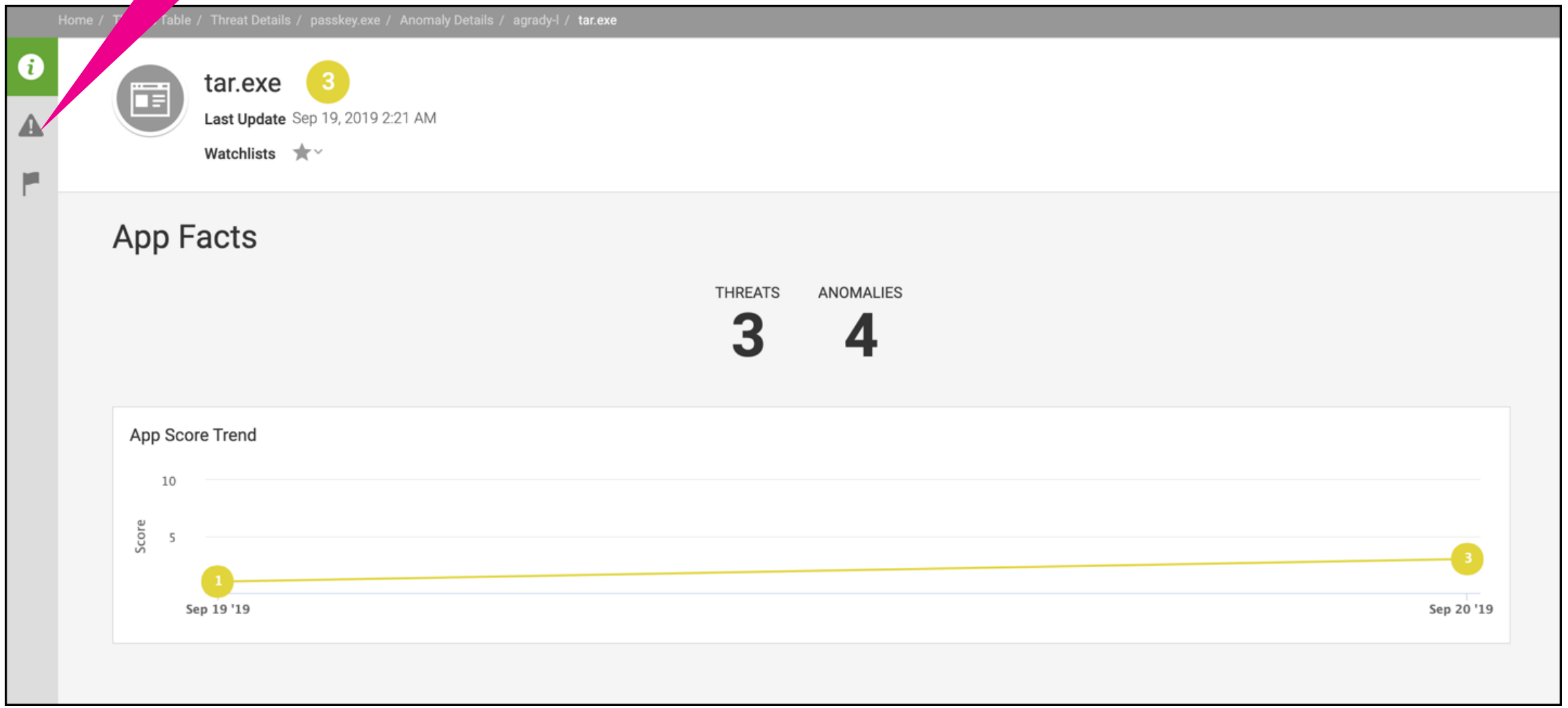
Users (1)	Devices (1)	Apps (1)	Threats (1)
frothly_helpdesk 5	**Internal**	passkey.exe 1	Process Initiated from Suspicious Directory (1) 7
	agrady-l 5		

