We Need to Talk about the Elephant in the SOC

A High–Level Overview of the Risk Based Alerting (RBA) approach

SANS SIEM Summit 2019

Todays Speaker

Jim Apger
Staff Architect, Splunk

Data Centric Approach to a Career
Electrons
Packets
Analytics

Deploying/Improving RBA for the past 2.5 years
With Splunk for past 5.5 years

Agenda

The Problem

A Change of Perspective

Mechanics

Endgame

The Problem

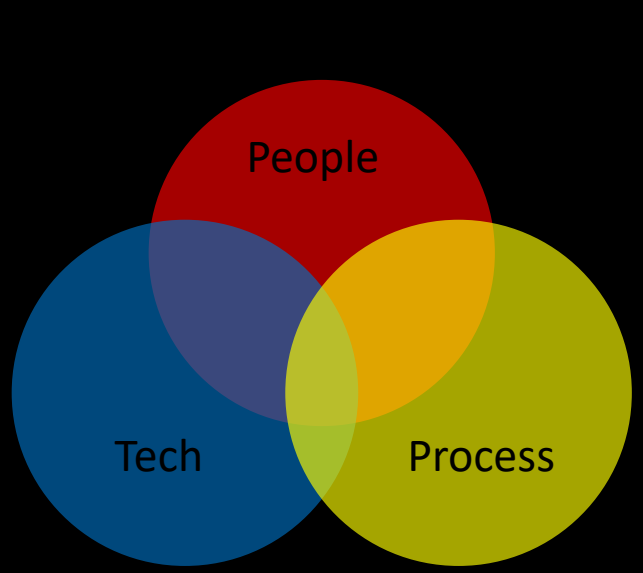
Alert Fatigue!

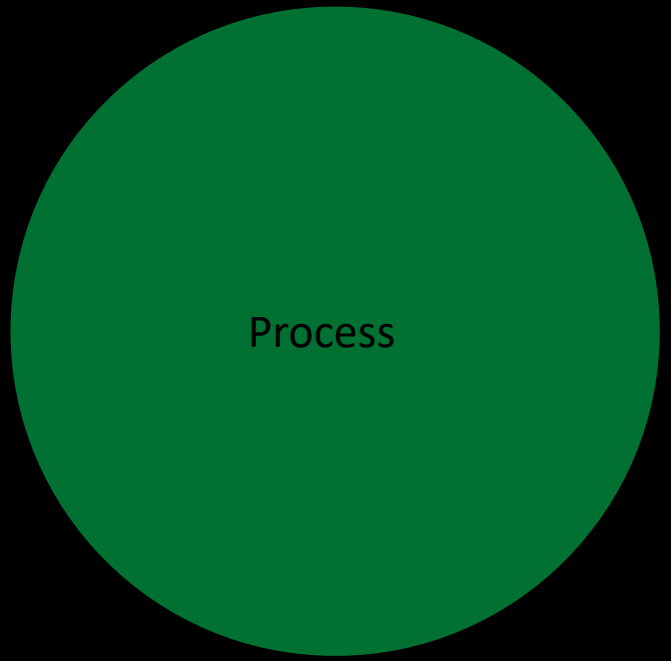
Incidents based on narrowly defined detections lead to majority noise within the SOC

