Full Speed Ahead With Risk-Based Alerting (RBA)

Jim Apger
Staff Security Strategist | Splunk

Kyle Champlin
Principal Product Manager | Splunk
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 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.
Agenda

1) More MITRE ATT&CK
   Improvements

2) Threat Objects and SOAR
   Introduction

3) Customer Win
   Compelling

4) Enterprise Security
   Acceleration
Jim Apger

Staff Security Strategist  |  Splunk
ALERT FATIGUE

facepalm
ALERT SUPRESSION

double facepalm
The Business of SOC

Traditional Approach

Operational Costs

DNS
Endpoint/EDR
Cloud

“Highly illogical.” — Spock
The Business of SOC

RBA

“Logic is the beginning of wisdom, not the end.” — Spock
RBA Milestones
3-Year Journey

**Early Adopters**
- 2018
  - Risk Rules
  - Risk Scoring
  - MITRE ATT&CK
- Risk Index
- Risk Notables
  - .Conf18 talk

**Accelerated Adoption**
- 2019
  - SA-RBA Reference App
  - (4) .Conf19 talks
  - SANS and ISC2 talks

**Evolution**
- 2020
  - MITRE ATT&CK
  - Threat Objects
  - SOAR
  - Attack Web Viz

**Turnkey Enterprise Security**
- 2020
  - PM Updates
MITRE ATT&CK
Map to Technique

|eval mitre_technique_id="T1170"
|lookup mitredict mitre_technique_id OUTPUTNEW mitre_tactic_id
|eval risk_message="Possible use mshta.exe to proxy execution of VBScript through a trusted Windows utility. Image=".Image.".
  parent_process_path=".parent_process_path"
|eval testmode=0
|eval threat_object=Image
|eval threat_object_type="commandline"
  `risk_score_system(src,5)`
  `risk_score_user(user,5)`
MITRE ATT&CK
Add ATT&CK Context

```
| eval mitre_technique_id="T1170"
| lookup mitredict mitre_technique_id OUTPUTNEW mitre_tactic_id
| eval risk_message="Possible use mshta.exe to proxy execution of VBScript through a trusted Windows utility. Image=".Image.".parent_process_path:"
| eval testmode=0
| eval threat_object=Image
| eval threat_object_type="commandline"
| risk_score_system(src,5)
| risk_score_user(user,5)
```
MITRE ATT&CK

|inputlookup mitredict|search mitre_technique_id="T1546.011"|transpose|

-OR-

https://rbaallday.com

-OR-

Supporting Add on for MITRE

-OR-

https://raw.githubusercontent.com/mitre/cti/master/enterprise-attack/enterprise-attack.json
MITRE ATT&CK

Adversaries may establish persistence and/or elevate privileges by executing malicious content triggered by application shims. The Microsoft Windows App Infrastructure/Framework (Application Shim) was created to allow for backward compatibility of software as the operating system codebase changes over time; this feature allows developers to apply fixes to applications (without rewriting code) that were created for Windows XP so that it will work with Windows 10. (2017)

Within the framework, shims are created to act as a buffer between the program (or more specifically, the Import Address Table) and the Windows OS. When referenced to determine if the program requires the use of the shim database (.sdb). If so, the shim database uses hooking to redirect the code as needed.

A list of all shims currently installed by the default Windows installer (sdbinst.exe) is kept in:

* `<code>\Windows\AppPatch\sysmain.sdb</code>` and
* `<code>\%hmsoftware\Microsoft\Windows NT\CurrentVersion\appcompatflags\installedsdb</code>`

Custom databases are stored in:

* `<code>\Windows\AppPatch\custom & \%hmsoftware\Microsoft\Windows NT\CurrentVersion\appcompatflags\custom</code>` and
* `<code>\%hmsoftware\Microsoft\Windows NT\CurrentVersion\appcompatflags\custom</code>`

To keep shims secure, Windows designed them to run in user mode so they cannot modify the kernel and you must have administrator privileges to install and manage them. Bypass User Access Control](https://attack.mitre.org/techniques/T1548/002) (UAC and RedirectEEXE), inject DLLs into processes (InjectDLL), disable Data Structure Exception Handling (DisableSEH), and intercept memory addresses (GetProcAddress).

