Building Behavioral Detections

Cross-Correlating Suspicious Activity with the MITRE ATT&CK Framework

Haylee Mills
SIEM Security Engineer | Charles Schwab

splunk> .conf19

Forward-Looking Statements

During the course of this presentation, we may make forward-looking statements regarding future events or plans 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 may differ materially. The forward-looking statements made in the this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, it may not contain current or accurate information. We do not assume any obligation to update any forward-looking statements made herein.

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 functionalities described or to include any such feature or functionality in a future release.

splunk> .conf19

>whois

haylee dawna-rae mills

1. Used to work in animation
   - Metalokalypse or China, IL fans?
2. Prefers 40 hour workweeks and getting paid for them
3. Likes bicycling across countries, playing board/tabletop games, digging through e-crates
4. Loves teaching infosec
   - @ | 7thdrxn | .com
     https://open.spotify.com/user/7thdrxn

Building Behavioral Detections

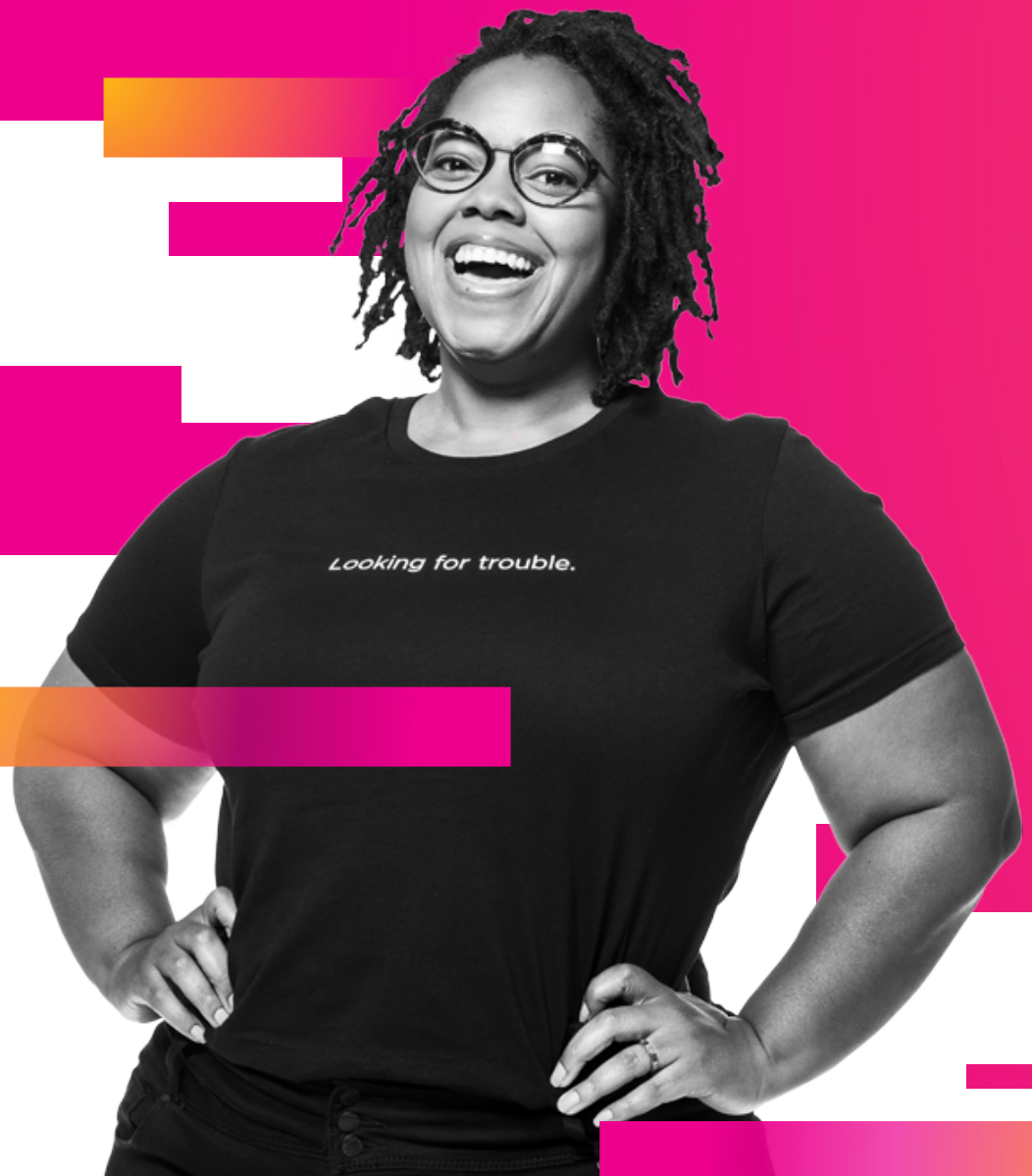
catching badness hiding in known-goods

Getting Started

Content Sources

Risk Building and Alerting

Tuning and Enrichment



Getting Started

logs, logs, and risk indexes

splunk> .conf19

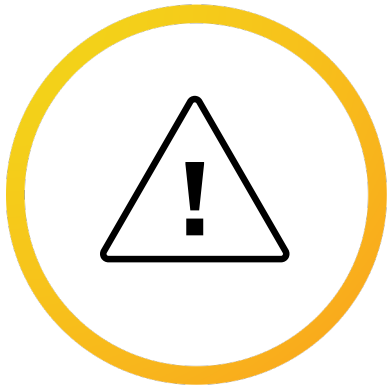
Getting Started

Endpoint logs

Network logs

Endpoint logs

Risk index



Network Logs

making sure we've got the goodies

- Proxy, firewall, Suricata HTTP/DNS
- Splunk Common Information Model (CIM)
  - find apps on Splunkbase with CIM normalization done for you
- Must be able to track **user** or **host** for risk model
  - IP != reliable
  - If necessary, build enrichment macros!

Oh yeah, of course. Enrichment... what's that again?

Enrichment

a handy sidetrack

- **`identify_asset(src_ip)`**
  | lookup assetIPList.csv ip_address AS src_ip OUTPUT src AS src

- **`identify_user(src)`**
  | lookup assetUserList.csv primaryMachine AS src OUTPUT user AS user

Lookup field