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

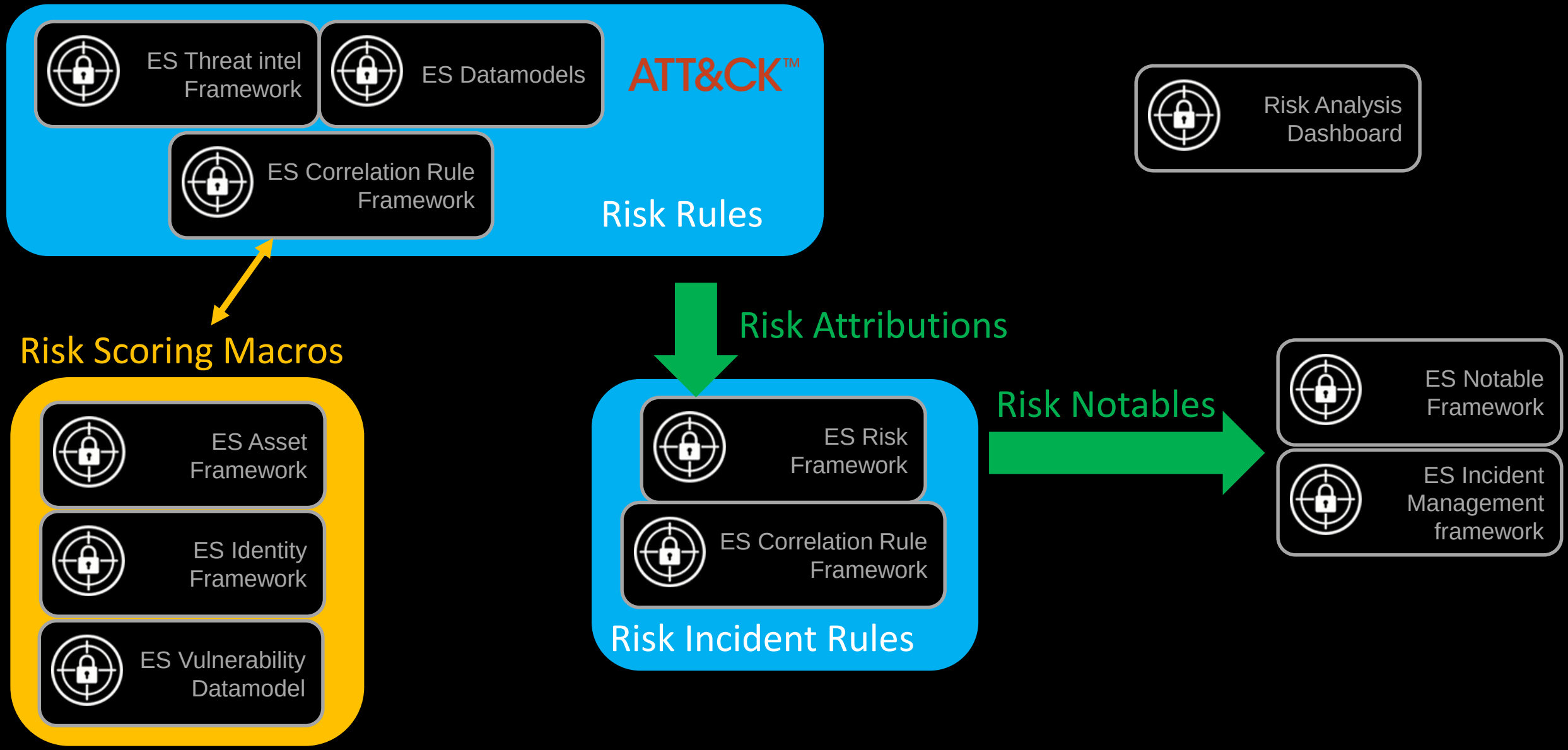
Alerting

Risk Attributions

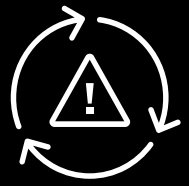
Analytics

Examine Attributions – Multiple Lenses

RBA Using a SIEM/Framework of Your Choice



Benefits of RBA



Reduce Alerts

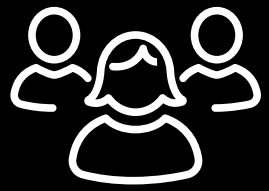
Leverage risk as a layer of abstraction

Improved Detections

Dramatic increase in the true positive rate

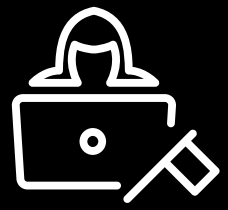
Quantified Maturity

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



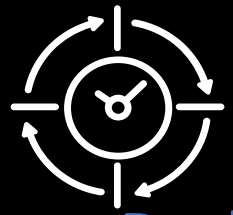
Analyst Scale

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

MITRE ATT&CK

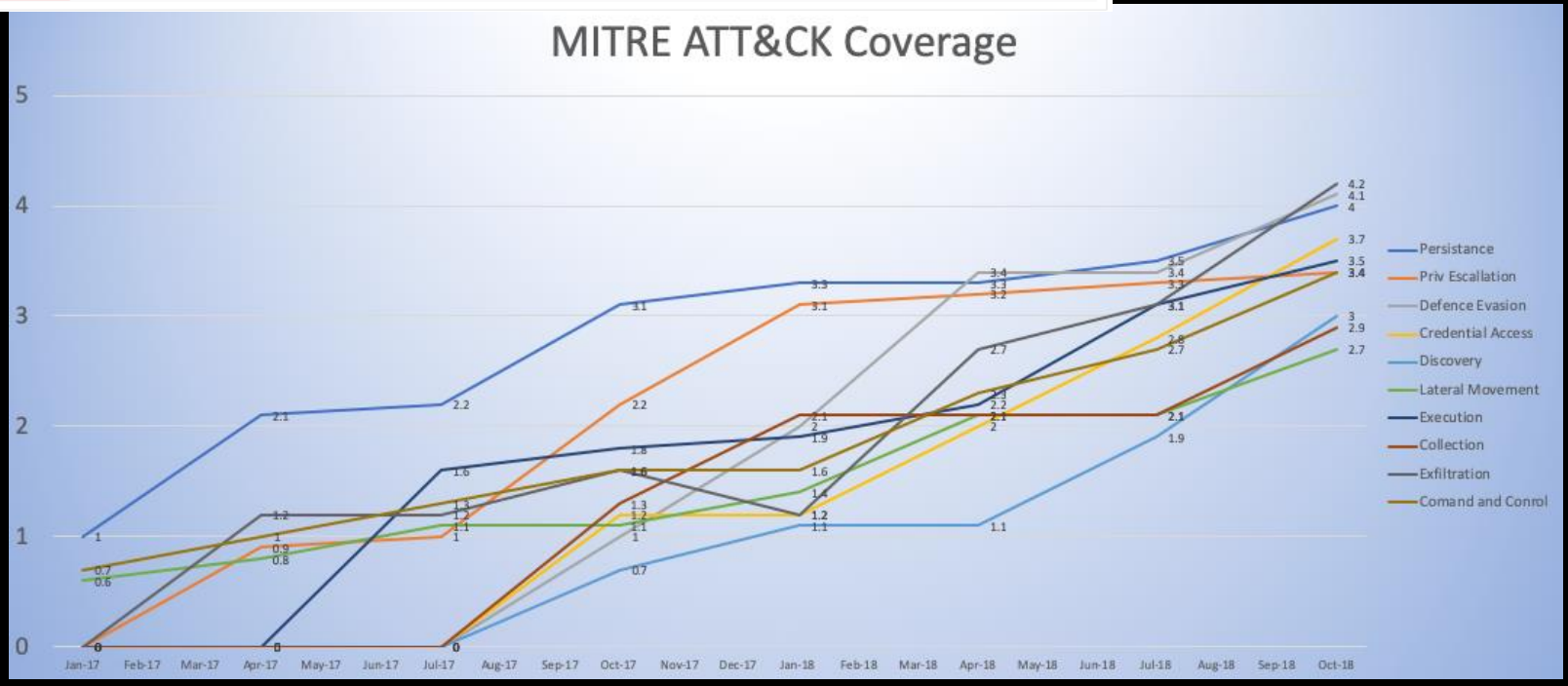
SOC Heatmap | SOC Data Source Heatmap | Purple Team | Purple Team - Scoring

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command And Control
1 items	6 items	2 items	3 items	7 items	1 items	3 items	3 items	3 items	1 items	6 items
Spearphishing Attachment	Command-Line Interface	New Service	New Service	Deobfuscate/Decode Files or Information	Credential Dumping	Account Discovery	Pass the Hash	Clipboard Data	Exfiltration Over Command and Control Channel	Data Encoding
	PowerShell	Scheduled Task	Process Injection	Indicator Blocking		File and Directory Discovery	Remote File Copy	Data from Local System		Multi-Stage Channels
	Scheduled Task		Scheduled Task	Indirect Command Execution		Network Share Discovery	Windows Admin Shares	Screen Capture		Remote File Copy
	Scripting			Masquerading						Standard Application Layer Protocol
	Service Execution			Obfuscated Files or Information						Standard Cryptographic Protocol
	Windows Management Instrumentation			Process Injection						Uncommonly Used Port
				Scripting						

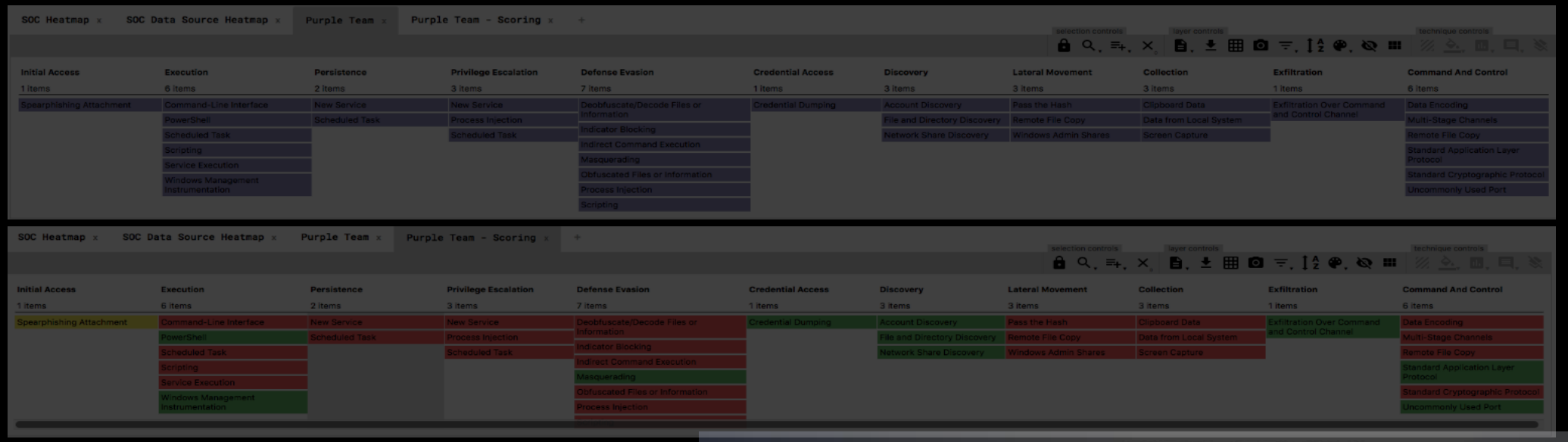
SOC Heatmap | SOC Data Source Heatmap | Purple Team | Purple Team - Scoring

