.conf19

splunk>

Jim Apger

Security Specialist | Splunk

Jimi Mills

SOC Manager | Texas Instruments

Modernize and Mature your SOC with Risk-Based Alerting

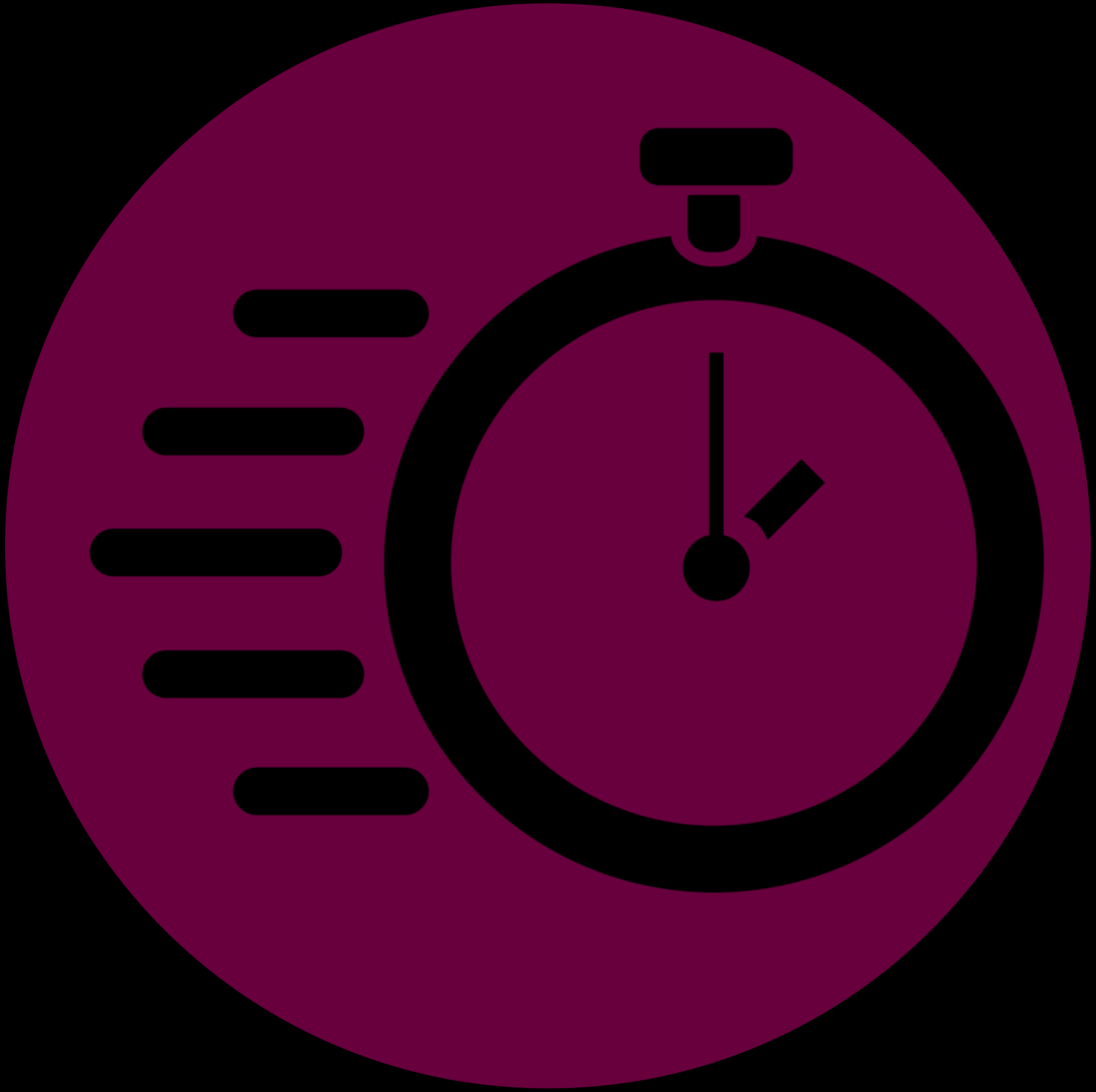
Forward-Looking Statements

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.

Super Sweet Agenda

- Intro
- Overview
- The Situation
- TI RBA Timeline
- RBA & MITRE ATT&CK
- Wrap up



Overview of Risk Based Alerting (RBA)

Hold on……I'm gonna fly through this

.conf19

splunk>

The Problem?

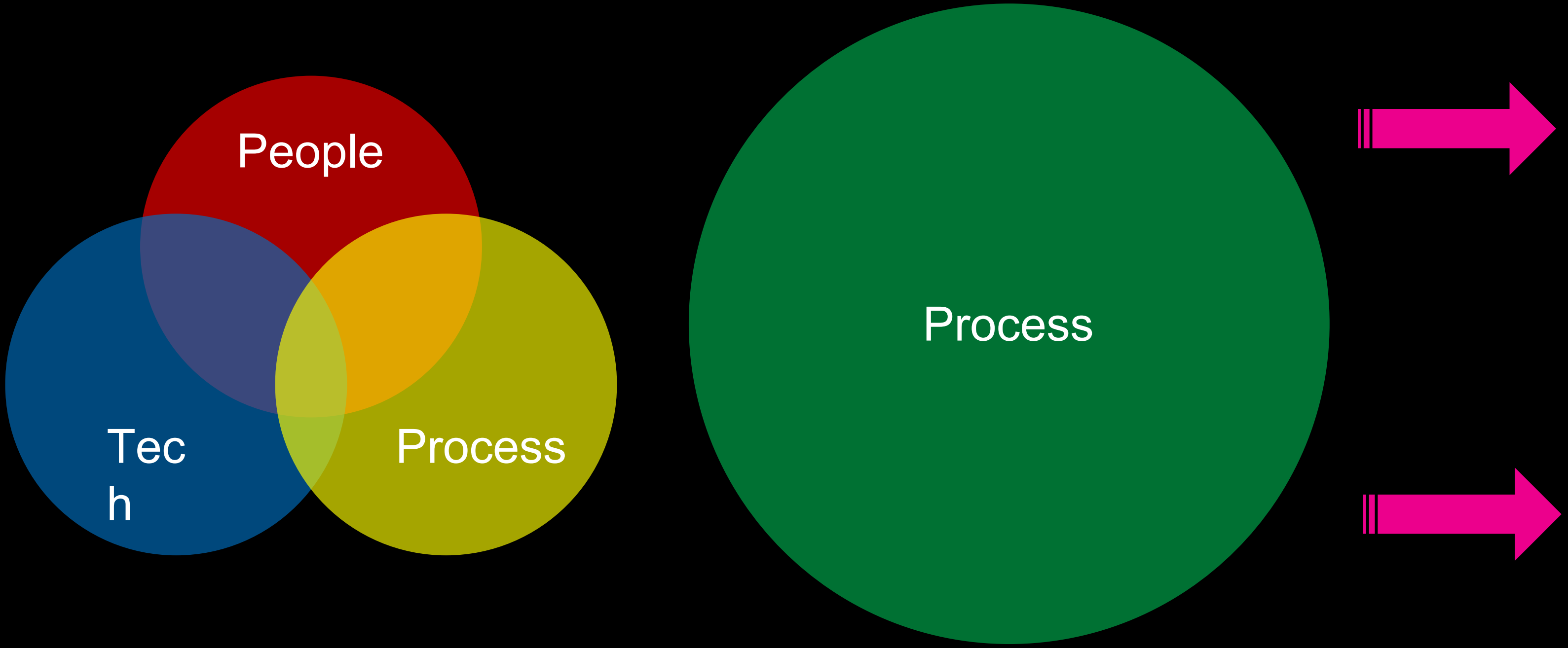
Alert Fatigue!