Event field

- **`enrich_asset(src)`**
  | lookup assetList.csv src AS src OUTPUT src_environment as src_bunit src_application AS src_application src_category as src_category
- **`enrich_user(user)`**
  | lookup userList.csv user AS user OUTPUT user_bunit AS user_bunit user_category AS user_category user_priority AS user_priority

Endpoint Logs

making sure we've got the goodies

sysmon, Sysmon, **SYSMON**

- Event ID 1 – *Process Creation*
- Event ID 3 – *Network Connection*
- Event ID 7 – *Image Loaded (DLLs)*
- Event ID 8 – *CreateRemoteThread (Process Injection)*
- Event ID 10 – *ProcessAccess (Credential Dumping)*
- Event ID 11 – *FileCreate*
- Event ID 12/13/14 – *RegistryCreateOrDelete / RegistryValueSet / RegistryKeyValueRename*
- Event ID 17/18 – *Pipe Created / Pipe Connected*

If you don't have endpoint logs, start with sysmon and Taylor Swift's excellent configuration

https://github.com/SwiftOnSecurity/sysmon-config

Endpoint Logs

making sure we've got the goodies

- Windows Event IDs; minimum **Authentication** and **Permissions** on DCs
  - If utilizing sysmon, disable:
    - 4688 (ProcessCreate) - 4657 (RegistryChange) - 4663 (FileCreate) - 5156 (FirewallConnection)
- Powershell Logging
  - If volume is INSANE, create unforgiving exceptions in Windows Event Forwarder

If starting from scratch, start here and GOOD LUCK
https://malwarearchaeology.com/cheatsheets

Risk Indexing

making sure we've got the goodies

If you haven't seen it… **immediately watch Jim Apger and Stuart McIntosh's conf18 talk:**

Say Goodbye to Your Big Alert Pipeline, and Say Hello to Your New Risk-Based Approach

RISK is the **FUTURE**

- Risk frameworks are lots of simple things strung together!
  - Lovely, normalized, comprehensive event logs
  - Enrich user/host with context
  - Add risk events with more context (like MITRE info) – by **user** or **host** -- to risk index
  - Create risk alerts from risk events

Content Sources

MITRE ATT&CK, LOLbins, and other friends

splunk> .conf19

MITRE ATT&CK

what's that again?

"MITRE ATT&CK™ is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations."