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command And Control
1 items	6 items	2 items	3 items	7 items	1 items	3 items	3 items	3 items	1 items	6 items
Spearphishing Attachment	Command-Line Interface	New Service	New Service	Deobfuscate/Decode Files or Information	Credential Dumping	Account Discovery	Pass the Hash	Clipboard Data	Exfiltration Over Command and Control Channel	Data Encoding
	PowerShell	Scheduled Task	Process Injection	Indicator Blocking		File and Directory Discovery	Remote File Copy	Data from Local System		Multi-Stage Channels
	Scheduled Task		Scheduled Task	Indirect Command Execution		Network Share Discovery	Windows Admin Shares	Screen Capture		Remote File Copy
	Scripting			Masquerading						Standard Application Layer Protocol
	Service Execution			Obfuscated Files or Information						Standard Cryptographic Protocol
	Windows Management Instrumentation			Process Injection						Uncommonly Used Port

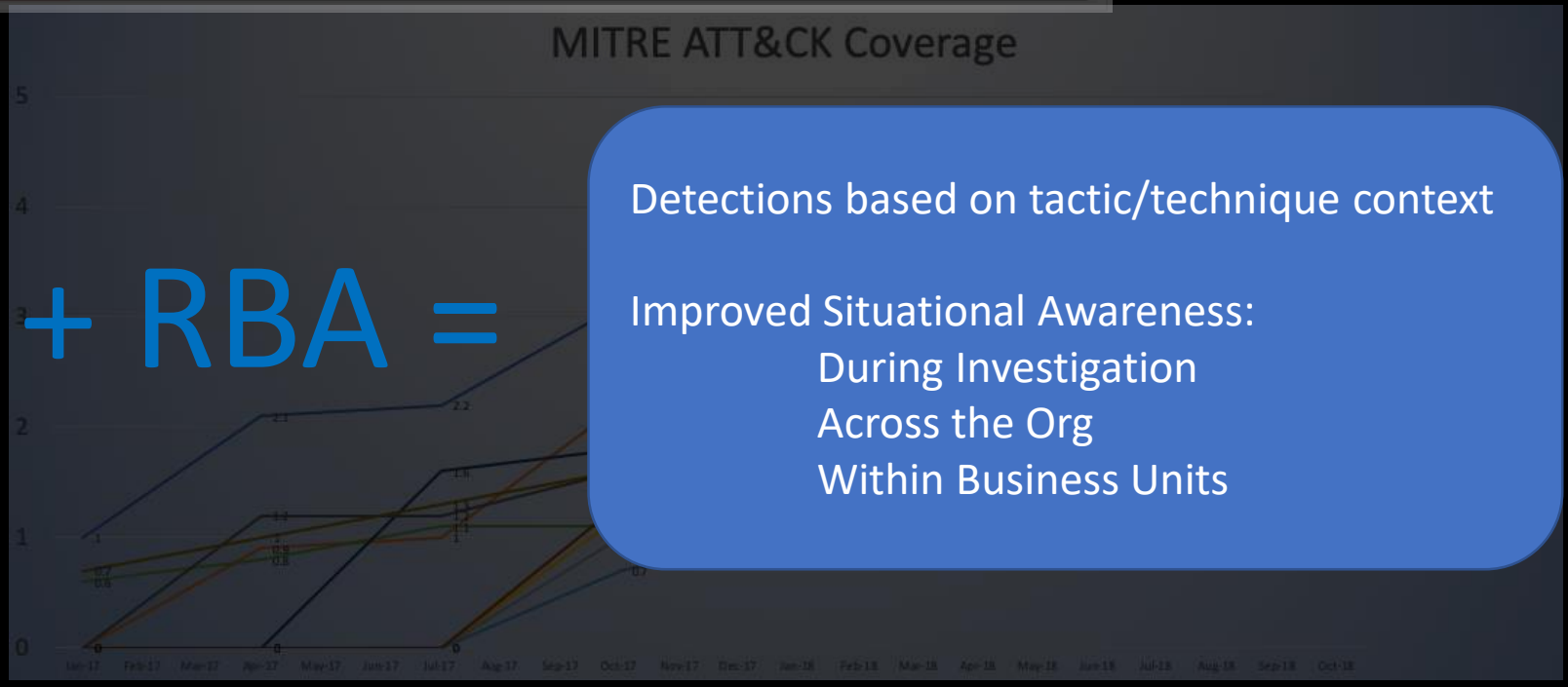
- Transparency with Leadership
- Sense of Community
- Prioritize new data source selection
- Purple team control validation



MITRE ATT&CK AMPLIFIED



- Transparency with Leadership
- Collaborate within the Enterprise
- Prioritize new data source selection
- Purple team control validation



2 Types of Analytics with RBA

Objects | Edit selection | Type: Correlation Search | App: SA-RBA | Status: All | filter | Clear filters | 25 per page

Name	Type	App	Next Scheduled Time	Actions
RIR - 24 hour risk threshold exceeded	Correlation Search	SA-RBA		Enable | Disabled
RIR - 7 day ATT&CK Tactic threshold exceeded	Correlation Search	SA-RBA		Enable | Disabled
RR - DDNS Activity Detected - System	Correlation Search	SA-RBA		Enable | Disabled
RR - DNS Activity to External IP Detected - System	Correlation Search	SA-RBA		Enable | Disabled
RR - Process Discrepancy Detected - System	Correlation Search	SA-RBA		Enable | Disabled
RR - Prohibited Process Detected - System	Correlation Search	SA-RBA		Enable | Disabled
RR - Threat Intel Match on DNS Domain request - System	Correlation Search	SA-RBA		Enable | Disabled
RR - USB Insertion with 1st time seen Serial Number - Combine	Correlation Search	SA-RBA		Enable | Disabled
RR - USB Insertion with 1st time seen Vendor ID - Combined	Correlation Search	SA-RBA		Enable | Disabled

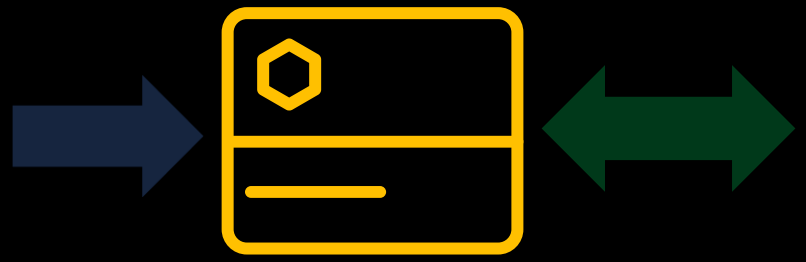
Risk Rules (attributions)

Risk Incident Rules

Create Incident

2 Types of Analytics

Risk Rules (attributions)



Risk Incident Rules

Some sort of high speed container full of beautiful attributions

Your data is trying to tell you a story

Go easy on the whitelisting

Layer of abstraction between analytics and detection

2 Types of Analytics

Risk Rules (attributions)

Risk Incident Rules

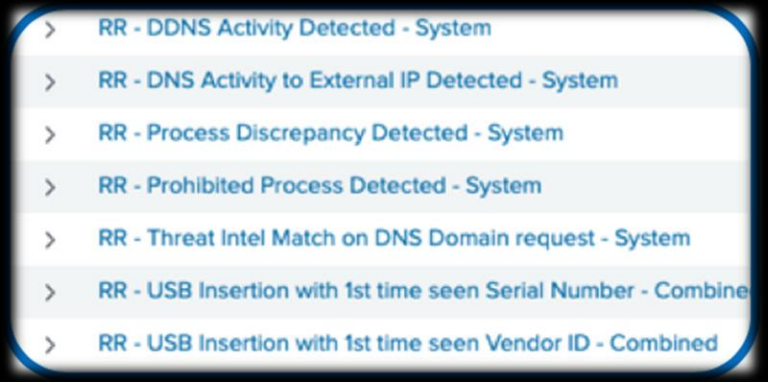
Investigative Worthy attributions

May not have scores/ATT&CK context

Scores weighted by asset/identity category

Bonus – weight by VM crits on system

1st Risk Rule is the hardest!