Incidents based on narrowly defined detections lead to majority noise within the SOC

Adding more sources and detection mechanisms continue to overburden the SOC Analysts with more alerts

Whitelisting as a reaction to the above results in a situational numbness

A Change of Perspective



Efficient use of existing toolchain

Scale and retain HAPPY analysts

Now Broken

How we (myself included) have been working

Analytics

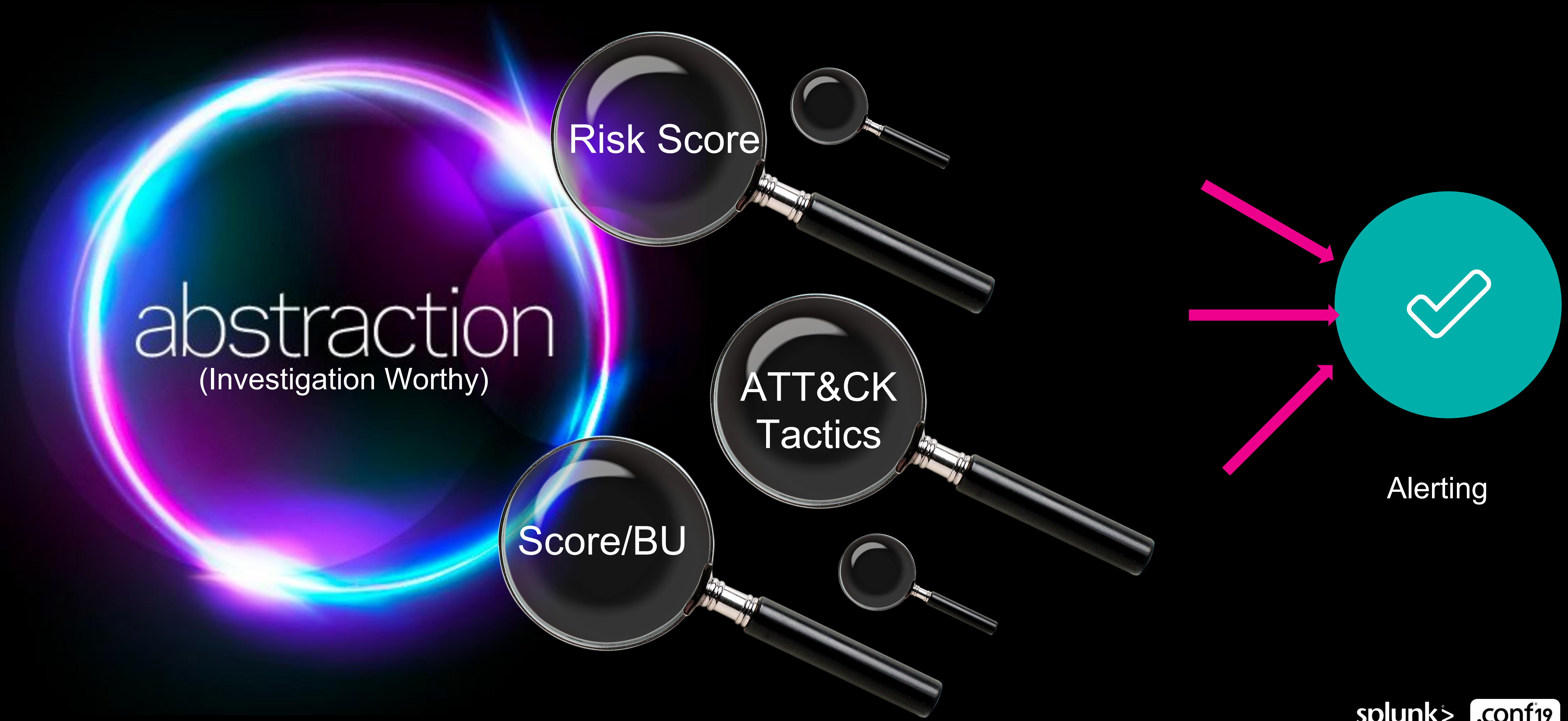
Alerting

Risk Attributions

abstraction

Analytics

Examine Attributions – Multiple Lenses



abstraction

(Investigation Worthy)