AKA

TONS of Work To Do

PROS:

- Visualize overall defenses against advanced attackers
- Pinpoint high value investments in security data sources and content development

CONS:

- Advanced techniques hide in noisy log sources
- Considerable amount of work to comprehensively address

MITRE ATT&CK

tactics to tack on

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact

- Tactics give us **categories** of activity
  - Techniques offer specifics of activity
- Single techniques from **one** tactic can be normal activity
- Sudden use of **multiple** tactics = badness?

Let's make a quick risk rule!

MITRE ATT&CK

I SEE YOU

| **search** index=security* sourcetype=sysmon process_name=psexec.exe

| **stats** values(process_command_line) as cmdline values(process_parent_path) as parent values(process_parent_command_line) as parent_cmdline values(user_name) as user values(user_category) as user_category values(src_category) as src_category by src

| **eval mitreAttack** = "execution – T1035 – Service Execution|lateral_movement – T1077 – Windows Admin Shares“

| **eval risk_message** = "Use of psexec.exe by ".user." on ".src

| **eval risk_information** = "cmdline=\"".cmdline."\"|parent=\"".parent."\"|parent_cmdline=\"".parent_cmdline

|`***risk_score_combined****(impact,confidence,user,user_category,src,src_category)*`

Stew on this for now; we’ll cover risk building more thoroughly!

LOLBins and Scripts

nothing to LOL about

https://lolbas-project.github.io/

LOL = "Living Off the Land" = Hiding in goodness

Most are **T1218 – Signed Binary Proxy Execution** or **T1216 – Signed Script Proxy Execution**…

MITRE Coverage % **NOT AS IMPORTANT AS** MITRE Coverage + **DEPTH**

UNIX equivalent if you have useful UNIX endpoint logging:
https://gtfobins.github.io/

Other Resources

lots to learn about and build content from

Monthly Staff Picks for Splunk Security Reading

https://www.splunk.com/blog/search.html?query=%22staff%2Bpicks%2Bfor%2Bsplunk%2Bsecurity%22

Splunk's security folks picking out some of the best articles, every MONTH!

Olaf Hartong's Threat Hunting Splunk App

https://github.com/olafhartong/ThreatHunting

Great collection of queries to use for risk rules.

Hunting with Splunk: The Basics

https://www.splunk.com/blog/2017/07/06/hunting-with-splunk-the-basics.html

A whopping **twenty-three** articles about threat hunting your data, from Splunk security superstars Ryan Kovar and Steve Brant.

Risk Building + Alerting

the meat and potatoes

splunk> .conf19

Risk Indexing and Alerting

the one two punch

Risk Indexing

collect events to a summary index *(doesn't incur license usage!)*

add useful metadata for tuning or analyst context

events don't need to add risk; can be for situational awareness

Risk Alerting

search events in the risk index by user or host

slice data to find potentially malicious activity

monitor and adjust enrichment to tune

add useful metadata for analyst

NOTE: you must add fields to your Risk data model; try to cap at 10-15 and combine information into single fields

Risk Indexing

building them risk scores

```
| search index=security* sourcetype=sysmon process_name=psexec.exe
| stats values(process_command_line) as cmdline values(process_parent_path) as parent
values(process_parent_command_line) as parent_cmdline values(user_name) as user
values(user_category) as user_category values(src_category) as src_category
last(sourcetype) as sourcetype by src
| eval mitreAttack = "execution – T1035 – Service Execution|lateral_movement – T1077 –
Windows Admin Shares"
| eval risk_message = "Use of psexec.exe by ".user." on ".src
| eval risk_information =
"cmdline=\"".cmdline."\"|parent=\"".parent."\"|parent_cmdline=\"".parent_cmdline."\""
```

```
|`risk_score_combined(impact,confidence,user,user_
category,src,src_category)`
```