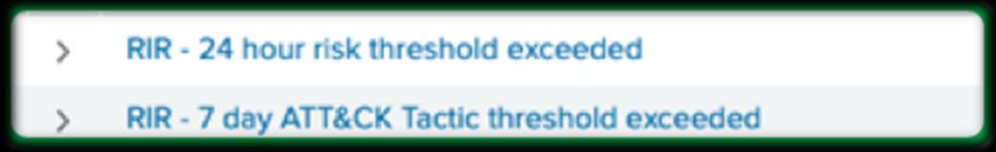


2 Types of Analytics

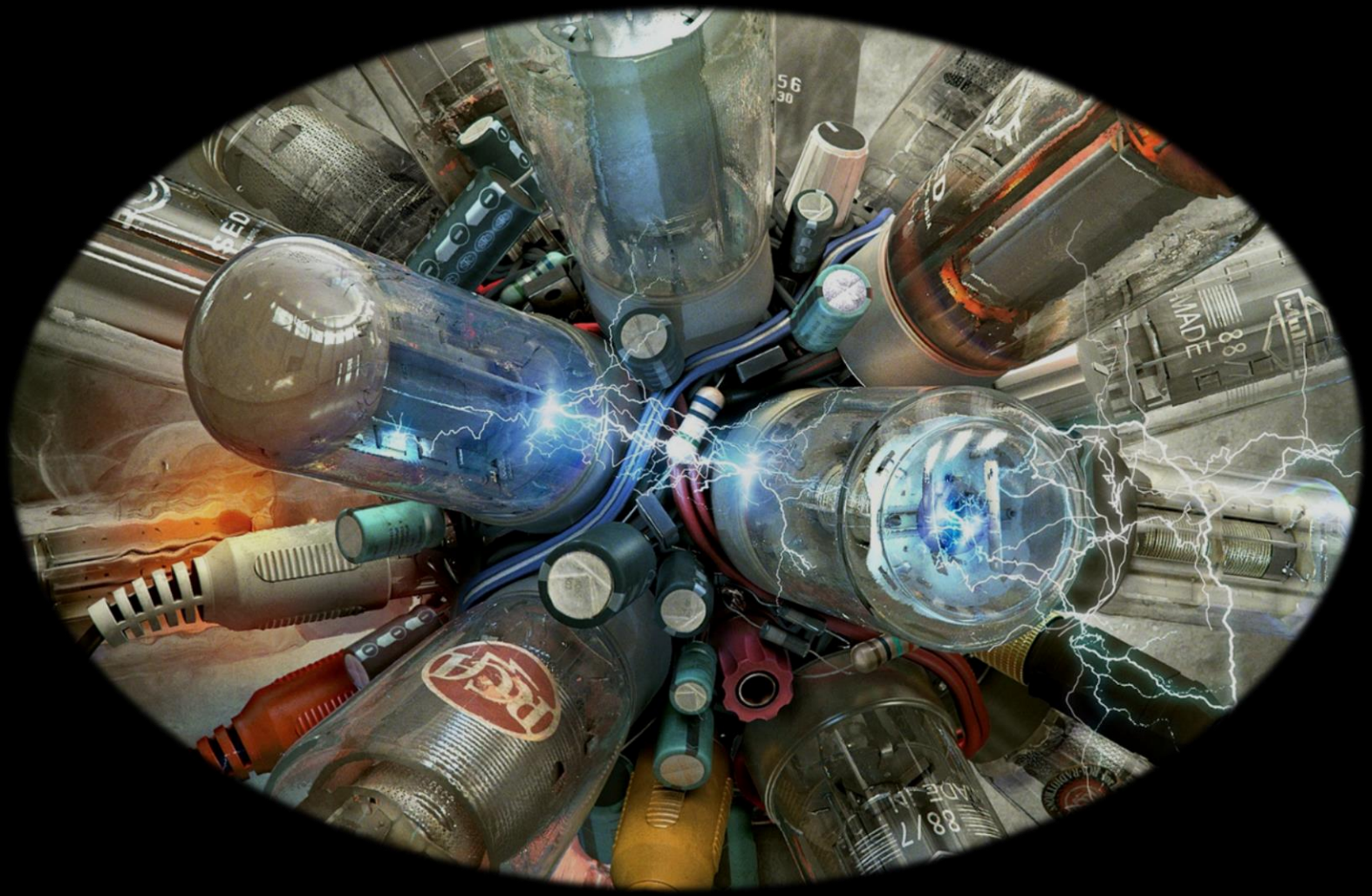
Risk Rules (attributions)

Risk Incident Rules

- Only 2-3 rules typically
- These create alerts/incidents
- Analyze the attributions via multiple lenses
- Incidents contain so much more context
- Dedup based on # tactics/techniques/sources



Mechanics



Scoring Macros

Risk Rule (attributions)

Risk Incident Rule

Resultant Alert/Incident

Investigative Dashboard

Example Risk Attribution Macro

risk_score_user(impact,confidence,object,category)

```
|eval risk_object_type="user" |eval risk_object=$object$ |eval risk_rule_impact=lower("$impact$")
|eval risk_rule_confidence=lower("$confidence$") |eval risk_user_category=$category$

|lookup rba_impact label as risk_rule_impact OUTPUT value as risk_rule_impact_num

|lookup rba_confidence label as risk_rule_confidence OUTPUT value as risk_rule_confidence_num

| eval risk_mod_count=0
| eval risk_mod_count=if(like(risk_user_category,"%privileged%"),risk_mod_count+1,risk_mod_count)
| eval risk_mod_count=if(like(risk_user_category,"%service-account%"),risk_mod_count+1,risk_mod_count)
| eval risk_mod_count=if(like(risk_user_category,"%contractor%"),risk_mod_count+1,risk_mod_count)
| eval risk_mod_count=if(like(risk_user_category,"%executive_assistant%"),risk_mod_count+1,risk_mod_count)
| eval risk_mod_count=if(like(risk_user_category,"%executive%"),risk_mod_count+1,risk_mod_count)
| eval risk_mod_count=if(like(risk_user_category,"%watchlist%"),risk_mod_count+1,risk_mod_count)
| eval risk_mod_count=if(like(user_bunit,"%Executives%"),risk_mod_count+1,risk_mod_count)
| eval risk_mod_count=if(watchlist="true",risk_mod_count+1,risk_mod_count)
|rename risk_mod_count as risk_modifier_count_user
|fillnull risk_modifier_count_user

|eval risk_score=risk_rule_impact_num * risk_rule_confidence_num * ((risk_modifier_count_user * .25)+1)

|collect index=risk
```