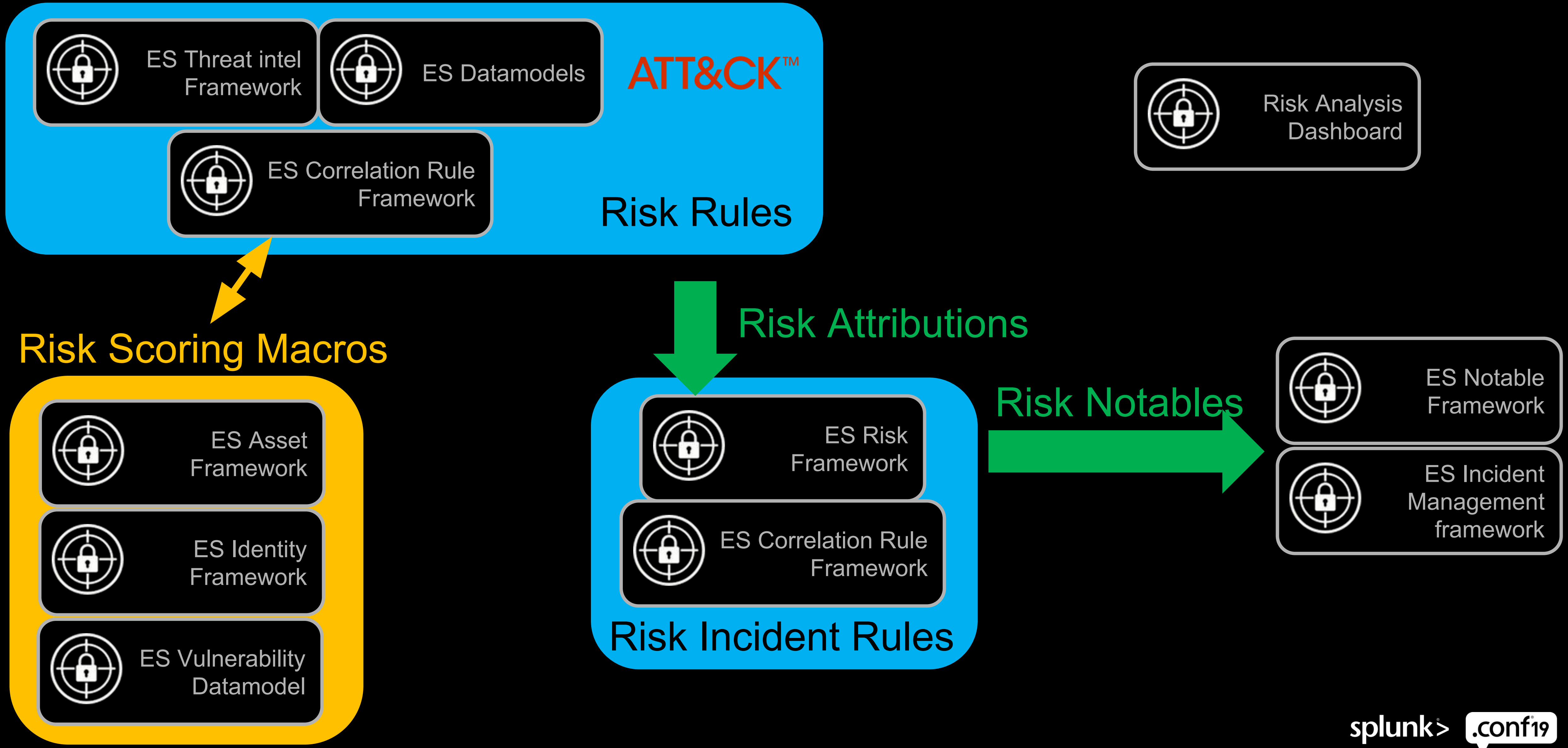
Risk Score

ATT&CK Tactics

Score/BU

Alerting

RBA Using Enterprise Security



ES Threat intel Framework

ES Datamodels

ATT&CK™

ES Correlation Rule Framework

Risk Rules

Risk Analysis Dashboard

Risk Scoring Macros

ES Asset Framework

ES Identity Framework

ES Vulnerability Datamodel

Risk Attributions

ES Risk Framework

ES Correlation Rule Framework

Risk Incident Rules

Risk Notables

ES Notable Framework

ES Incident Management framework

Benefits of RBA

Reduce Alerts

Leverage risk as a layer of abstraction

Improved Detections

Dramatic increase in the true positive rate

Quantified Maturity

Easier to align with a framework like MITRE ATT&CK for data sources, detections, and purple teaming

Analyst Scale

Decouple # detections and data sources from the linear scaling of the SOC analysts

Increased Analytics Window

Ability to look across much larger windows for low and slow. Red team's job is MUCH harder

Easy to Deploy

Easier to map against an industry framework than general use cases. Easy to integrate with SSE and ESCU

After viewing the presentation at 2018 .conf on RBA, we quickly set out to adopt the approach in our Security Operations. In January of 2019, before implementing RBA, we saw a 7.07% True Positive Rate. The next month we rose to a 19% True Positive Rate. In quarter two of 2019 we have been able to maintain a 33% True Positive Rate using the RBA system while also onboarding 29 new correlation searches. Quantifying threats has empowered our small security operations team to scale with evolving threats without overwhelming us.”

Kelby Shelton - Cybersecurity Engineer - Children’s Mercy Hospitals and Clinics

The Situation

Texas Instruments (TI) and Risk-Based Alerting (RBA)

The Situation

Why we decided to go down the RBA path

- Fear of what we are missing
  - Too many alerts to handle
  - SOCs have to be selective and hope you are looking at the most impactful alerts
- Do more with less
  - Never enough people; need to optimize efficiency with what you currently have
  - Close to **3 million** job shortage of cybersecurity professionals
    - ISC2 Cybersecurity Workforce Study, 2018

The Situation

Goals of this talk

- Illustrate the real world benefits of this approach
- Be forthcoming with our discoveries to help your ramp up

- Not a deep dive into risk mechanics, scoring, macros, etc.
  - SEC1479 - Say Goodbye to Your Big Alert Pipeline, and Say Hello to Your New Risk-Based Approach (.conf18)

The Situation

Overview of TI’s environment

- Organization
  - ~50,000 endpoints
  - ~33,000 users
- Diverse global infrastructure
  - Large Manufacturing, Lab, Design, Administration networks
  - Every OS under the sun
  - Many remote users

The Situation

Tremendous success and discoveries with RBA

- Embarked on journey after .conf18
- Seamless integration to MITRE ATT&CK
- Well tuned risk scoring to assets and identities
  - Use of subnet, assets, and identities for modifiers
- Utilize Risk flexibility
  - Risk Object Types (systems, users, external, expanding insider threat)
  - Cases abstracted from Risk (malware, policy violations, misconfigurations, etc.)
  - Great place to hunt and check risk objects over long periods of time

The Situation

By the numbers

80 + **70,000** + **4**

Risk attribution rules

Average RBA attributions per day

Risk Incident Rules (Notables)

TI RBA Timeline

Walk-through of TI’s RBA growth

.conf19

splunk>

TI RBA Timeline

5 RBA rules

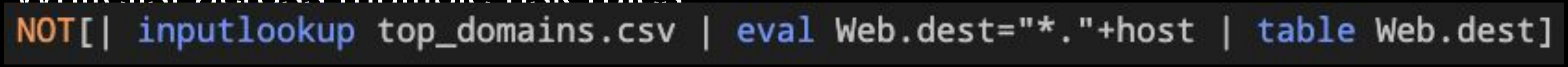
- The first risk rule is the hardest
- Not sure where to start?
  - AV detections
  - IDS events
  - Proxy blocks
  - Proxy non-HTTP/S port traffic
  - Proxy uncategorized traffic

- Pull as much investigative worthy context into Risk
  - User agents, HTTP Methods, HTTP Content type, Ports, etc.
- Immediately saw wins solely based on attributions by risk object

TI RBA Timeline

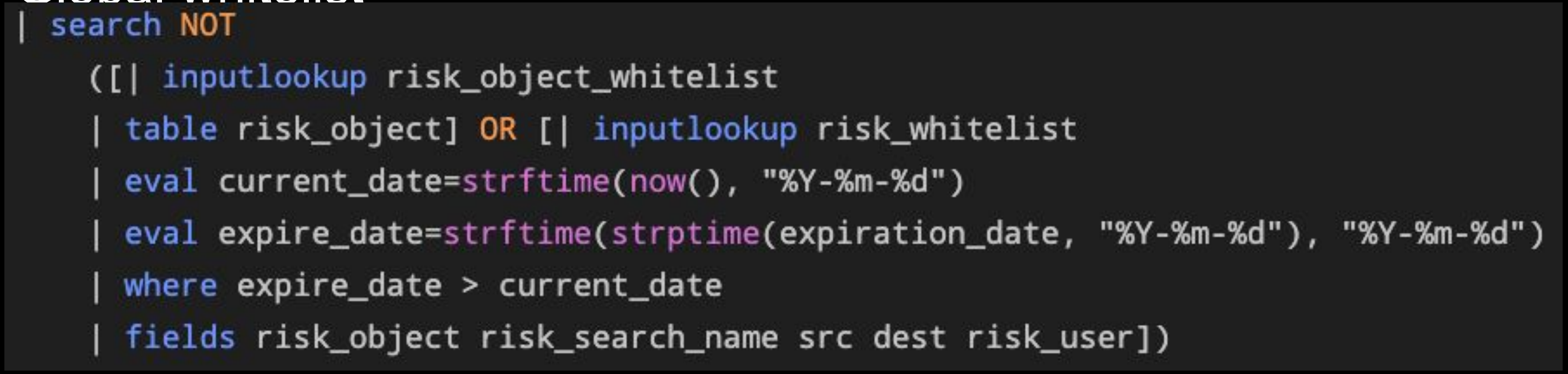
10-15 RBA rules

- Evolved whitelisting strategy
  - Whitelist per risk rule
    - Spend more time tuning and evaluating a rule
  - Whitelist across multiple risk rules



```
NOT[| inputlookup top_domains.csv | eval Web.dest="*."+host | table Web.dest]
```