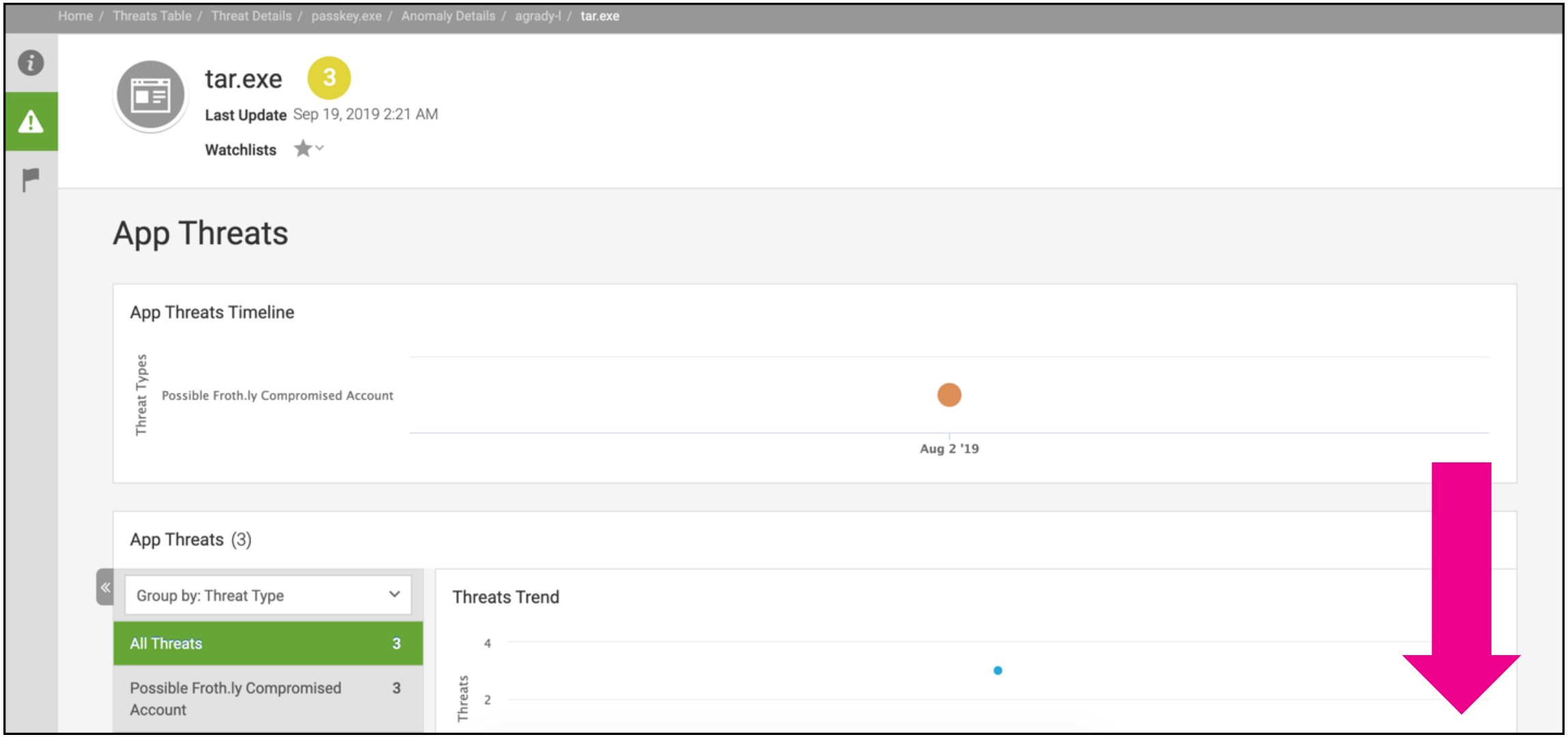


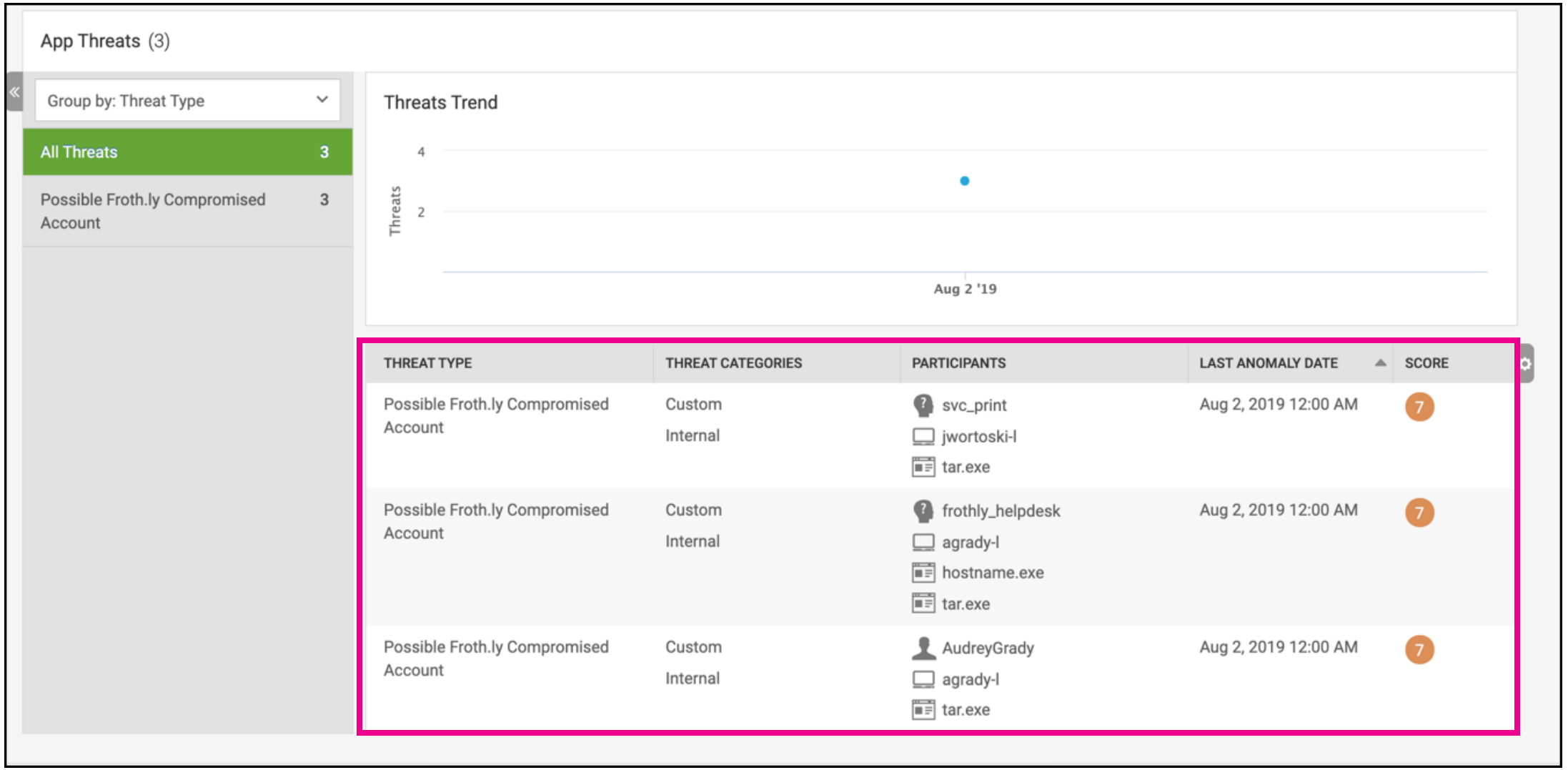




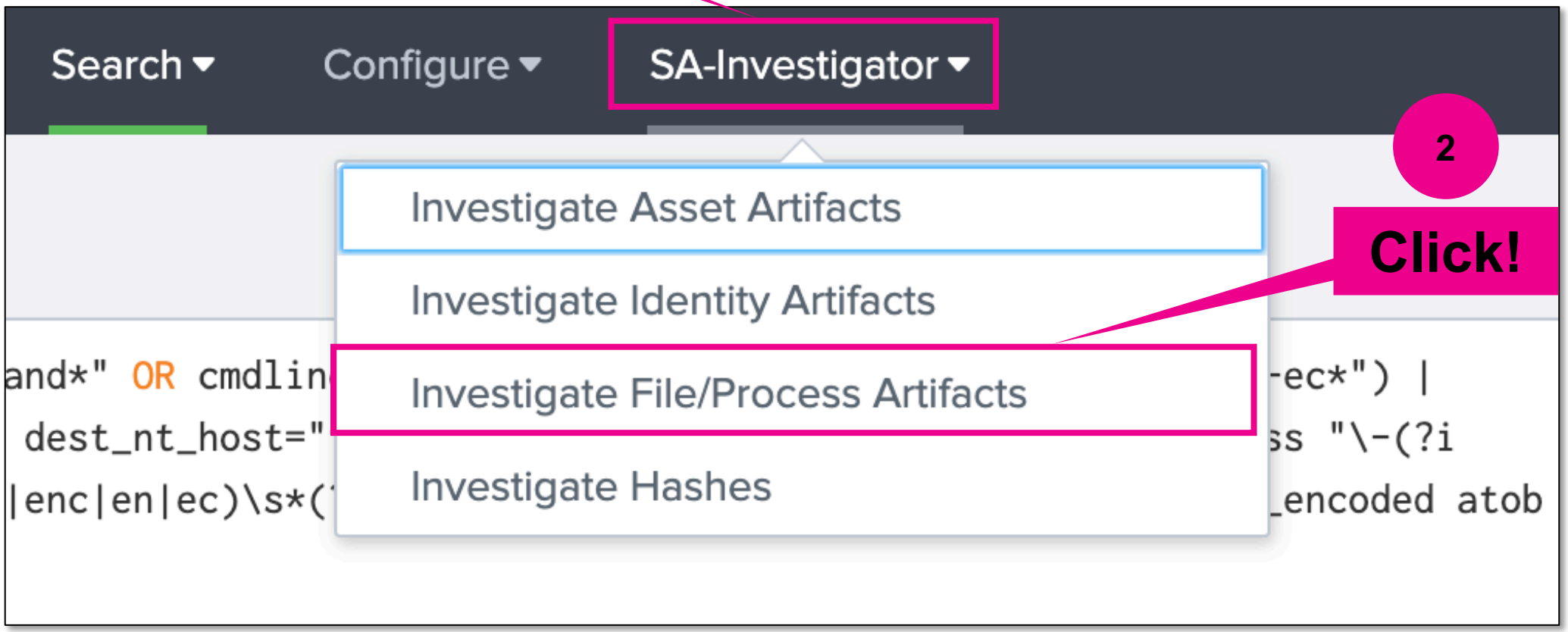
Click!