Utilizing these shims may allow an adversary to perform several malicious acts such as elevate privileges, install backdoors, disable defenses like Windbg (Application Shimming). Shims can also be abused to establish persistence by continuously being invoked by affected programs.

There are several public tools available that will detect shims that are currently available (Citation: Black Hat 2015 App Shim):

* Shim-Process-Scanner - checks memory of every running process for any shim flags
* Shim-Detector-Lite - detects installation of custom shim databases
* Shim-Guard - monitors registry for any shim installations
* ShimScanner - forensic tool to find active shims in memory
* ShimCacheMonitor - Volatility plug-in that pulls shim cache from memory (note: shims are only cached after reboot)

Monitor process execution for sdbinst.exe and command-line arguments for potential indications of application shim abuse.
## MITRE ATT&CK

| mitre_software_name | ShimRat  
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>SDBot</td>
</tr>
</tbody>
</table>
| mitre_software_platform | Windows   
|                     | Windows     |
| mitre_software_type  | malware        
|                     | malware     |
| mitre_software_url   | https://attack.mitre.org/software/S0444     
|                     | https://attack.mitre.org/software/S0461     |
| mitre_tactic         | privilege-escalation  
|                     | persistence    |
| mitre_tactic_id      | TA0004         
|                     | TA0003         |
| mitre_technique      | Application Shimming |
| mitre_technique_id   | T1546.011      |
| mitre_threat_group_aliases | FIN7    |
| mitre_threat_group_name | FIN7       |
| mitre_threat_group_url | https://attack.mitre.org/groups/G0046 |
| mitre_url            | https://attack.mitre.org/techniques/T1546/011 |
MITRE ATT&CK

Slow-and-Low

days or even weeks
MITRE ATT&CK

Improved Detections!

RBA: ATT&CK Tactic threshold exceeded (≥3) over previous 7 days for user=billy.tun spanning 6 Risk Rules, 5 ATT&CK tactics, and 6 ATT&CK techniques.
MITRE ATT&CK

Investigation

RBA attribution - User

User: billy.tun
Time Range: All time

Aggregate Risk Score: 512

ATT&CK Tactics

ATT&CK Techniques

Risk Rule Timeline

Suspicious Developer Utility Command

Suspicious Scheduled Task

Suspicious PowerShell Command

Security Control Disabled

System Information Discovery

System Information Discovery

Potential Phish With Attachment

Wed 23 August

23:05

23:10

23:15

23:20

23:25
IOCs as Threat Objects
Threat Objects

Per Risk Rule

| eval threat_object = process_name
| eval threat_object_type = "cmdline"
Threat Objects

Set the Stage
Threat Objects
Detect and Carry Forward

Notable Events

- Risk Object
- Risk Score
- ATT&CK Context

+ Threat Object
Threat Objects

Related Objects
Threat Objects

Visualize

"Fascinating." -- Spock
Threat Objects
Risk Notables Into Phantom
Threat Objects

Automation
“As a security practitioner and network defender, the RBA methodology is **dramatically streamlining the amount of effort** security analysts spend triaging security alerts, and finally giving them the opportunity to zero in on high fidelity, high confidence risk alerts that are absolutely worth their time and effort.”