  - Global whitelist

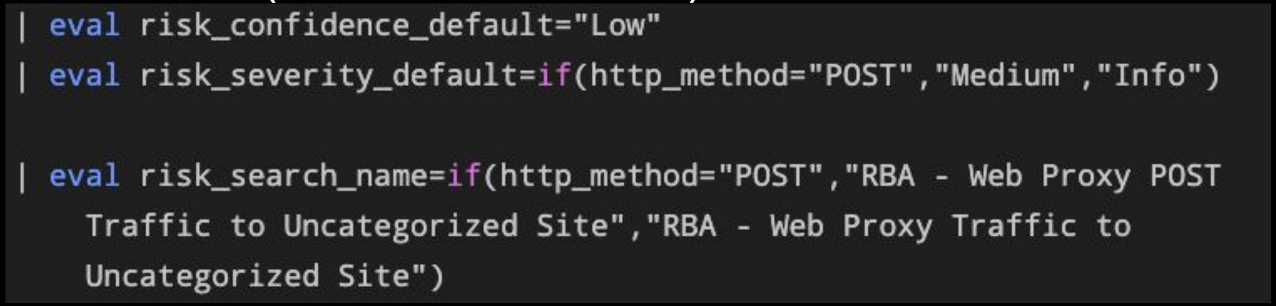


```
| search NOT
    ([| inputlookup risk_object_whitelist
    | table risk_object] OR [| inputlookup risk_whitelist
    | eval current_date=strftime(now(), "%Y-%m-%d")
    | eval expire_date=strftime(strptime(expiration_date, "%Y-%m-%d"), "%Y-%m-%d")
    | where expire_date > current_date
    | fields risk_object risk_search_name src dest risk_user])
```

TI RBA Timeline

15-20 RBA rules

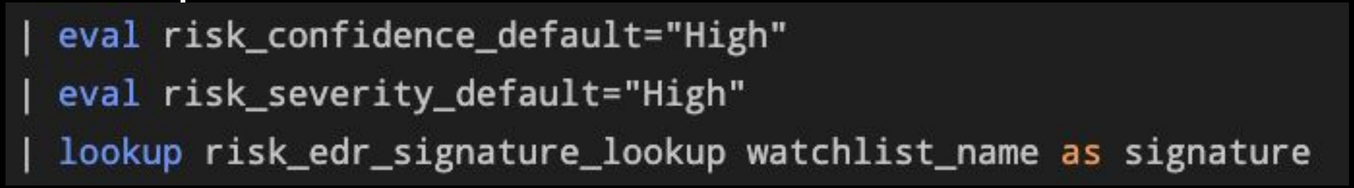
- Further matured risk scoring
  - Use Eval (if, case, coalesce)



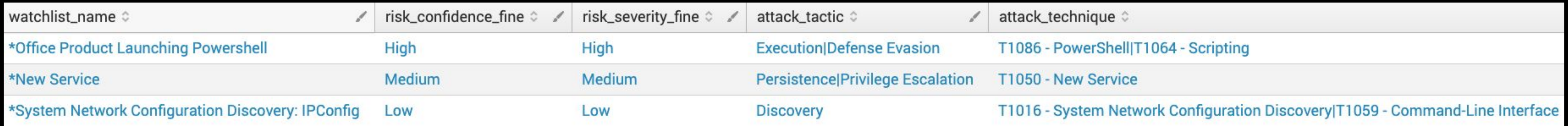
```
| eval risk_confidence_default="Low"
| eval risk_severity_default=if(http_method="POST","Medium","Info")

| eval risk_search_name=if(http_method="POST","RBA - Web Proxy POST
   Traffic to Uncategorized Site","RBA - Web Proxy Traffic to
   Uncategorized Site")
```

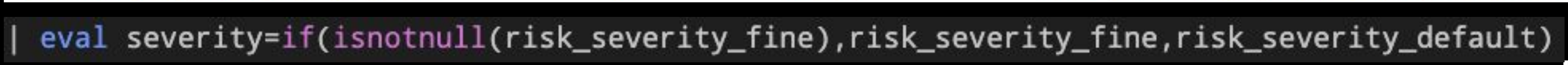
  - Lookups



```
| eval risk_confidence_default="High"
| eval risk_severity_default="High"
| lookup risk_edr_signature_lookup watchlist_name as signature
```



watchlist_name	risk_confidence_fine	risk_severity_fine	attack_tactic	attack_technique
*Office Product Launching Powershell	High	High	Execution|Defense Evasion	T1086 - PowerShell|T1064 - Scripting
*New Service	Medium	Medium	Persistence|Privilege Escalation	T1050 - New Service
*System Network Configuration Discovery: IPConfig	Low	Low	Discovery	T1016 - System Network Configuration Discovery|T1059 - Command-Line Interface



```
| eval severity=if(isnotnull(risk_severity_fine),risk_severity_fine,risk_severity_default)
```

