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

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

Jim Apger
Staff Architect, Splunk
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
Risk Attributions
Examine Attributions – Multiple Lenses

Risk Score

ATT&CK Tactics

Score/BU

abstraction
(Investigation Worthy)

Alerting
RBA Using a SIEM/Framework of Your Choice

- **ES Threat intel Framework**
- **ES Datamolds**
- **ES Correlation Rule Framework**

**ATT&CK™**

**Risk Rules**

**Risk Scoring Macros**

- **ES Asset Framework**
- **ES Identity Framework**
- **ES Vulnerability Datamodel**

**Risk Attributions**

**Risk Incident Rules**

**Risk Notables**

- **ES Notable Framework**
- **ES Incident Management framework**

**Risk Analysis Dashboard**
**Benefits of RBA**

**Reduce Alerts**
Leverage risk as a layer of abstraction

**Improved Detections**
Dramatic increase in the true positive rate

**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

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

**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.”
MITRE ATT&CK

- 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

Detections based on tactic/technique context

Improved Situational Awareness:
- During Investigation
- Across the Org
- Within Business Units
# 2 Types of Analytics with RBA

## Risk Rules (attributions)

- RIR - 24 hour risk threshold exceeded
- RIR - 7 day ATT&CK Tactic threshold exceeded
- RR - DDNS Activity Detected - System
- RR - DNS Activity to External IP Detected - System
- RR - Process Discrepancy Detected - System
- RR - Prohibited Process Detected - System
- RR - Threat Intel on DNS Domain request - System
- RR - USB Insertion with 1st time seen Serial Number - Combined
- RR - USB Insertion with 1st time seen Vendor ID - Combined

## Risk Incident Rules

Create Incident
2 Types of Analytics

Risk Rules (attributions) → Some sort of high speed container full of beautiful attributions → Risk Incident Rules

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)

- Investigative Worthy attributions
- May not have scores/ATT&CK context
- Scores weighted by asset/identity category
- Bonus – weight by VM crits on system

Risk Incident Rules

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

```
| 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%"),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(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(risk_watchlist="true",risk_mod_count+1,risk_mod_count) |
| rename risk_mod_count as risk_mod_risk_count_user |
| fillnull risk_mod_risk_count_user |

| eval risk_score=risk_rule_impact_num * risk_rule_confidence_num * ((risk_mod_risk_count_user * .25)+1) |
| collect index=risk |
```

**Values passed into macro**
- `impact`
- `confidence`
- `object`
- `category`

**Impact**
- `rba_impact`
- `risk_rule_impact`
- `risk_rule_impact_num`

**Confidence**
- `rba_confidence`
- `risk_rule_confidence`
- `risk_rule_confidence_num`

**Modifiers**
- `risk_mod_count`
- `risk_mod_risk_count_user`

**SCORE**
- `risk_score`

**Write results**
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/ 
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

| 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!
We see our first 2 RBA Incidents!
RBA Driven Incidents

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

- adversary_opsec
- collection
- command_and_control
- defense_evasion
- establish_and_maintain_infrastructure
- exfiltration
- initial_access
- lateral_movement
- stage_capabilities

Lots of throttling options. Some customers are checking for % increase in other factors like risk score.
<table>
<thead>
<tr>
<th>Risk Object</th>
<th>kutekitten</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk Object Type</td>
<td>system</td>
</tr>
<tr>
<td>ATT&amp;CK Tactic and Technique</td>
<td></td>
</tr>
</tbody>
</table>

**Additional Information**

- Edit Tags
  - Google kutekitten
  - Examine the Risk Attributions for System=kutekitten
  - Examine the Risk Attributions for User=kutekitten
RBA attribution System/User dashboards

Aggregate Risk Score

228

ATT&CK Tactics

ATT&CK Techniques

Notables for the System

<table>
<thead>
<tr>
<th><em>time</em></th>
<th>owner</th>
<th>status_label</th>
<th>search_name</th>
</tr>
</thead>
<tbody>
<tr>
<td>2017-06-01 06:25:00</td>
<td>unassigned</td>
<td>New</td>
<td>RBA: Threat - RIR - 7 day ATT&amp;CK tactic threshold exceeded - Rule</td>
</tr>
</tbody>
</table>

Specific Risk Messages associated with System=kutekitten

<table>
<thead>
<tr>
<th>risk_message</th>
<th>count</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS activity detected (duckdns.org) via query=weidk.duckdns.org and provider=cyberconll</td>
<td>1</td>
</tr>
<tr>
<td>DNS activity detected (hopto.org) via query=weidk.hopto.org and provider=so-iop.com</td>
<td>1</td>
</tr>
<tr>
<td>DNS activity detected (hopto.org) via query=weidk.hopto.org and provider=so-iop.com</td>
<td>1</td>
</tr>
<tr>
<td>DNS request to locally sourced domain IDC (duckdns.org). Query=weidk.duckdns.org. Threat Intel Desc=Previous Incident - Firefly phone home domain for command/control</td>
<td>1</td>
</tr>
<tr>
<td>DNS request to locally sourced domain IDC (hopto.org). Query=weidk.hopto.org. Threat Intel Desc=Previous Incident - Firefly phone home domain for command/control</td>
<td>1</td>
</tr>
<tr>
<td>DNS request to locally sourced domain IDC (hopto.org). Query=weidk.hopto.org. Threat Intel Desc=Previous Incident - Firefly phone home domain for command/control</td>
<td>1</td>
</tr>
<tr>
<td>Process Discrepancy (java XPC_FLAGS=0x8 as per[5.18]) on system=kutekitten</td>
<td>1</td>
</tr>
<tr>
<td>Prohibited Process Detected [/usr/bin/perl(18)] on host=kutekitten</td>
<td>1</td>
</tr>
<tr>
<td>USB Insertion with 1st time seen Vendor ID (15FF). Serial number=645969AB</td>
<td>1</td>
</tr>
<tr>
<td>USB Insertion with 1st time seen Vendor ID (15FF). Serial number=645969AB</td>
<td>1</td>
</tr>
<tr>
<td>USB Insertion with 1st time seen serial number (87916e0e49e4e5f). Vendor=15ff</td>
<td>1</td>
</tr>
</tbody>
</table>
## Recent Attack

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

- Inbound Phish
- Meterpreter Session
- Domain Fronting
- Persistence
- Mimikatz
- Lots of encoded powershell
RBA attribution System/User dashboards

Recent Attack (continued)

Aggregate Risk Score

4,180

Risk Attributions by MITRE ATT&CK Tactic

Risk Attributions by MITRE ATT&CK Technique
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:
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