Risk Indexing

```
|`risk_score_combined(impact,confidence,user,user_category,src,src_category)`
| eval risk_mod_count_user = 0
| eval risk_mod_count_user = case(user_category="executive",risk_mod_count_user+1,
user_category="privileged",risk_mod_count_user+1, user_category="service-account",risk_mod_count_user+1,
tag="watchlist",risk_mod_count_user+1)


| eval risk_mod_count_sys = 0
| eval risk_mod_count_sys = case(src_category="production",risk_mod_count_sys+1,
src_category="database",risk_mod_count_sys+1, src_category="dmz",risk_mod_count_sys+1)
| lookup assetVulnerabilities.csv system AS src OUTPUT critVulnCount as critVulnCount highVulnCount as
highVulnCount
| fillnull value="0" critVulnCount highVulnCount
| eval risk_mod_count_vuln = 0
| eval risk_mod_count_vuln = case(critVulnCount!=0,risk_mod_count_vuln+(1*critVulnCount),
highVulnCount!=0,risk_mod_count_vuln+(0.5*highVulnCount))
| eval risk_mod_count_sys = risk_mod_count_vuln+risk_mod_count_sys

| eval risk_mod_count_combined = risk_mod_count_sys + risk_mod_count_user
```

Risk Indexing

|`*risk_score_combined*(*impact,confidence,user,user_category,src,src_category*)`

| *eval risk_mod_count_combined = risk_mod_count_sys + risk_mod_count_user*

| eval risk_impact = lower("impact") , risk_confidence = lower("confidence")
| lookup rba_scores impactLabel AS risk_impact confidenceLabel AS risk_confidence OUTPUT impactValue AS risk_impact_num confidenceValue AS risk_confidence_num

| eval risk_score = risk_impact_num * risk_confidence_num * ((risk_mod_count_combined * .25)+1)

| eval risk_object_type="user" , risk_object=user | fillnull risk_object value="null" | collect index=risk
| eval risk_object_type="system" , risk_object=src | fullnull risk_object value="null" | collect index=risk

Now we're cooking with RISK!

I have risk scores…

now what?

It's not just risk scores, it's ANY cool way to slice it!

Risk Score Exceeds Threshold

Multiple MITRE Tactics

High Number of Unique ATT&CK Techniques

Sudden Increase in ATT&CK Techniques

Sudden Significant Increase in Risk Score

Risk Events from Numerous Sourcetypes

take any of these and try them over 24 hours, 7 days, 30 days

Risk Incidents

importing our useful fields

```
| eval mitreAttack = "execution – T1035 – Service Execution|lateral_movement – T1077 – Windows Admin Shares"
| eval risk_information = "cmdline=\"".cmdline."\"|parent=\"".parent."\"|parent_cmdline=\"".parent_cmdline
```

Remember this part? Let's use it!

Schema Accelerated Event Searching

```
| from datamodel="Risk.All_Risk" | search risk_object=* | table risk_object risk_object_type risk_message risk_score source sourcetype mitreAttack risk_information

| eventstats sum(risk_score) as riskSum by risk_object, risk_object_type

| makemv delim="|" mitreAttack | rex field=mitreAttack "(?<tactic>.+?) (-|–) (?<technique_num>.+?) (-|–) (?<technique>.+)“

| rex field=risk_information "cmdline=\"(?<cmdline>.+)\"\|parent=\"(?<parent>.+)\"\|parent_cmdline=\"(?<parent_cmdline>.+)\""

| fields – mitreAttack risk_information
```

Now we can build the rest of the rule!

Risk Incidents

alerting on interesting things

*| **from** datamodel="Risk.All_Risk" | **search** risk_object=* | **table** risk_object risk_object_type risk_message risk_score source sourcetype mitreAttack risk_information | **eventstats** sum(risk_score) as riskSum by risk_object, risk_object_type | **makemv** delim="|" mitreAttack | **rex** field=mitreAttack "(?<tactic>.+?) (-|–) (?<technique_num>.+?) (-|–) (?<technique>.+)" | **rex** field=risk_information "cmdline=\"(?<cmdline>.+)\"\|parent=\"(?<parent>.+)\"\|parent_cmdline=\"(?<parent_cmdline>.+)\"" | **fields** – mitreAttack risk_information*

| **where** riskSum > 200

| **eventstats** **dc(tactic) as tacticCount** by risk_object,risk_object_type

| **where** tacticCount > 2

| **eventstats** **dc(tactic) as tacticCount dc(technique) as techCount** by risk_object,risk_object_type

| **where** techCount > 5 AND tacticCount > 2 AND riskSum > 50

| **eval** alertMessage = "High Risk Score from ".risk_object_type." ".risk_object." with ".tacticCount " Tactics and ".techCount." Techniques

Risk rules are super **MODULAR;** go ahead, mix and match!