splunk> .conf19

TI RBA Timeline

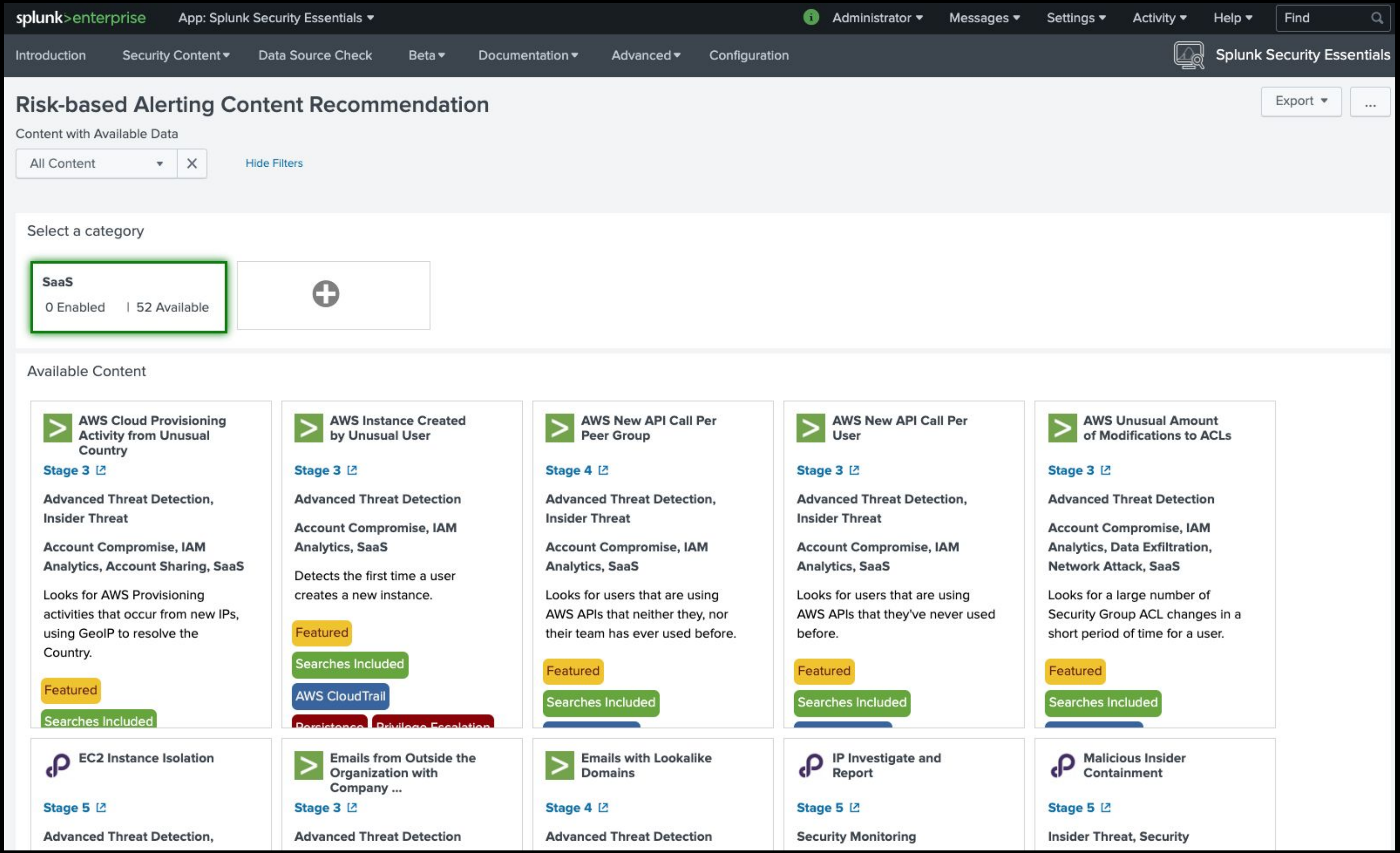
25-30 RBA rules

- Developed first RBA Notables
  - Began folding into existing alerting ecosystem
  - Tier 1 started getting to do deeper security investigations
    - Mindset change to understand an attack sequence vs alert, alert, alert
- Struggled with how to get big picture of a Risk Object
  - Created a ”Risk Object Search” dashboard to streamline investigations

TI RBA Timeline

50+ RBA rules

- Helped alpha test Splunk Security Essentials (SSE) as RBA content engine



Risk-based Alerting Content Recommendation

Content with Available Data

Select a category

SaaS
0 Enabled | 52 Available

Available Content

AWS Cloud Provisioning Activity from Unusual Country
Stage 3
Advanced Threat Detection, Insider Threat
Account Compromise, IAM Analytics, Account Sharing, SaaS
Looks for AWS Provisioning activities that occur from new IPs, using GeoIP to resolve the Country.

AWS Instance Created by Unusual User
Stage 3
Advanced Threat Detection
Account Compromise, IAM Analytics, SaaS
Detects the first time a user creates a new instance.
Persistence Privilege Escalation

AWS New API Call Per Peer Group
Stage 4
Advanced Threat Detection, Insider Threat
Account Compromise, IAM Analytics, SaaS
Looks for users that are using AWS APIs that neither they, nor their team has ever used before.

AWS New API Call Per User
Stage 3
Advanced Threat Detection, Insider Threat
Account Compromise, IAM Analytics, SaaS
Looks for users that are using AWS APIs that they've never used before.

AWS Unusual Amount of Modifications to ACLs
Stage 3
Advanced Threat Detection
Account Compromise, IAM Analytics, Data Exfiltration, Network Attack, SaaS
Looks for a large number of Security Group ACL changes in a short period of time for a user.

EC2 Instance Isolation
Stage 5
Advanced Threat Detection,

Emails from Outside the Organization with Company ...
Stage 3
Advanced Threat Detection