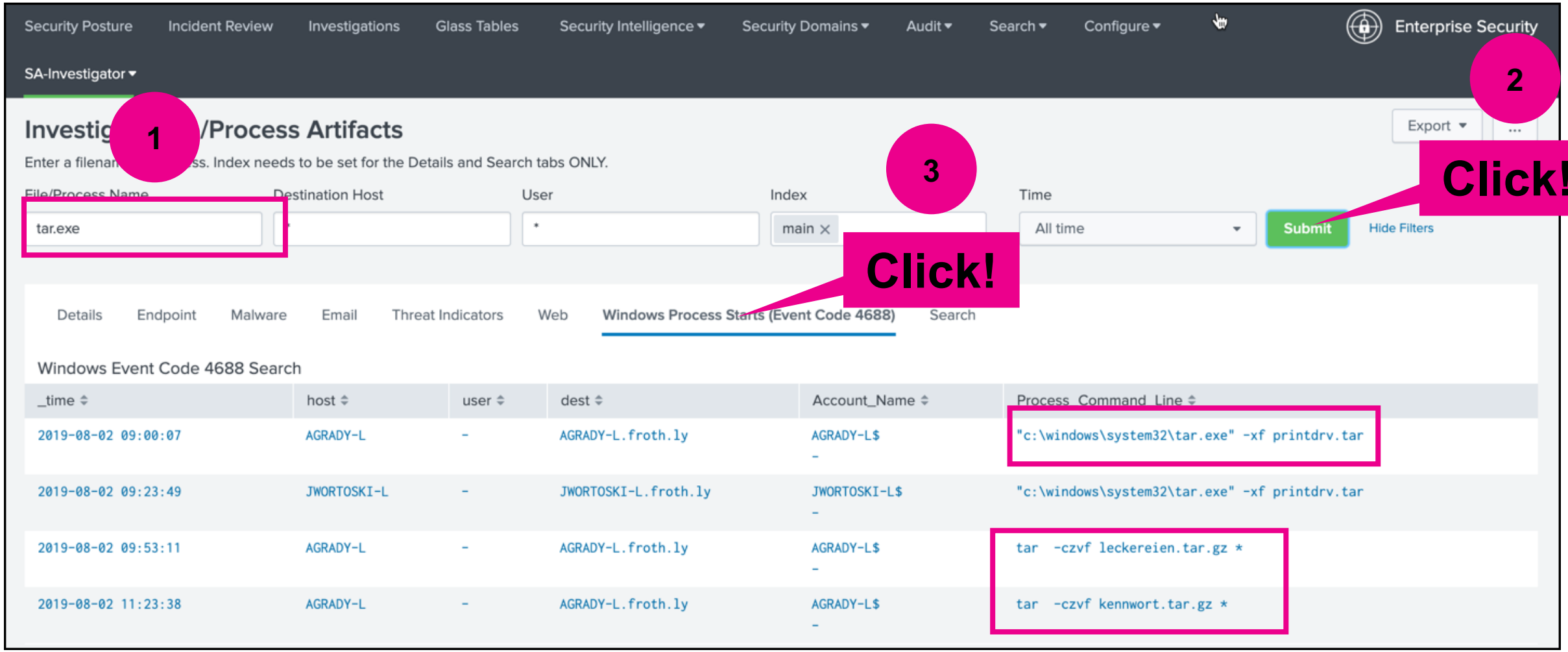




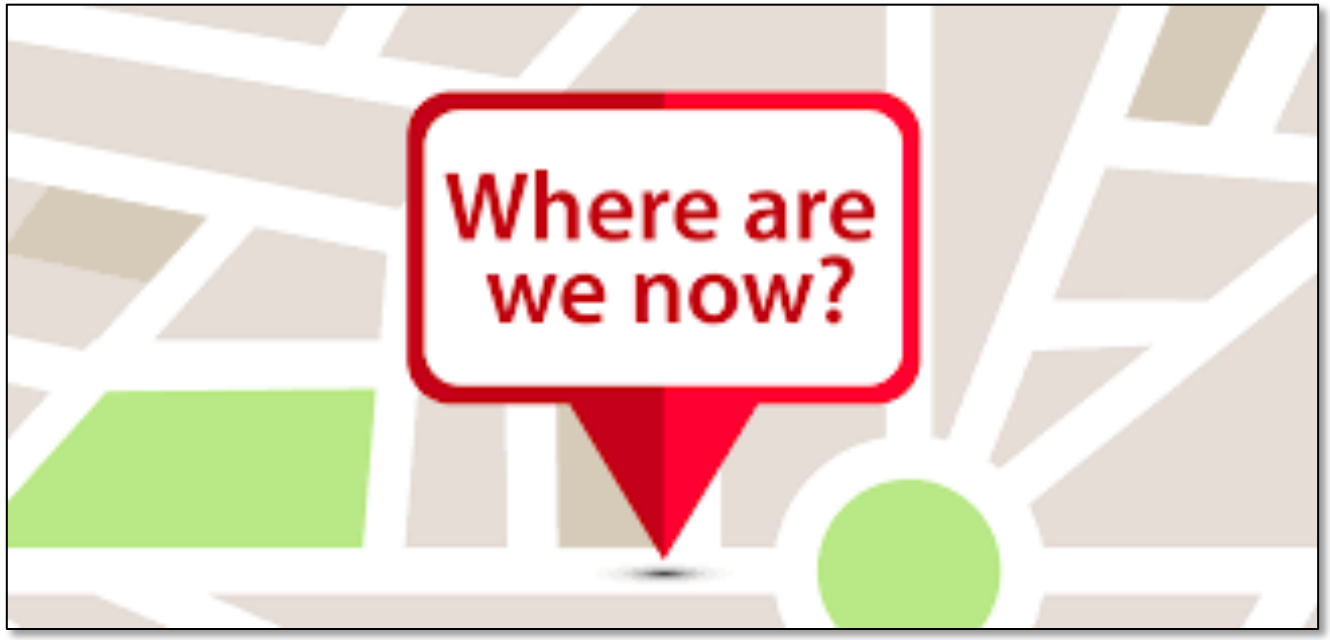
1 Click!



Back in ES Asset Investigator



splunk> .conf19

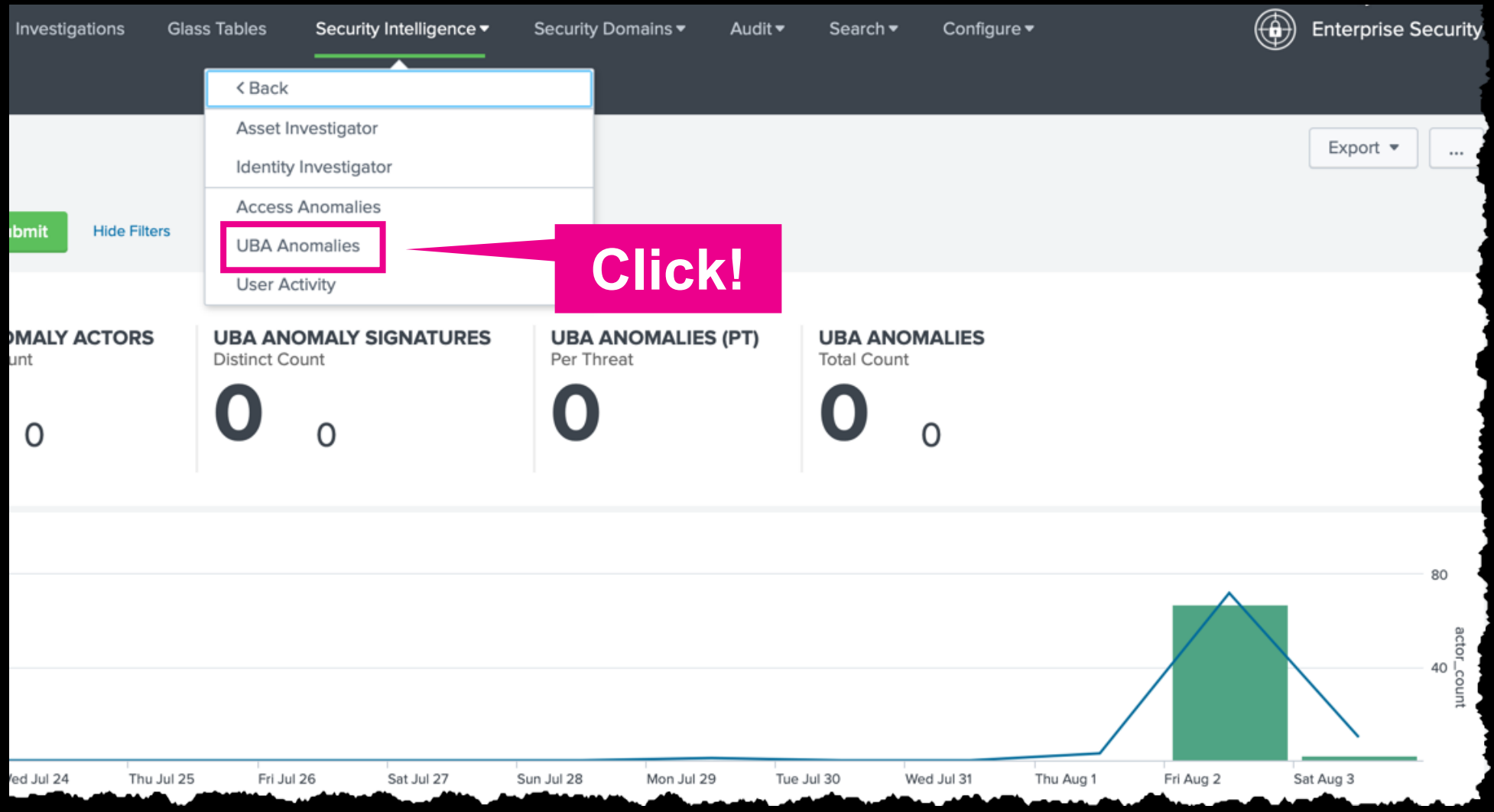


- The exe passkey triggered in UBA
- Threat associated with it due to suspicious location of process (c:\windows\system32\printdrv)
  - agrady-l is the associated workstation
  - frothly_helpdesk is the associated user
- Looking further into agrady-l, we see previous IOCs of tar.exe and hostname.exe
- 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