Values passed into macro

Impact

Confidence

Modifiers

SCORE

Write results

Example Risk Rule

Common correlation search

Message specific to the attribution

Align with ATT&CK

Risk macro

```
| from datamodel:Network_Resolution.DNS
| search _time < 1501848000 record_type="A" `Exclude_DNS_Server_src_ip`
| eval list="iana" | `ut_parse(query,list)` | fields ut_domain,src,query
| bucket _time span=5m
| stats count by ut_domain,query,src _time
| lookup DDNS_lookup domain as ut_domain
| search provider=*
|lookup dhcpLogs dest_ip as src OUTPUT dest_nt_host as host

|eval risk_message="DDNS activity detected (".ut_domain.") via query=".query." and provider=".provider

|eval rule_attack_tactic_technique=
"establish_and_maintain_infrastructure - T1333 - Dynamic DNS - https://attack.mitre.org/techniques/T1333/
|command_and_control - T1071 - Standard Application Layer Protocol -
https://attack.mitre.org/techniques/T1071/
|adversary_opsec - T1311 - Dynamic DNS - https://attack.mitre.org/techniques/T1311/"


`risk_score_system(low,low,host,src_category,src_priority)`
```

Example Risk Incident Rule

Common Data Fetch

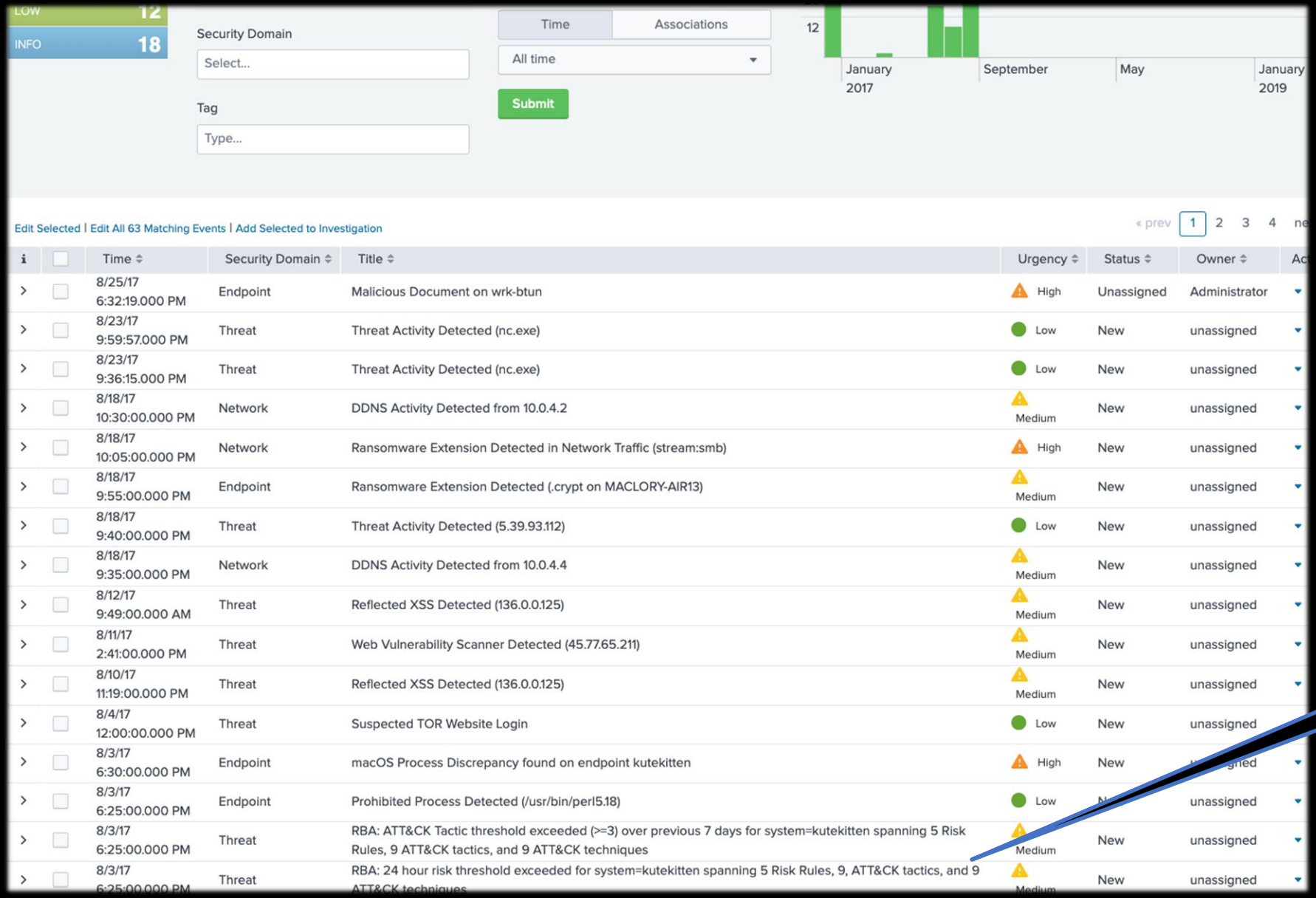
Build Constraints/Context

Apply Constraints

```
|from datamodel:"Risk.All_Risk"|search source="Threat - RR*"
|table risk_object risk_object_type risk_message source risk_score rule_attack_tactic_technique
|eventstats sum(risk_score) as risk_scoreSum by risk_object
|makemv delim="|" rule_attack_tactic_technique
|mvexpand rule_attack_tactic_technique
|rex field=rule_attack_tactic_technique "(^|\|)(?<tactic>.+?) - (?<tactic_num>.+?) - (?<technique>.+?) - (?<technique_ref>.*)"

|stats values(risk_scoreSum) as risk_ScoreSum
values(risk_message) as risk_message
dc(source) as sourceCount
values(source) as source
values(rule_attack_tactic_technique) as rule_attack_tactic_technique
dc(tactic) as tacticCount
values(tactic) as tactic
dc(technique) as techniqueCount
values(technique) as technique
by risk_object,risk_object_type

|where tacticCount >=3 and sourceCount >=4

|eval message="ATT&CT Tactic threshold exceeded (>=3) over previous 7 days for ".risk_object_type."=".risk_object." spanning ".sourceCount."
Risk Rules, ".tacticCount." ATT&CK tactics, and ".techniqueCount." ATT&CK techniques"
```

This specific search is a great one for looking backward several weeks to pickup low-and-slow in a performant manner!