Emails with Lookalike Domains
Stage 4
Advanced Threat Detection

IP Investigate and Report
Stage 5
Security Monitoring

Malicious Insider Containment
Stage 5
Insider Threat, Security

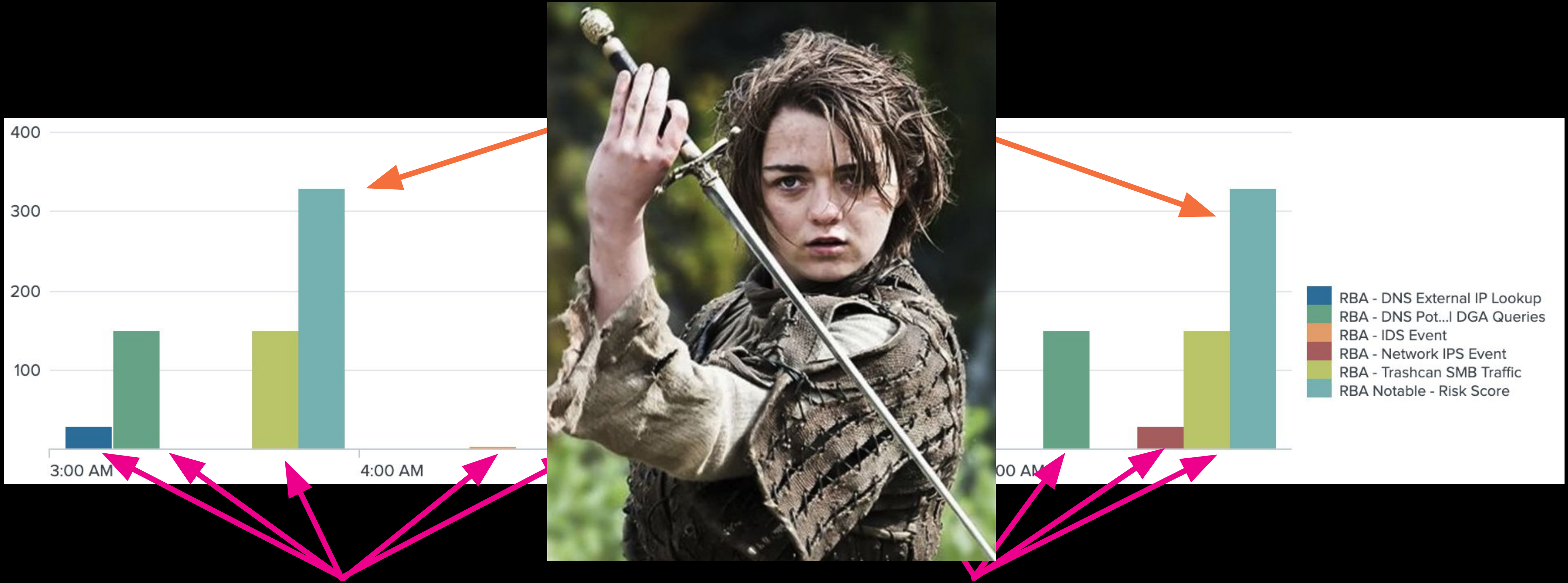
TI RBA Timeline

70+ RBA rules

- Continued building rules mapped to ATT&CK
  - Enterprise Security Content Update (ESCU) – https://splunkbase.splunk.com/app/3449/
  - Florian Roth's Sigma – https://github.com/Neo23x0/sigma
- Built "Newly seen" rules
- How do you maintain this intricate ecosystem?
  - Risk Health & Analytic Dashboard
  - Monitor failed searches
- **Attend: SEC1908** - Tales From a Threat Team: Lessons and Strategies for Succeeding with a Risk-Based Approach

Finding the Needle

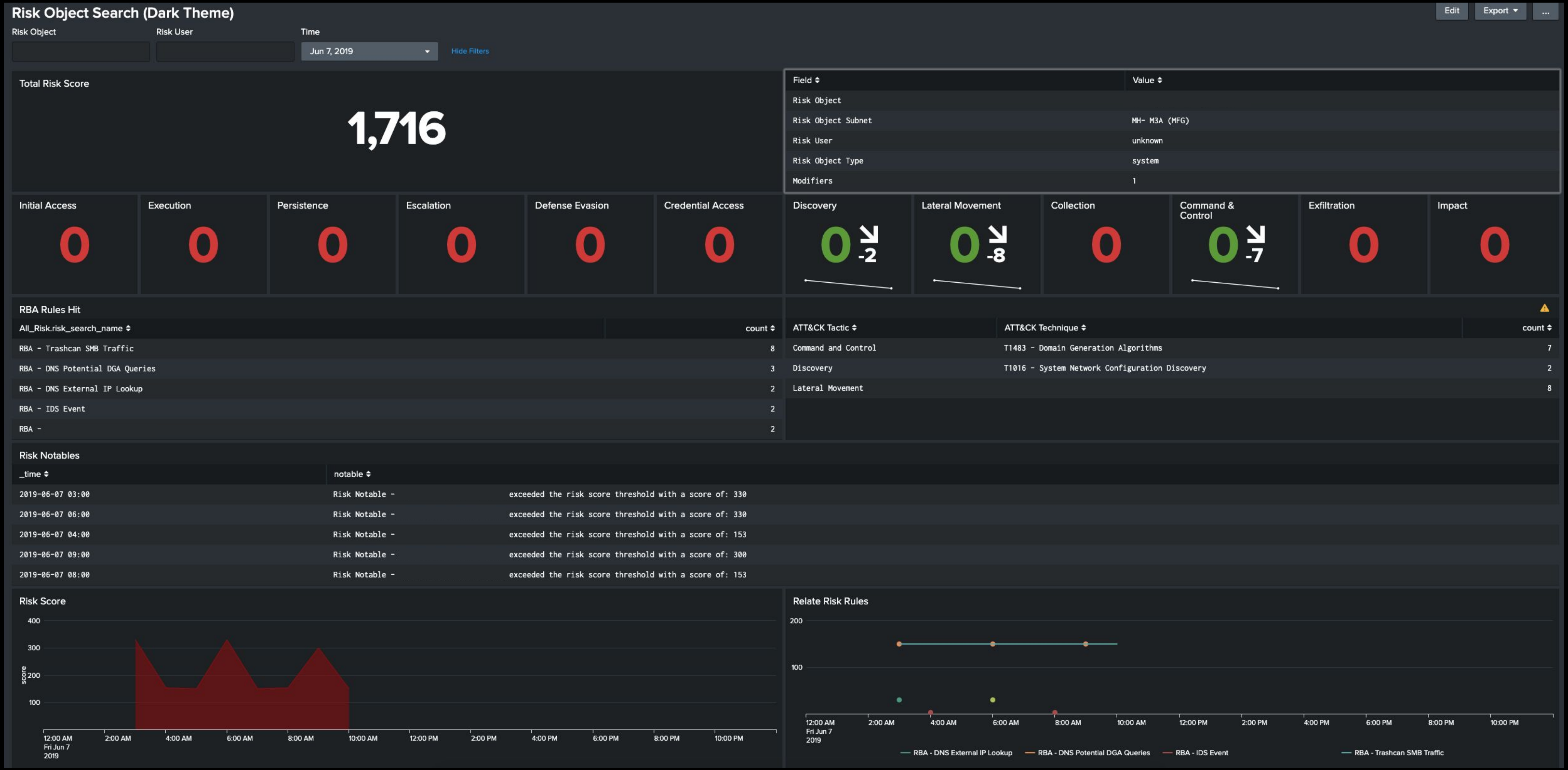
Complex detection in action



Normally lost in the ocean of noise…

The Needle

Risk Object Dashboard Glance



Risk Object Search (Dark Theme)

Risk Object

Risk User

Time: Jun 7, 2019

Total Risk Score

1,716

Field ⇕	Value ⇕
Risk Object	
Risk Object Subnet	MH- M3A (MFG)
Risk User	unknown
Risk Object Type	system
Modifiers	1

Initial Access	Execution	Persistence	Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command & Control	Exfiltration	Impact
0	0	0	0	0	0	0 ↘ -2	0 ↘ -8	0	0 ↘ -7	0	0

RBA Rules Hit

All_Risk.risk_search_name ⇕	count ⇕
RBA - Trashcan SMB Traffic	8
RBA - DNS Potential DGA Queries	3
RBA - DNS External IP Lookup	2
RBA - IDS Event	2
RBA -	2

ATT&CK Tactic ⇕	ATT&CK Technique ⇕	count ⇕
Command and Control	T1483 - Domain Generation Algorithms	7
Discovery	T1016 - System Network Configuration Discovery	2
Lateral Movement		8

Risk Notables

_time ⇕	notable ⇕
2019-06-07 03:00	Risk Notable - exceeded the risk score threshold with a score of: 330
2019-06-07 06:00	Risk Notable - exceeded the risk score threshold with a score of: 330
2019-06-07 04:00	Risk Notable - exceeded the risk score threshold with a score of: 153
2019-06-07 09:00	Risk Notable - exceeded the risk score threshold with a score of: 300
2019-06-07 08:00	Risk Notable - exceeded the risk score threshold with a score of: 153