<1m ago

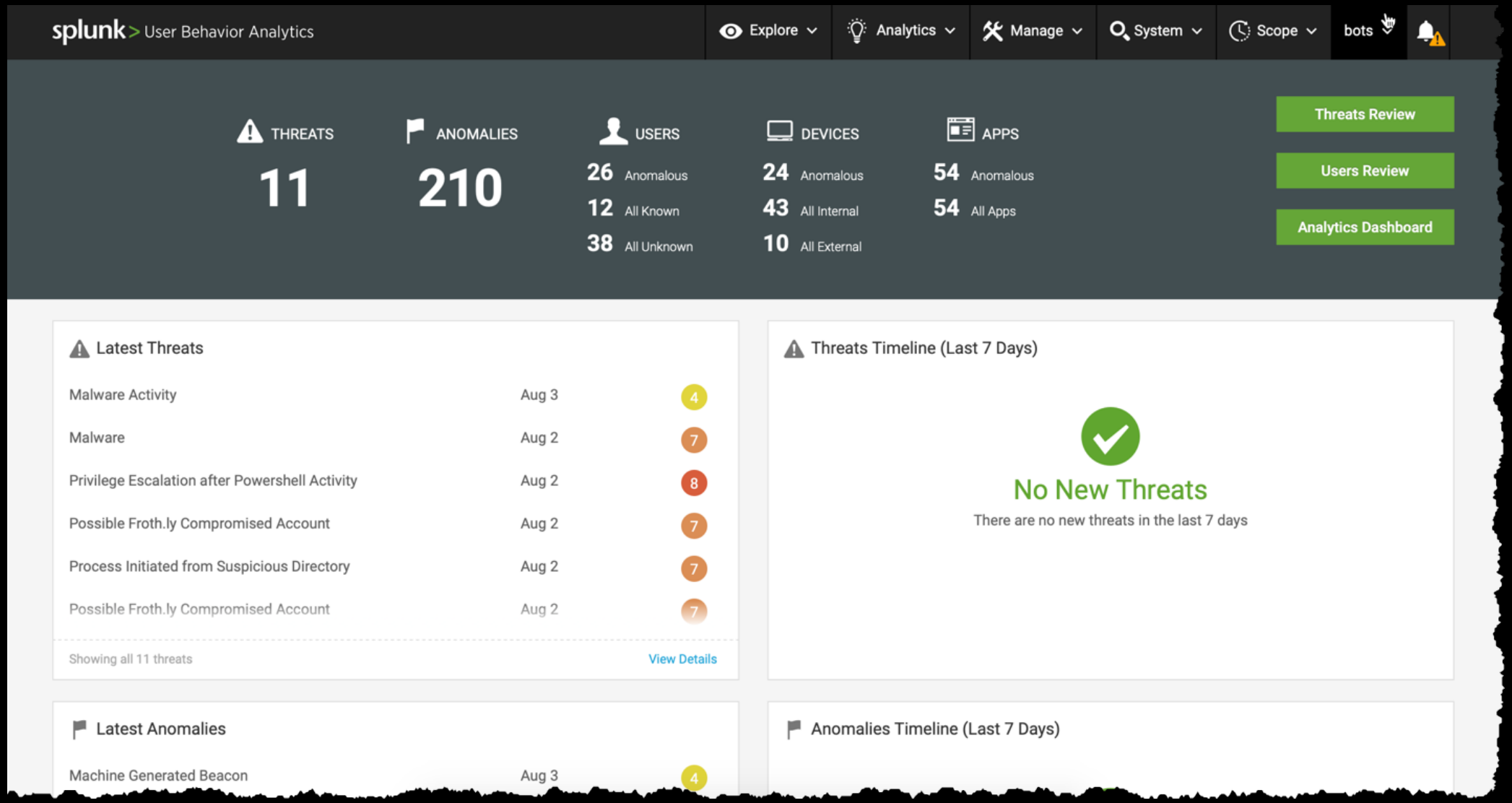
_time	signature	category	severity	app	dvc	url	user
2019-08-02		Internal Infection	low	verclsid.exe	mkraeusen-l		
2019-08-02		Internal Infection	low	hostname.exe	agrady-l		frothly_helpdesk
2019-08-02		Internal Infection	low	tar.exe	agrady-l		frothly_helpdesk
2019-08-02		Internal Infection	low	sd.exe	agrady-l		AudreyGrady
2019-08-02		Internal Infection	low	prl_vshadow.exe	jwortoski-l		dwm-1
2019-08-02		Internal Infection	low	am_delta_patch_1.299.805.0.exe	fmaltekesko-l		
2019-08-02		Internal Infection	low	microsoftpdfreader.exe	mvalitus-l		MateoValitus
2019-08-02		Internal	low	cmd.exe	jwortoski-l		JeremiahWortoski
2019-08-02		Internal Infection	low	peopleapp.exe	ghoppy-l		GraceHoppy
2019-08-02		Internal Infection	low	am_delta_patch_1.299.883.0.exe	fmaltekesko-l		FyodorMalteskesko

« Prev 1 2 3 4 5 6 7 8 9 10

Click!