RBA Driven Incidents

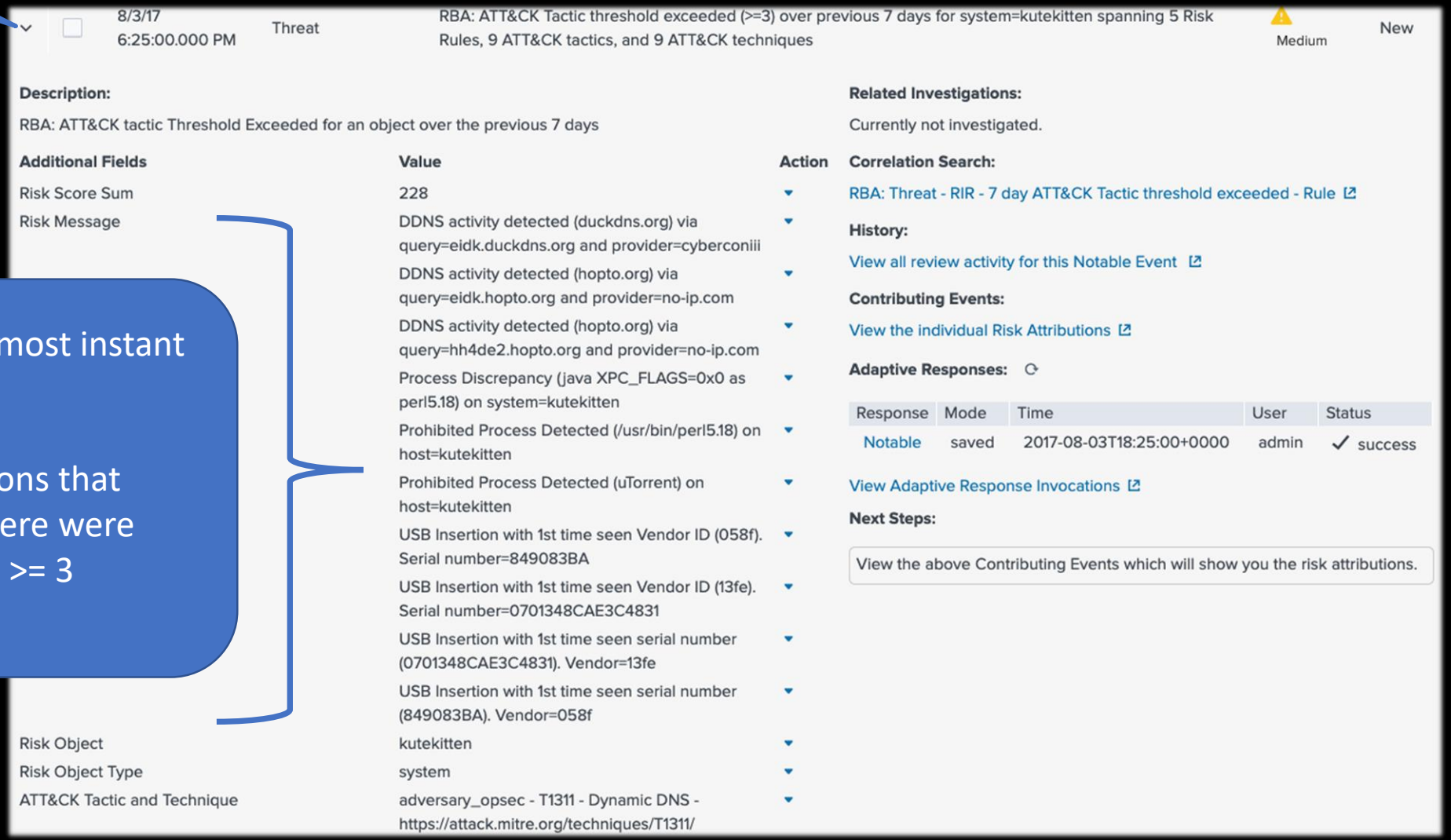


i	Time	Security Domain	Title	Urgency	Status	Owner	Act
>	8/25/17 6:32:19.000 PM	Endpoint	Malicious Document on wrk-btun	High	Unassigned	Administrator	
>	8/23/17 9:59:57.000 PM	Threat	Threat Activity Detected (nc.exe)	Low	New	unassigned	
>	8/23/17 9:36:15.000 PM	Threat	Threat Activity Detected (nc.exe)	Low	New	unassigned	
>	8/18/17 10:30:00.000 PM	Network	DDNS Activity Detected from 10.0.4.2	Medium	New	unassigned	
>	8/18/17 10:05:00.000 PM	Network	Ransomware Extension Detected in Network Traffic (stream:smb)	High	New	unassigned	
>	8/18/17 9:55:00.000 PM	Endpoint	Ransomware Extension Detected (.crypt on MACLORY-AIR13)	Medium	New	unassigned	
>	8/18/17 9:40:00.000 PM	Threat	Threat Activity Detected (5.39.93.112)	Low	New	unassigned	
>	8/18/17 9:35:00.000 PM	Network	DDNS Activity Detected from 10.0.4.4	Medium	New	unassigned	
>	8/12/17 9:49:00.000 AM	Threat	Reflected XSS Detected (136.0.0.125)	Medium	New	unassigned	
>	8/11/17 2:41:00.000 PM	Threat	Web Vulnerability Scanner Detected (45.77.65.211)	Medium	New	unassigned	
>	8/10/17 11:19:00.000 PM	Threat	Reflected XSS Detected (136.0.0.125)	Medium	New	unassigned	
>	8/4/17 12:00:00.000 PM	Threat	Suspected TOR Website Login	Low	New	unassigned	
>	8/3/17 6:30:00.000 PM	Endpoint	macOS Process Discrepancy found on endpoint kutekitten	High	New		
>	8/3/17 6:25:00.000 PM	Endpoint	Prohibited Process Detected (/usr/bin/perl5.18)	Low		unassigned	
>	8/3/17 6:25:00.000 PM	Threat	RBA: ATT&CK Tactic threshold exceeded (>=3) over previous 7 days for system=kutekitten spanning 5 Risk Rules, 9 ATT&CK tactics, and 9 ATT&CK techniques	Medium	New	unassigned	
>	8/3/17 6:25:00.000 PM	Threat	RBA: 24 hour risk threshold exceeded for system=kutekitten spanning 5 Risk Rules, 9, ATT&CK tactics, and 9 ATT&CK techniques	Medium	New	unassigned	

We see our first 2 RBA Incidents!