Risk Score

Relate Risk Rules

RBA & MITRE ATT&CK

How TI leverages ATT&CK with RBA

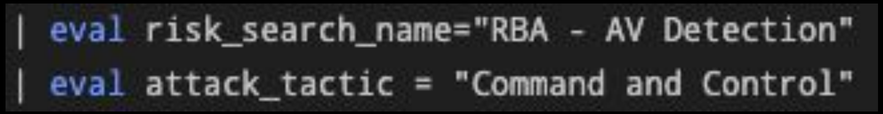
.conf19
splunk>

RBA & ATT&CK

ATT&CK all the things…

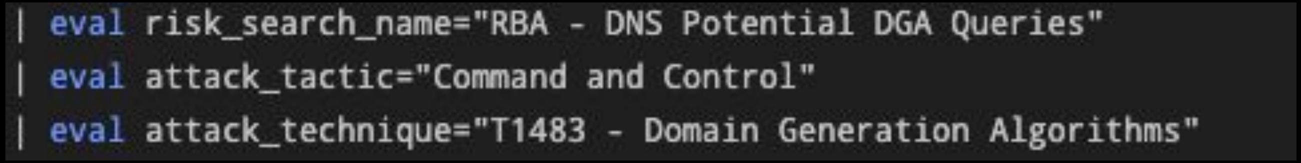
- Utilize ATT&CK to assist quantifying detection coverage
- Provides great context to an attack sequence

- Add ATT&CK Tactic attribution to all RBA rules



```
| eval risk_search_name="RBA - AV Detection"
| eval attack_tactic = "Command and Control"
```

- Add ATT&CK Technique attribution where possible to RBA rules

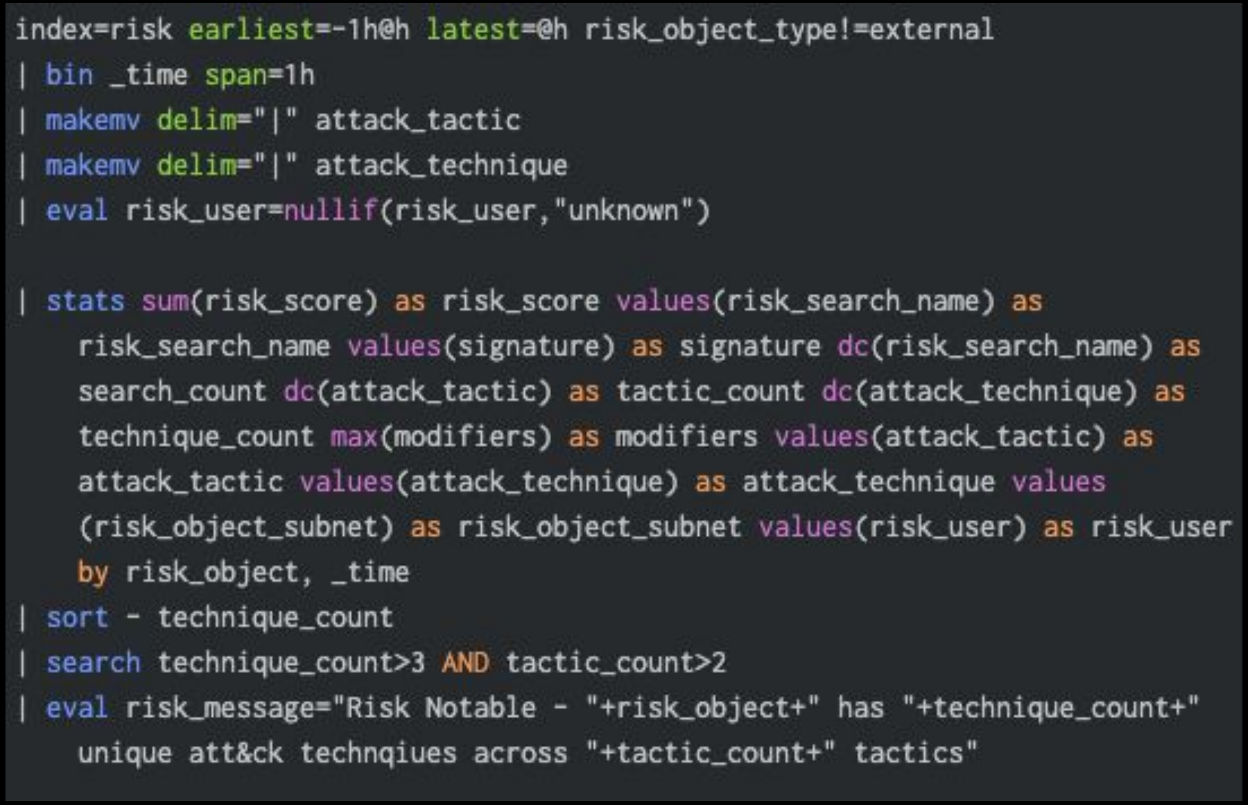


```
| eval risk_search_name="RBA - DNS Potential DGA Queries"
| eval attack_tactic="Command and Control"
| eval attack_technique="T1483 - Domain Generation Algorithms"
```

RBA & ATT&CK

Utilizing ATT&CK with RBA

- Notables look for large hits across ATT&CK
  - You can’t always depend on risk score
- Allows ability to look back for “slow and low” with quick search performance



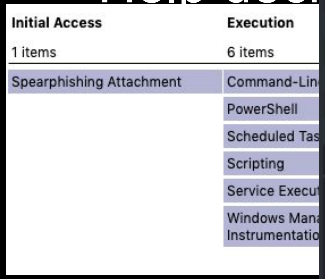
```
index=risk earliest=-1h@h latest=@h risk_object_type!=external
| bin _time span=1h
| makemv delim="|" attack_tactic
| makemv delim="|" attack_technique
| eval risk_user=nullif(risk_user,"unknown")

| stats sum(risk_score) as risk_score values(risk_search_name) as
    risk_search_name values(signature) as signature dc(risk_search_name) as
    search_count dc(attack_tactic) as tactic_count dc(attack_technique) as
    technique_count max(modifiers) as modifiers values(attack_tactic) as
    attack_tactic values(attack_technique) as attack_technique values
    (risk_object_subnet) as risk_object_subnet values(risk_user) as risk_user
    by risk_object, _time
| sort - technique_count
| search technique_count>3 AND tactic_count>2
| eval risk_message="Risk Notable - "+risk_object+" has "+technique_count+"
    unique att&ck technqiues across "+tactic_count+" tactics"
```