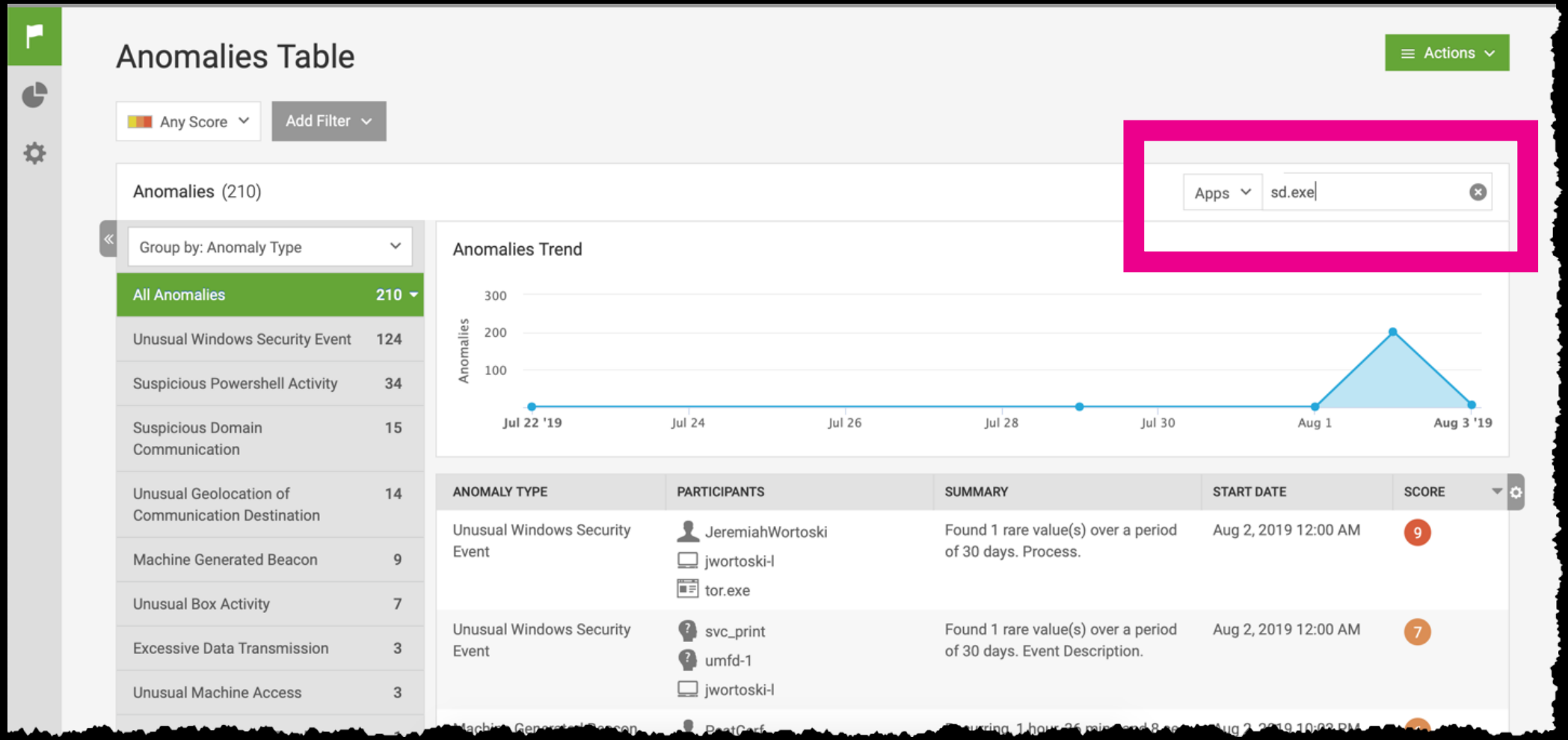
splunk> .conf19

Switch to UBA!



splunk> .conf19

List those Anomalies!



SD Anomaly List

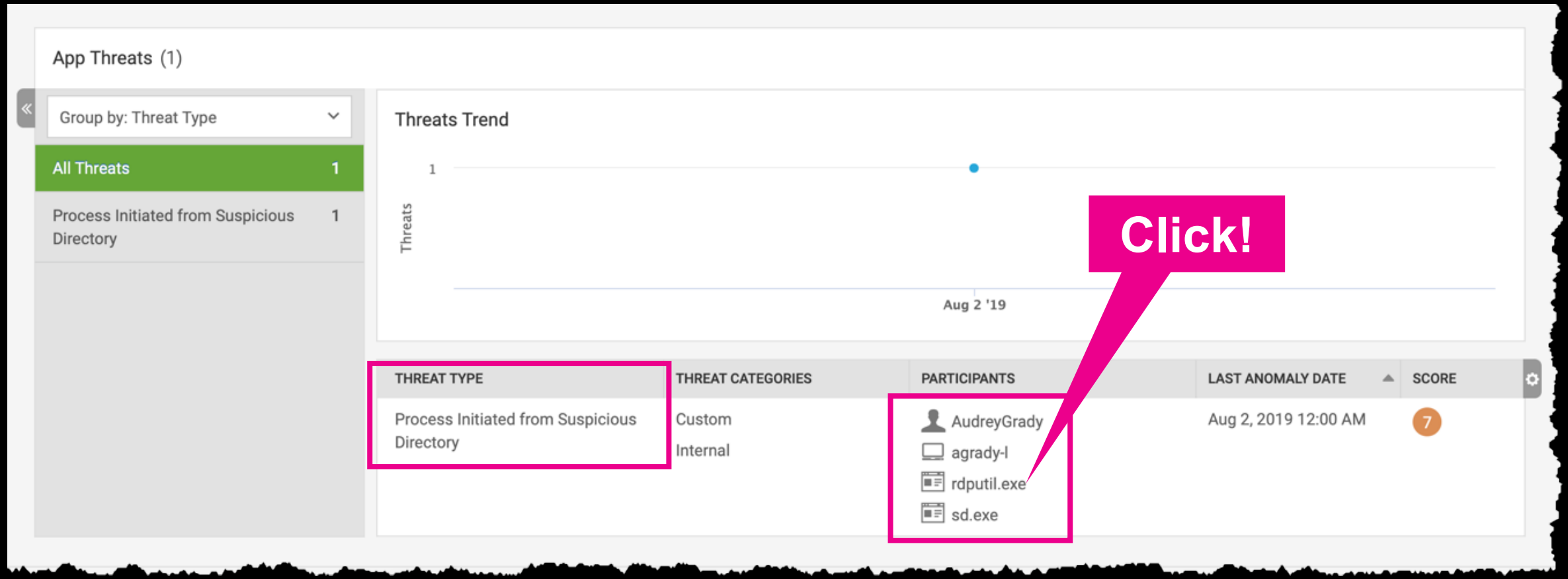
ANOMALY TYPE	PARTICIPANTS	SUMMARY	START DATE	SCORE
Unusual Windows Security Event	agrady-l sd.exe	Found 1 rare value(s) over a period of 30 days. Process.	Aug 2, 2019 12:00 AM	3
Unusual Windows Security Event	AudreyGrady agrady-l sd.exe	Found 1 rare value(s) over a period of 30 days. Process.	Aug 2,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

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



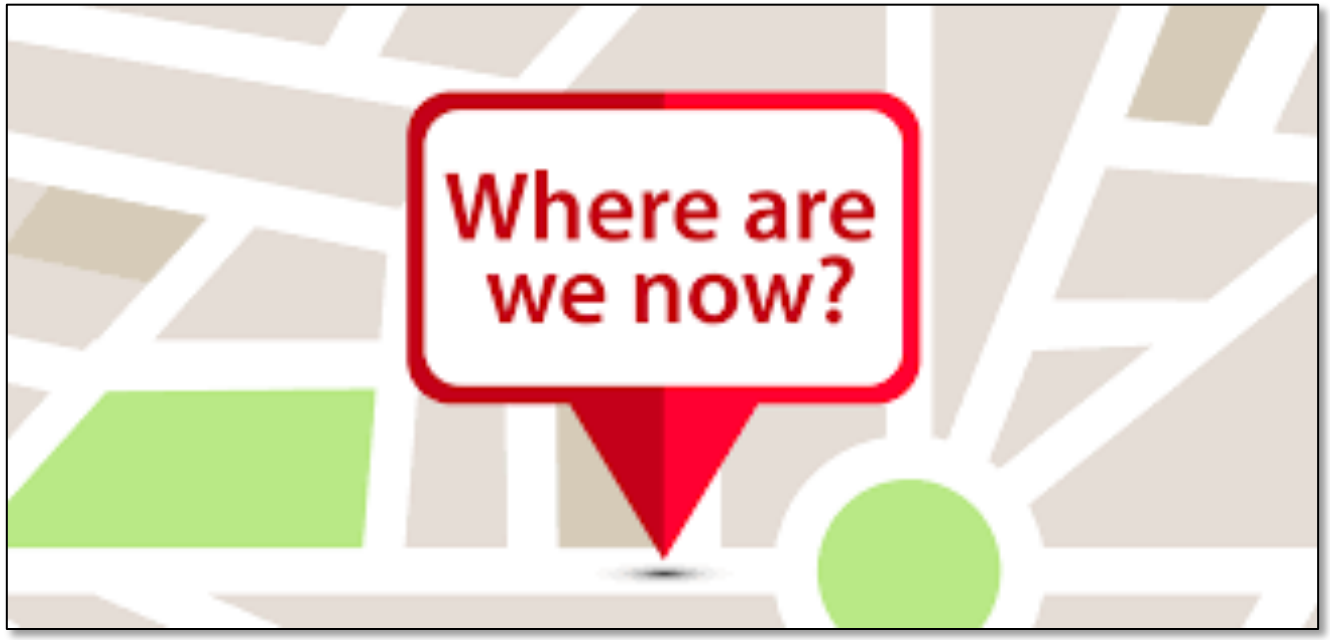
Rdputil Threats

Click!