Tuning + Enrichment

the dessert

splunk> .conf19

Tuning

Your new full-time job!

Finding Sweet Spots

Tune risk incident rules with confirmed incidents from standard alerts

Tune risk building events by slicing up your risk index for insight

Red team is your new best friend!

Smart Tuning

Risk lets you retain potentially useful "noise" as baselines and context

Trim useless noise, but lean toward downgrading to informational, 0 / 1 risk score events

Tuning our Risk Events

oh THAT event again?

```
| search index=security* sourcetype=sysmon process_name=psexec.exe
```

NOT (user_name=srv.* AND process_command_line IN ("normal behavior1","normal behavior2","etc"))

```
| stats values(process_command_line) as cmdline values(process_parent_path) as parent
values(process_parent_command_line) as parent_cmdline values(user_name) as user values(user_category) as
user_category values(src_category) as src_category by src
| eval mitreAttack = "execution – T1035 – Service Execution|lateral_movement – T1077 – Windows Admin Shares"
| eval risk_message = "Use of psexec.exe by ".user." on ".src
```

| lookup riskAdjust-T1035.csv cmdline AS cmdline OUTPUT adjust AS adjust impact AS impact confidence AS confidence
| eval impact = case(adjust="true",impact,1=1,"medium") , confidence = case(adjust="true",confidence,1=1,"medium")

```
| eval risk_information = "cmdline=\"".cmdline."\"|parent=\"".parent."\"|parent_cmdline=\"".parent_cmdline
| `risk_score_combined(impact,confidence,user,user_category,src,src_category)`
```

Tuning our Risk Incidents

sorting the wheat from chaff

```
| from datamodel:"Risk.All_Risk“

    | search risk_message!="blahblah*" NOT risk_object IN ("1","2","etc")

| table risk_object risk_object_type risk_message risk_score source sourcetype mitreAttack risk_information

| eventstats sum(risk_score) as riskSum by risk_object, risk_object_type

| makemv delim="|" mitreAttack | rex field=mitreAttack "(?<tactic>.+?) (-|–) (?<technique_num>.+?) (-|–)
(?<technique>.+)" | rex field=risk_information
"cmdline=\"(?<cmdline>.+)\"\|parent=\"(?<parent>.+)\"\|parent_cmdline=\"(?<parent_cmdline>.+)\"" | fields – mitreAttack
risk_information

    | mvexpand technique
    | search NOT ((risk_object IN ("1") AND technique IN ("1a"))
    OR (risk_object IN ("2") AND cmdline IN ("2a")))

| eventstats sum(risk_score) as riskSum dc(tactic) as tacticCount dc(technique) as techniqueCount by
risk_object,risk_object_type

| where tacticCount > 2
```

Enrichment

<3 ur analysts

Provide Useful Context

If you were working this alert, what info would YOU want handy?

URLs – Descriptions – Explanations – Next Steps – Documentation

ADD IT ALL WITH LOOKUPS!

Enrichment

turn ought-to-haves to gotta-haves

```
| from datamodel="Risk.All_Risk" | search risk_object=* | table risk_object risk_object_type
risk_message risk_score source sourcetype mitreAttack risk_information | eventstats sum(risk_score)
as riskSum by risk_object, risk_object_type | makemv delim="|" mitreAttack | rex field=mitreAttack
"(?<tactic>.+?) (-|–) (?<technique_num>.+?) (-|–) (?<technique>.+)" | rex field=risk_information
"cmdline=\"(?<cmdline>.+)\"\|parent=\"(?<parent>.+)\"\|parent_cmdline=\"(?<parent_cmdline>.+)\"" |
fields – mitreAttack risk_information | where riskSum > 200
```