RBA Driven Incidents

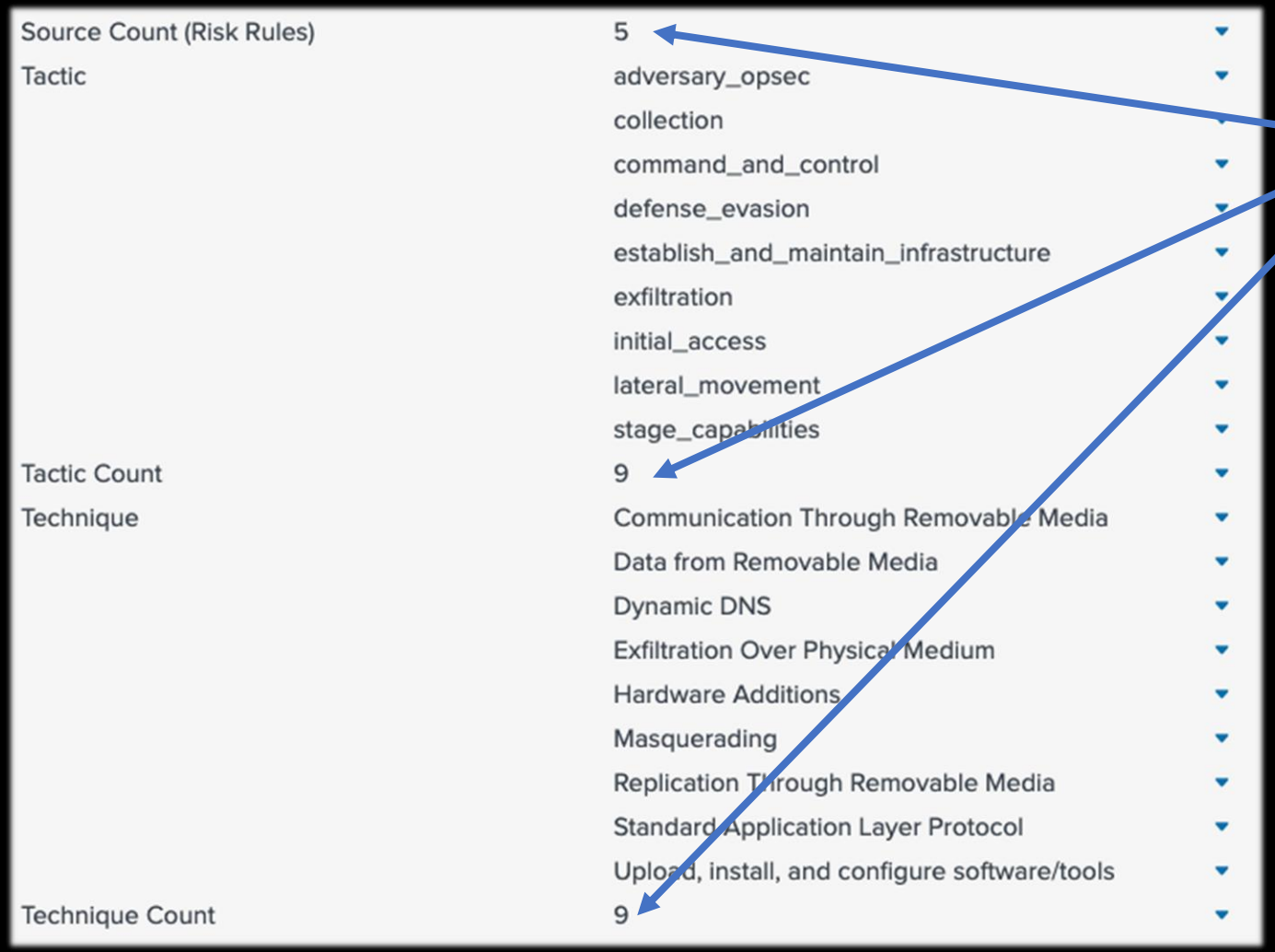
Click to Expand



Great context delivering almost instant situational awareness.

These are the risk attributions that triggered the notable as there were greater than 4 sources and >= 3 ATT&CK tactics