THREAT TYPE	CATEGORIES	PARTICIPANTS	LAST ANOMALY DATE	SCORE
Process Initiated from Suspici… 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

Wait a second!!!

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



- sd.exe was executed (unknown executable)
- rdputil.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

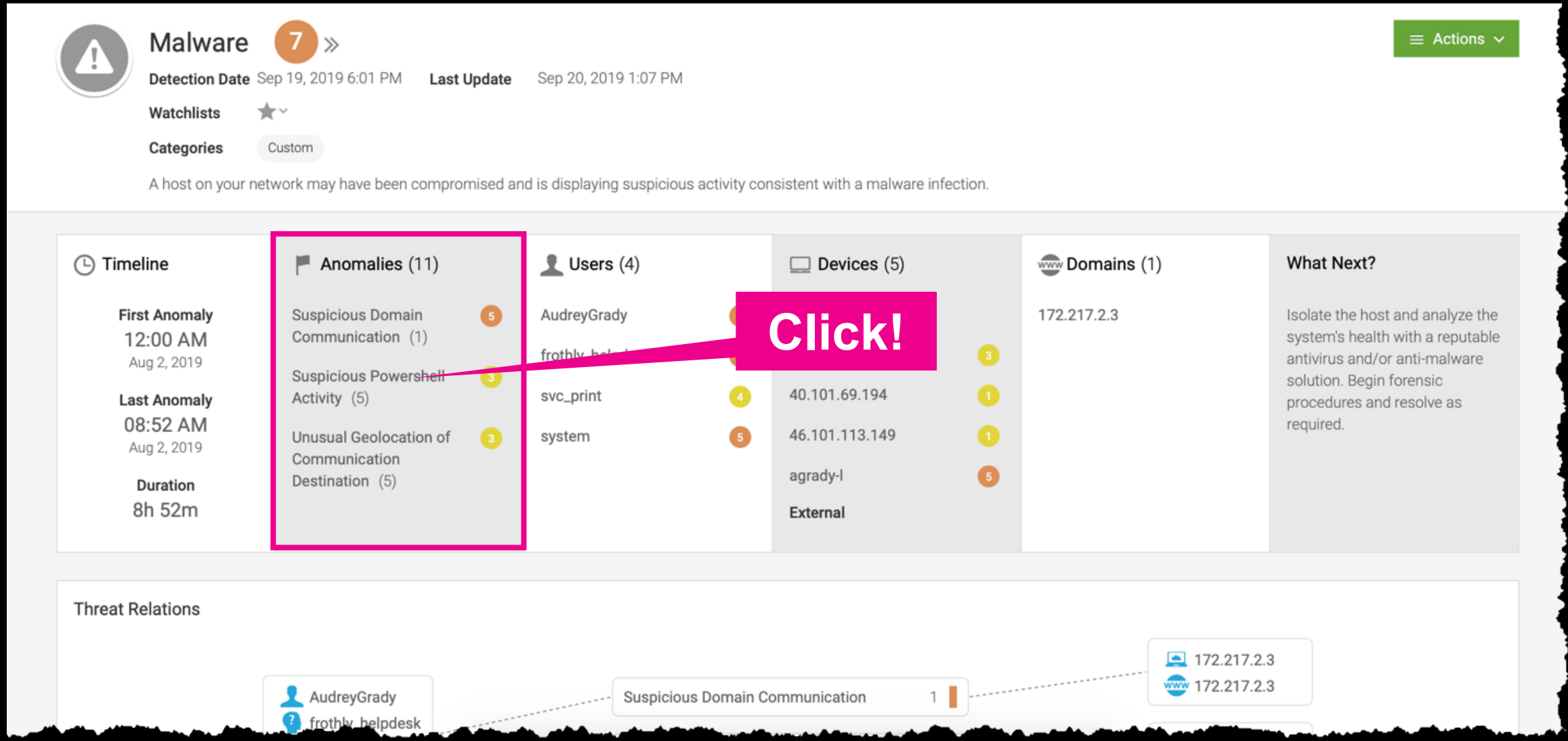
THREAT TYPE	THREAT CATEGORIES	PARTICIPANTS	LAST ANOMALY DATE	SCORE
Process Initiated from Suspicious Directory	Custom Internal	AudreyGrady agrady-l rdputil.exe sd.exe	Aug 2, 2019 12:00 AM	7
Process Initiated from Suspicious Directory	Custom Internal	svc_print jwortoski-l rdputil.exe	Aug 2, 2019 12:00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



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)