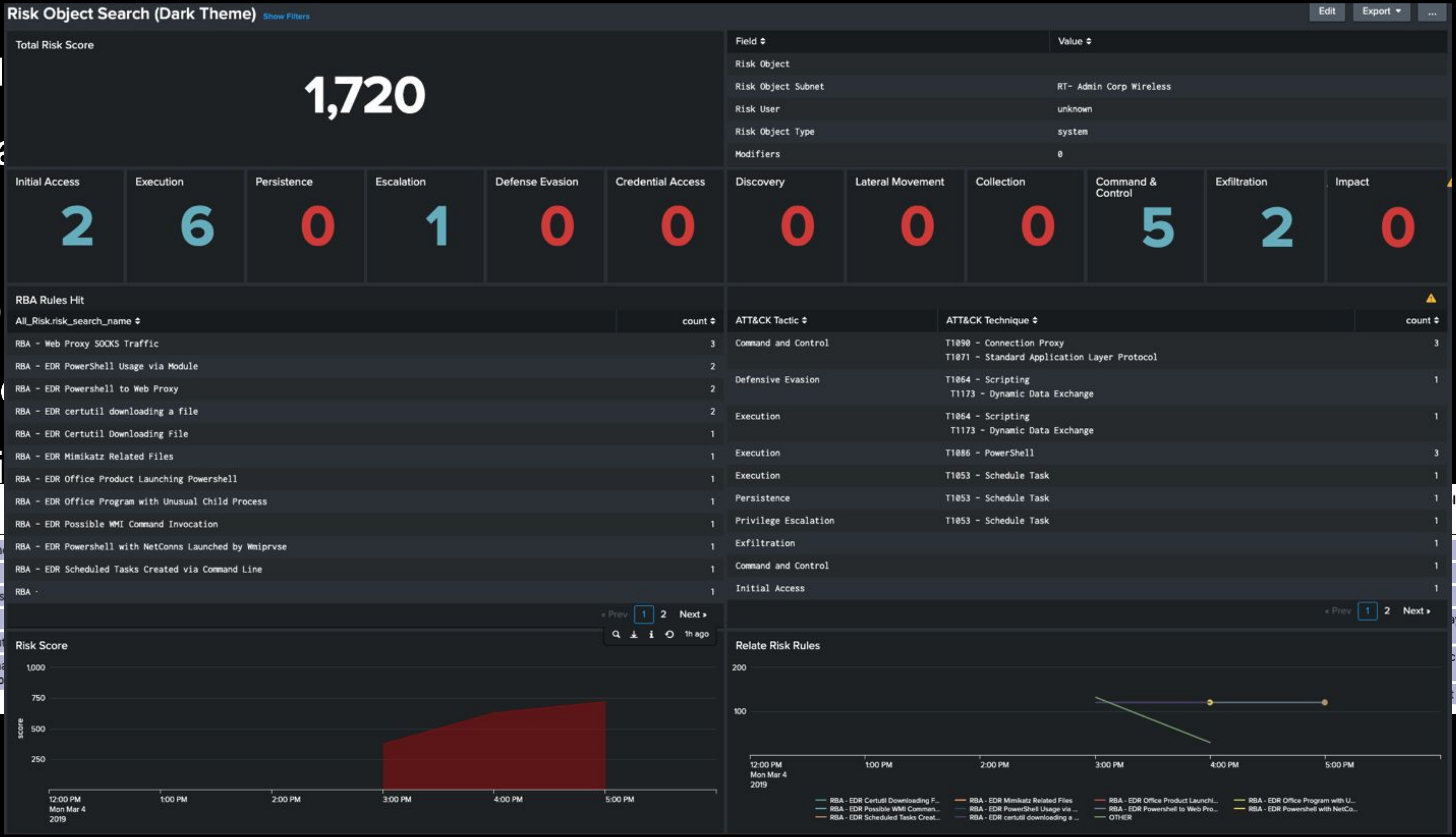
RBA & ATT&CK

Train like you fight!

- Utilize Pu
  - Develop a
  - Execute
  - Grade yo
  - Identify d
  - Help deci



Initial Access	Execution
1 items	6 items
Spearphishing Attachment	Command-Lin
	PowerShell
	Scheduled Tas
	Scripting
	Service Execu
	Windows Mana Instrumentatio



Risk Object Search (Dark Theme)

Total Risk Score

1,720

Field ⬍	Value ⬍
Risk Object	
Risk Object Subnet	RT- Admin Corp Wireless
Risk User	unknown
Risk Object Type	system
Modifiers	0

Initial Access	Execution	Persistence	Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command & Control	Exfiltration	Impact
2	6	0	1	0	0	0	0	0	5	2	0

RBA Rules Hit

All_Risk.risk_search_name ⬍	count ⬍
RBA - Web Proxy SOCKS Traffic	3
RBA - EDR PowerShell Usage via Module	2
RBA - EDR Powershell to Web Proxy	2
RBA - EDR certutil downloading a file	2
RBA - EDR Certutil Downloading File	1
RBA - EDR Mimikatz Related Files	1
RBA - EDR Office Product Launching Powershell	1
RBA - EDR Office Program with Unusual Child Process	1
RBA - EDR Possible WMI Command Invocation	1
RBA - EDR Powershell with NetConns Launched by Wmiprvse	1
RBA - EDR Scheduled Tasks Created via Command Line	1
RBA ·	1

ATT&CK Tactic ⬍	ATT&CK Technique ⬍	count ⬍
Command and Control	T1090 - Connection Proxy T1071 - Standard Application Layer Protocol	3
Defensive Evasion	T1064 - Scripting T1173 - Dynamic Data Exchange	1
Execution	T1064 - Scripting T1173 - Dynamic Data Exchange	1
Execution	T1086 - PowerShell	3
Execution	T1053 - Schedule Task	1
Persistence	T1053 - Schedule Task	1
Privilege Escalation	T1053 - Schedule Task	1
Exfiltration		1
Command and Control		1
Initial Access		1

« Prev
1
2
Next »
Risk Score
1,000
750
500
250
score
12:00 PM
Mon Mar 4
2019
1:00 PM
2:00 PM
3:00 PM
4:00 PM
5:00 PM
Relate Risk Rules
200
100
12:00 PM
Mon Mar 4
2019
1:00 PM
2:00 PM
3:00 PM
4:00 PM
5:00 PM
RBA - EDR Certutil Downloading F...
RBA - EDR Possible WMI Comman...
RBA - EDR Scheduled Tasks Creat...
RBA - EDR Mimikatz Related Files
RBA - EDR PowerShell Usage via ...
RBA - EDR certutil downloading a ...
RBA - EDR Office Product Launchi...
RBA - EDR Powershell to Web Pro...
OTHER
RBA - EDR Office Program with U...
RBA - EDR Powershell with NetCo...

Exfiltration
1 items
Exfiltration Over Command and Control Channel

Wrap Up

.conf19 splunk>

"RBA has changed how we fundamentally operate, raising visibility into the cumulative risk related to behaviors and allowing us to focus on the most impactful events."

Brandon Cass
Cyber Defense Operations Manager, Texas Instruments

RBA Related Sessions

- SEC 1556 – Building Behavioral Detections: Cross-Correlating Suspicious Activity with the MITRE ATT&CK Framework
  Tuesday, October 22, 01:45 PM - 02:30 PM

- SEC 1803 – Modernize and Mature Your SOC with Risk-Based Alerting
  Tuesday, October 22, 03:00 PM - 03:45 PM

- SEC 1538 - Getting started with Risk-Based Alerting and MITRE
  Wednesday, October 23, 12:30 PM - 01:15 PM

- SEC 1908 – Tales from a Threat Team: Lessons and Strategies for Succeeding with a Risk-Based Approach
  Wednesday, October 23, 03:00 PM - 03:45 PM

- Birds of the Feather – Meet the RBA community
  SUGARCANE Raw Bar Grill – Tuesday, 6:30pm – 830pm

.conf19

splunk>

Thank You!

Go to the .conf19 mobile app to

RATE THIS SESSION