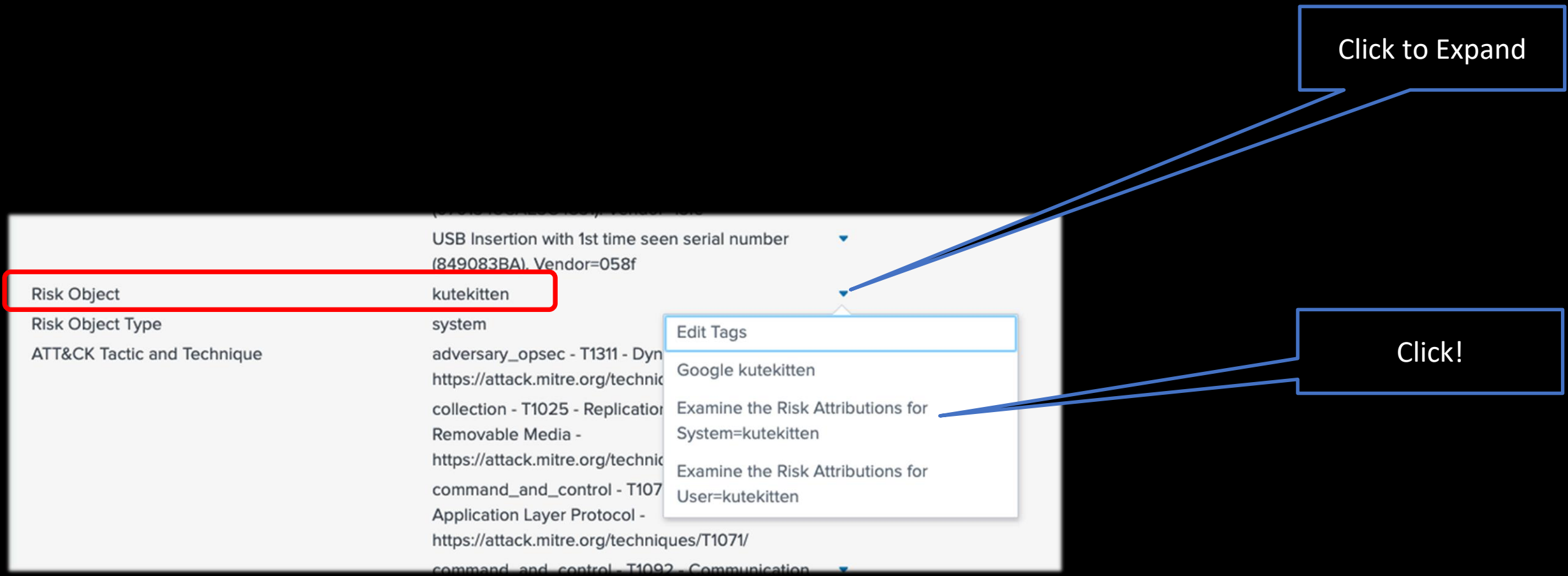
RBA Driven Incidents



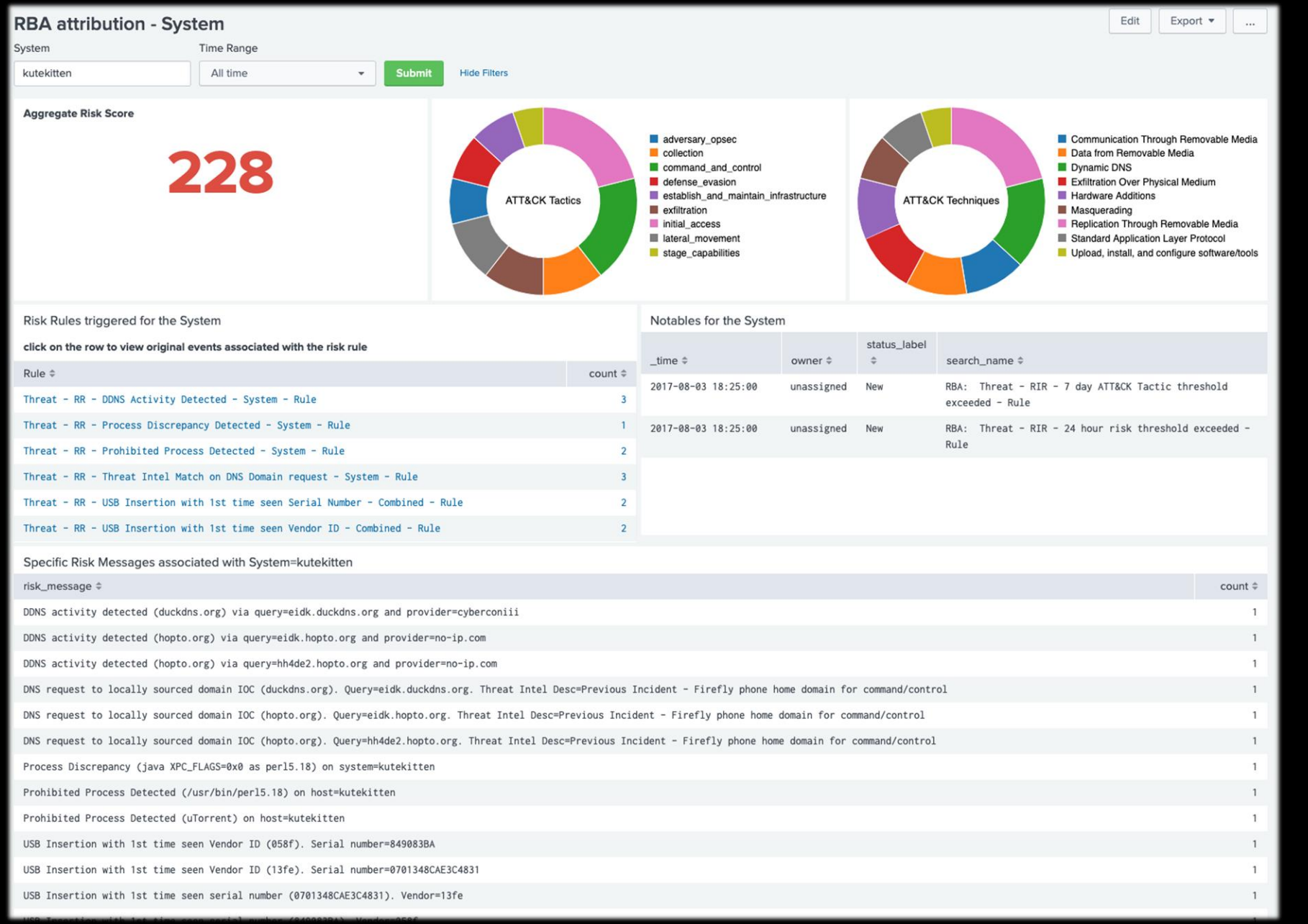
These are the fields we use for throttling (by risk_object)

Lots of throttling options. Some customers are checking for % increase in other factors like risk score.

RBA Driven Incidents



RBA attribution System/User dashboards



RBA attribution System/User dashboards

Recent Attack

Risk Rules triggered for the User

click on the row to view original events associated with the risk rule

Rule	count
Threat - RR - Command and Control Activity Detected - Combined - Rule	4
Threat - RR - Credential Theft Tool Detected - Combined - Rule	9
Threat - RR - Malware detected by Windows Defender - Combined - Rule	3
Threat - RR - Suspicious CLI command - Combined - Rule	6
Threat - RR - Suspicious CLI command related to information gathering - Combined - Rule	2
Threat - RR - Suspicious activity or known framework detected - Combined - Rule	29
Threat - RR - Suspicious activity related to escalation of privs has been detected - Combined - Rule	42
Threat - RR - Suspicious service or registry change detected - Combined - Rule	5
Threat - RR - Suspisious Process or DLL detected - Combined - Rule	11

2m ago

Inbound Phish

Meterpreter Session

Domain Fronting

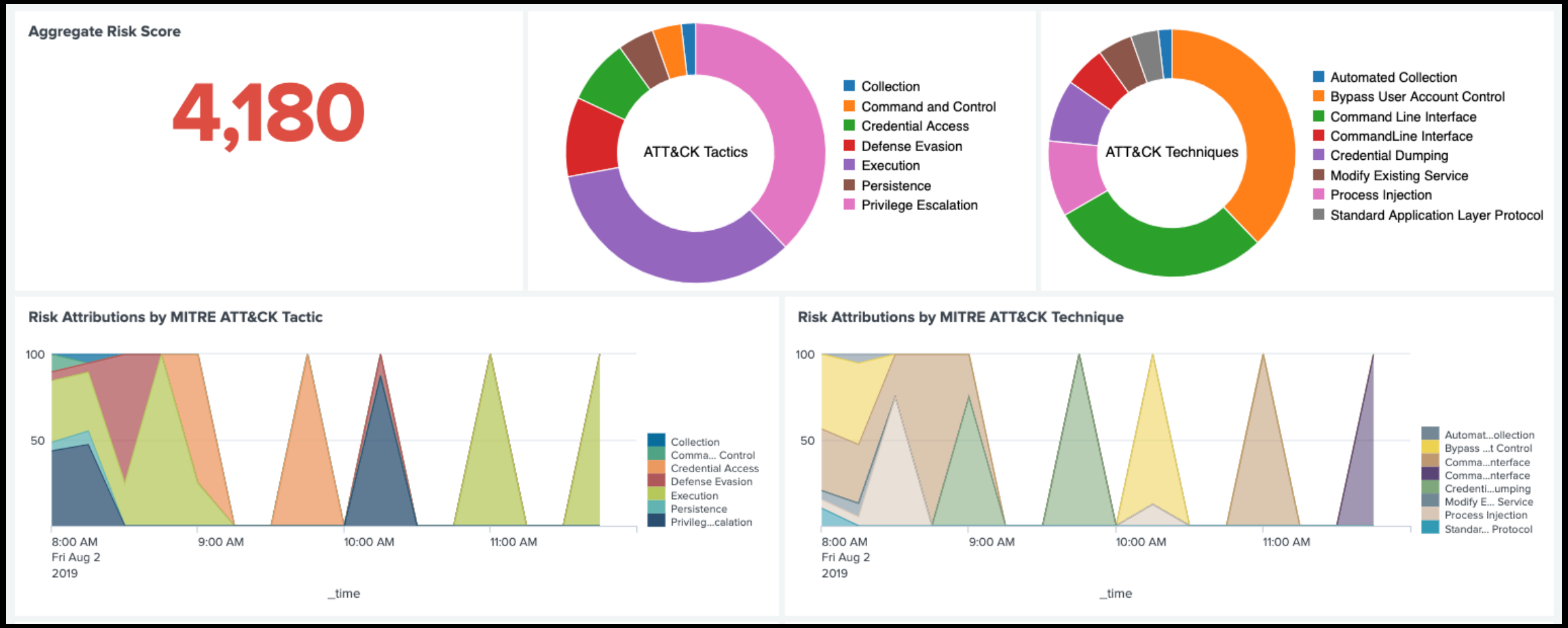
Persistence

Mimikatz

Lots of encoded powershell

RBA attribution System/User dashboards

Recent Attack (continued)



.Conf 2018 – SEC1479

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

Details a 3-month customer journey to transition SOC to a Risk Based Alerting (RBA) approach

Recording/Slides here:

https://conf.splunk.com/conf-online.html?search=%22Big%20Alert%22#/

Also of note:

https://conf.splunk.com/files/2017/slides/the-art-of-detection-using-splunk-enterprise-security.pdf

As an early contributor of the RBA process and as a Threat Hunter in a mid-sized enterprise, we increased our detections by 300%, reduced our security alerts by 50%, aligned with MITRE ATT&CK, and achieved a 60% true positive rate in the SOC in less than a year without increasing the size of the security team by leveraging a risk based approach

Stuart McIntosh, CTO Outpost Front Line