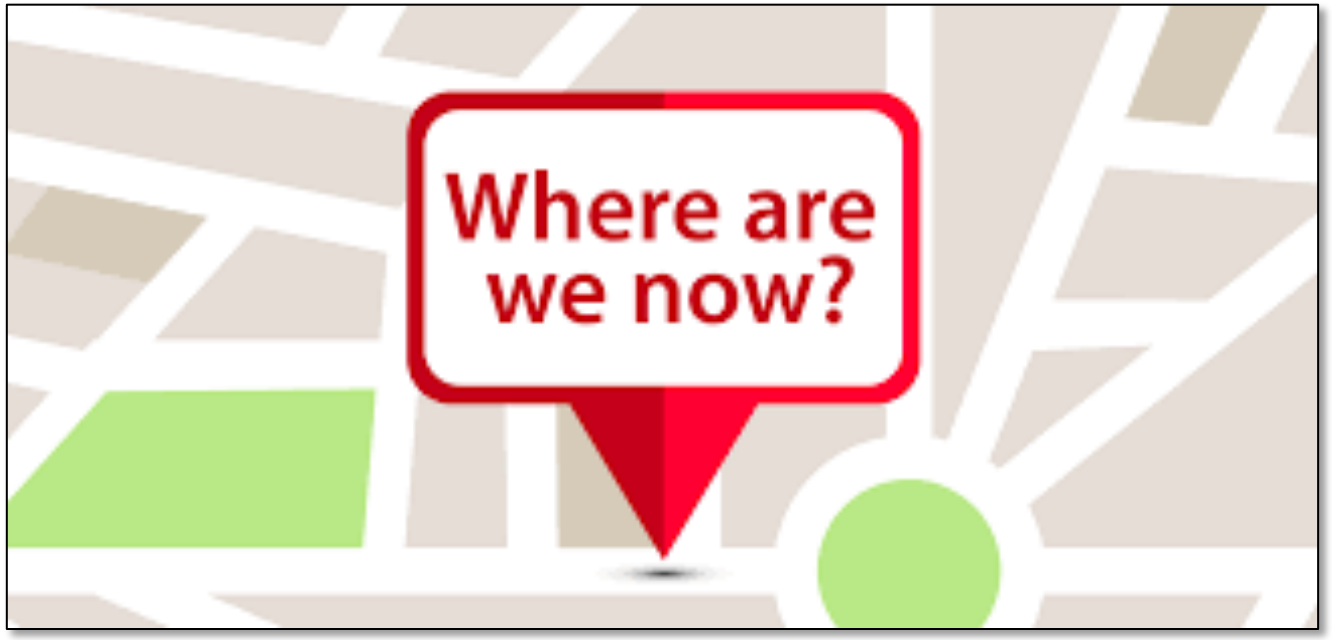
Command Executed by the user

```
powershell -ec
LgBcAHMAbQBiAC4AZQB4AGUAIABcAFwAdABpAHQAYQBuACAAYwBtAGQAIAAvAGMAIABjADoAX
AB3AGkAbgBkAG8AdwBzAFwAcwB5AHMAdABlAG0AMwAyAFwAcwBjAGgAdABhAHMAawBzACAA
LwBjAHIAZQBhAHQAZQAgAC8AcgB1ACAAJwBOAFQAIABBAFUAVABIAE8AUgBJAFQAWQBcAFMA
WQBTAFQARQBNACcAIAAvAHQAbgAgAE0AaQBjAHIAbwBzAG8AZgB0AFwAVwBpAG4AZABvAHcA
cwBcAFAAcgBpAG4AdABpAG4AZwBcAFAAcgBpAG4AdABEAHIAaQB2AGUAcgBVAHAAZABhAHQA
ZQAgAC8AcwBjACAAbwBuAGwAbwBnAG8AbgAgAC8AdAByACAAJwBwAG8AdwBlAHIAcwBoAGUA
bABsACAALQB3ACAAaAAgAEMAOgBcAFcAaQBuAGQAbwB3AHMAXABTAHkAcwB0AGUAbQAzADI
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)
- rdputil.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

.conf19
splunk>

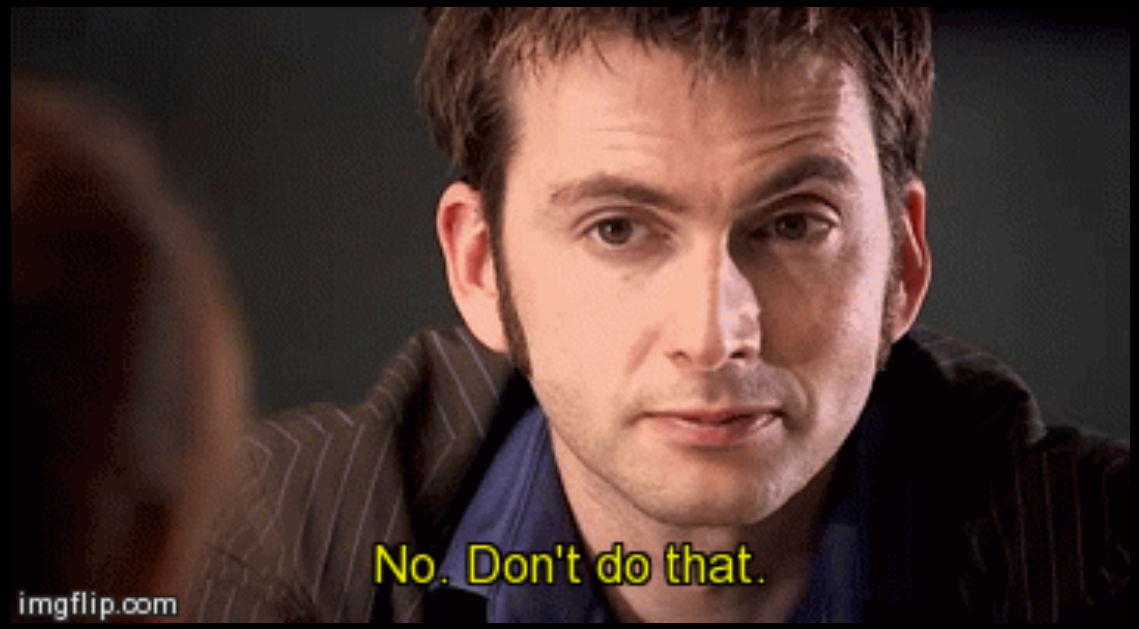
Quick Synopsis

- 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…



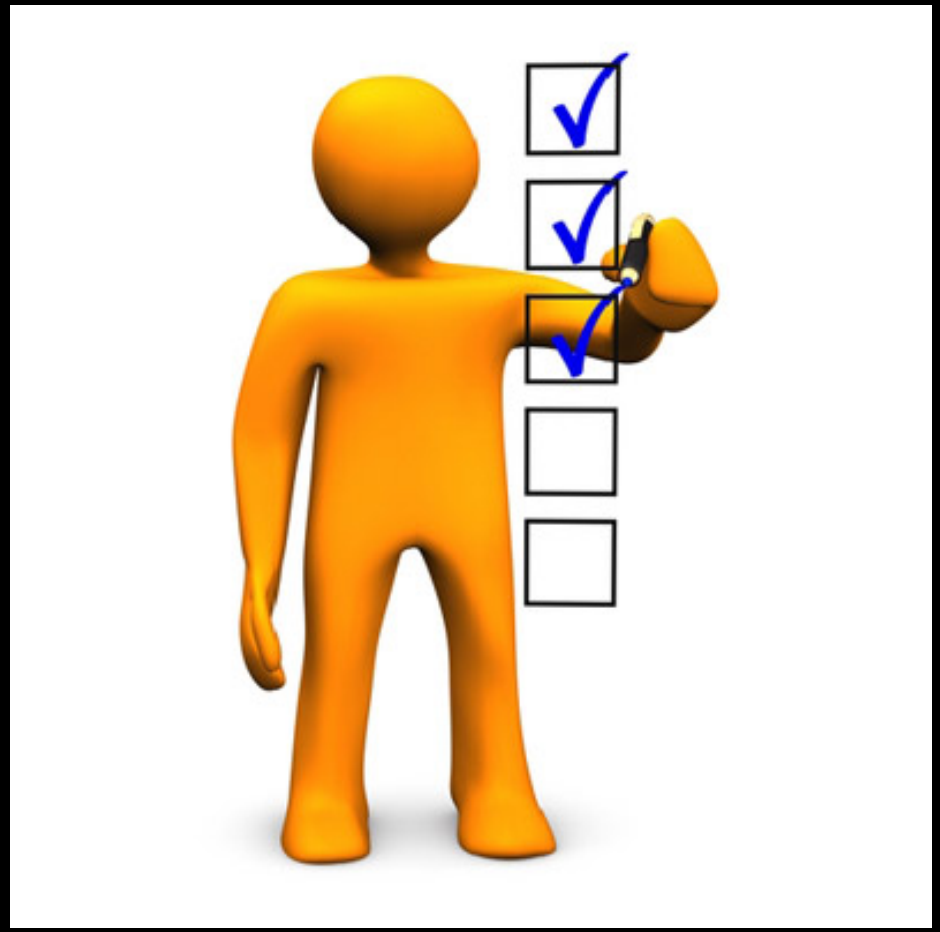
- Size UBA for 1000 accounts when there's 15,000 accounts
- Assure us all data is CIM compliant and on-boarded into Splunk
- IOPS of 800? No problem!
- Limit data or decrease logging
- Block basic networking ports (80/443)