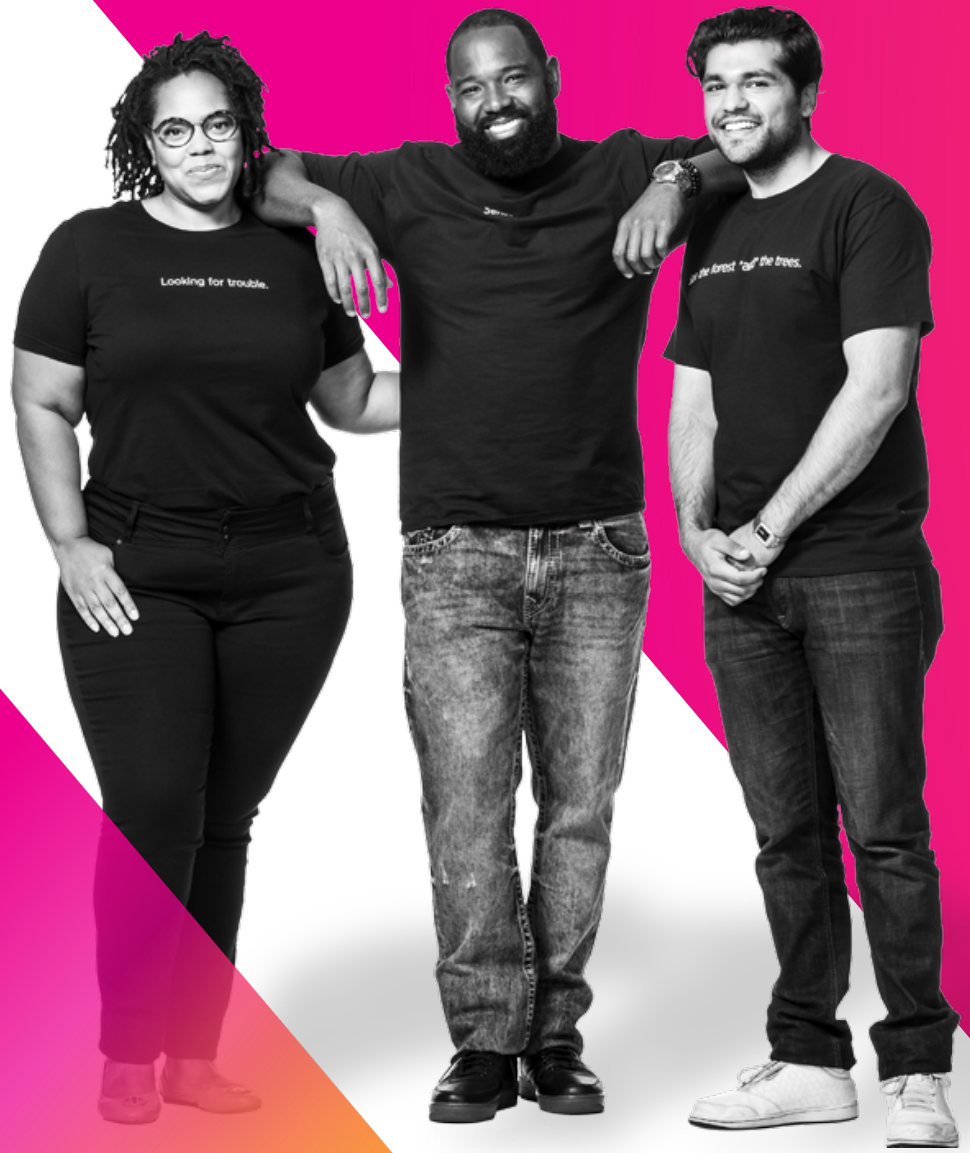
```
| lookup mitreEnrichment.csv technique_num AS technique_num OUTPUT
url AS url description AS description detectionMethod AS detectionMethod
dataSources AS relevantData
```

Get creative and ask your analysts what info helps them that YOU could provide!

Takeaways

level up your content

1. Enrichments increase context
2. Risk alerts catch advanced attackers
3. Tuning will take forever



Q&A

splunk> .conf19

Risk-Based Alerting (RBA) Sessions

let's learn even MORE and make new friends!

SEC 1803 – Modernize and Mature Your SOC with Risk-Based Alerting

Tuesday, October 22nd 03:00PM – 03:45PM - where I'm going right after this!

SEC 1538 – Getting Started with Risk-Based Alerting and MITRE

Wednesday, October 23rd 12:30PM – 01:15PM

SEC 1908 – Tales from a Threat Team: Lessons and Strategies for Succeeding with a Risk-Based Approach

Wednesday, October 23rd 03:00PM – 03:45PM

Birds of the Feather – The RBA Community – Join the Slack Channel!

TBD

.conf19

splunk>

Thank You!

Go to the .conf19 mobile app to

RATE THIS SESSION