- 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

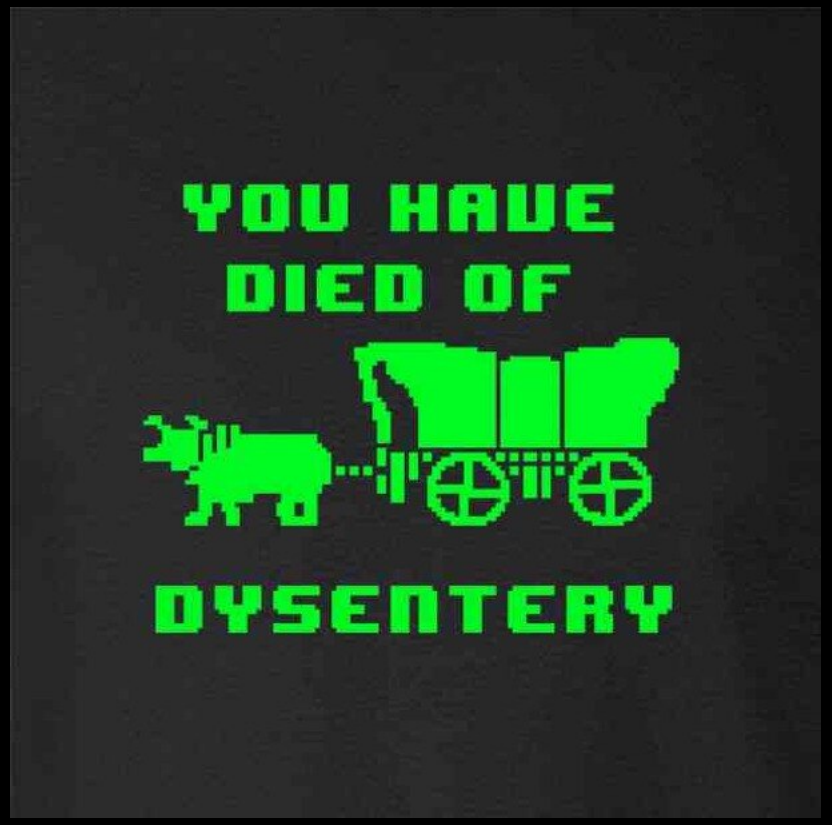
Sizing and Configuration

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

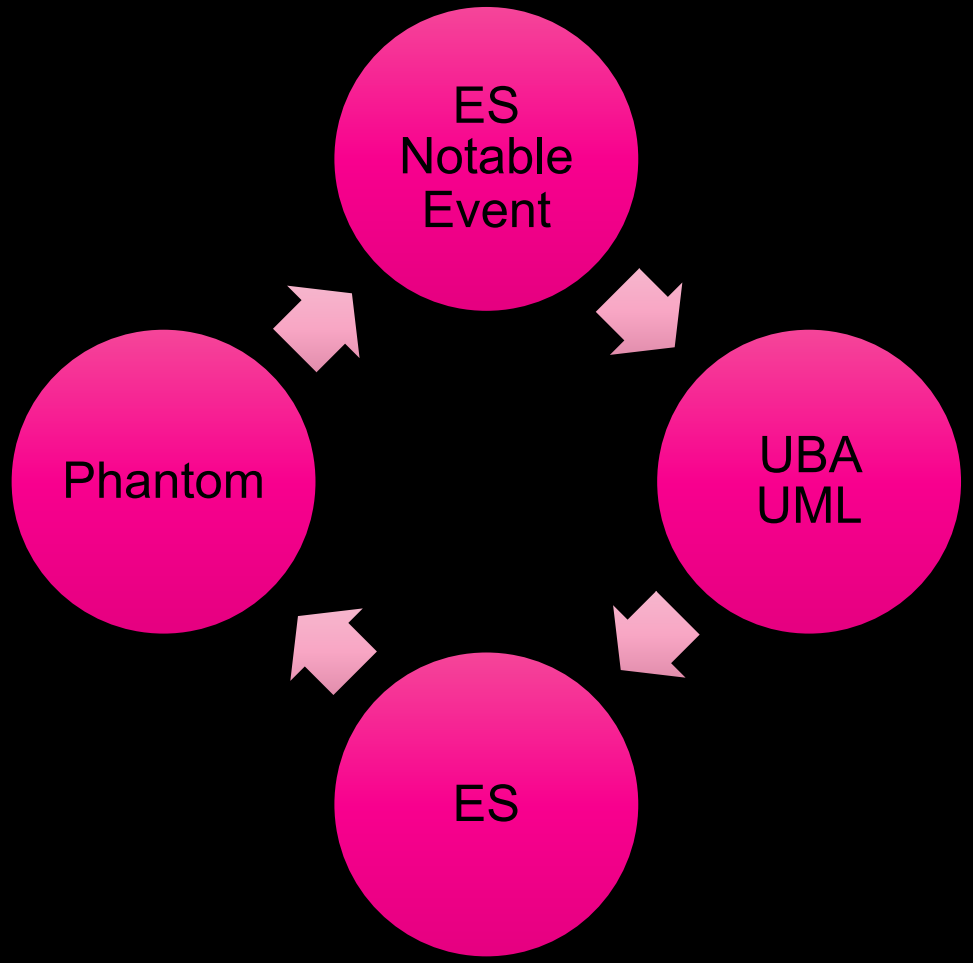
- Sizing exercise with you Splunk SME to verify data load
- 16 Core/64 RAM is set – throwing 96 cores at it will not affect data processing
- 50 GB/1 TB/1 TB drives are required – SSD preferred
- AMI and OVA are available

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



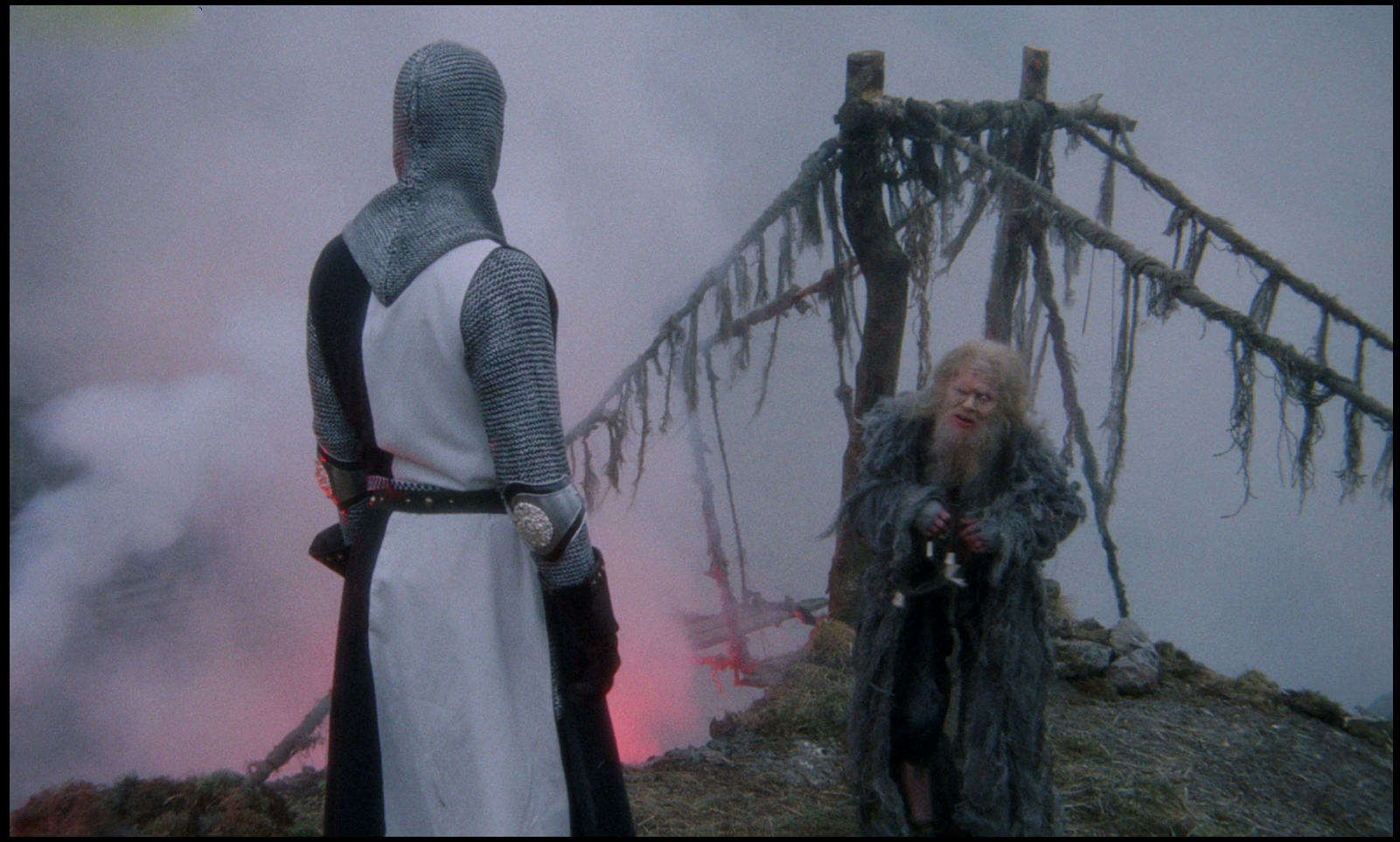
- Pull in correlation notable events from ES
- Send anomalies back to ES and the ES risk framework – see RBA deck for more!
- Send threats back to ES as notable events
- Reactions and responses to UBA data should be done through Splunk
- Take the online training!
- Use in conjunction with SSE, ES, and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

Where to go from here?

- Product Page: https://www.splunk.com/en_us/software/user-behavior-analytics.html
- 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



splunk>

Thank You!

Go to the .conf19 mobile app to

RATE THIS SESSION