– Marquis Montgomery, Principal Security Architect, Global Security Services at Splunk
Average Event Abandonment

RBA Goes Live in Production

Further Notable Reduction after Tuning

Notable Event Trends

Provided by Viasat and the Viasat CSOC
Notable Abandonment Drops to Zero

Notable Abandonment Percentage over Time

Standard and RIR Notables over Time by Abandonment Status

Provided by Viasat and the Viasat CSOC
Only Critical and High Notables Addressed, Resulting in High Abandonment Rate

Thousands of Notable Events Every Day

Provided by Viasat and the Viasat CSOC
Average Event Abandonment

Notable Abandonment
Below 10% Target

Daily Notables Reduced by 10x

Provided by Viasat and the Viasat CSOC
More RBA Content

SEC1113A
Streamlining Analysis of Security Stories with Risk-Based Alerting

Haylee Mills
Sr. Security Developer | Charles Schwab
MAKE IT SO

NUMBER ONE
Risk Based Alerting

Is It Right For Me?

Do you suffer from any of these symptoms?
• alert fatigue, ballooning allow/deny lists, situational numbness

Are you
• An existing ES user who wants to get ES more "operationalized"?
• Brand new ES customers who would benefit from a more turn-key SIEM experience?
• A smaller SOC team that wants a solution that will mature and grow with them?
Risk Based Alerting

What Are We Doing In ES?

• Shipped out-of-box Correlation Searches mapped to MITRE ATT&CK annotations (ESCU inclusive!)

• Shipped out-of-box Correlation Searches that deploy the new "Risk" adaptive response action (existing and new, ESCU inclusive!)

• Shipped out-of-box dashboards and panels that provide a risk-centric investigative experience

• Shipped new Correlation Searches that mine the risk index for notables (risk incident rules)
SA-RBA to ES
Map to Technique

| eval mitre_technique_id="T1170"
| lookup mitredict mitre_technique_id OUTPUTNEW mitre_tactic_id
| eval risk_message="Possible use mshta.exe to proxy execution of VBScript through a trusted Windows utility. Image=".Image.".parent_process_path:
| eval testmode=0
| eval threat_object=Image
| eval threat_object_type="commandline"
`risk_score_system(src,5)`
`risk_score_user(user,5)`
Risk Annotations

Annotate correlation searches directly in the CS editor
ATT&CK techniques are pre-populated

Annotations

CIS 20
Type an attribute and press enter

Kill Chain
Type an attribute and press enter

MITRE ATT&CK
- Brute Force
- Password Policy Discovery

NIST
- .bash_profile and .bashrc
- /etc/passwd and /etc/shadow
Risk Annotations

Intelligence Downloads

Showing 1-1 of 1 item

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Interval</th>
<th>Type</th>
<th>URL</th>
<th>Weight</th>
<th>Debug</th>
<th>Status</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>mitre_attack</td>
<td>MITRE ATT&amp;CK framework</td>
<td>86400</td>
<td>mitre_attack</td>
<td><a href="https://raw.githubusercontent.com/mitre/cti/master/enterprise-attack/enterprise-attack.json">https://raw.githubusercontent.com/mitre/cti/master/enterprise-attack/enterprise-attack.json</a></td>
<td>60</td>
<td>False</td>
<td>Enabled</td>
<td>Disable Clone</td>
</tr>
</tbody>
</table>

Always kept up to date with the latest from MITRE
SA-RBA to ES
Dynamic Scoring & Multiple Risk Objects

```
| eval mitre_technique_id="T1170"
| lookup mitredict mitre_technique_id OUTPUTNEW mitre_tactic_id
| eval risk_message="Possible use mshta.exe to proxy execution of VBScript through a trusted Windows utility. Image=".Image.".
| eval parent_process_path=".parent_process_path"
| eval testmode=0
| eval threat_object=Image
| eval threat_object_type="commandline"
`risk_score_system(src,5)`
`risk_score_user(user,5)`
```
Risk Action

Score multiple objects per correlation

Extensible Object Type List
Risk Factors

Manage your risk factors

Create simple or advanced matching conditions, as well as stack conditions within a single factor
SA-RBA to ES

Threat Object Support

```| eval mitre_technique_id="T1170"
| lookup mitredict mitre_technique_id OUTPUTNEW mitre_tactic_id
| eval risk_message="Possible use mshta.exe to proxy execution of VBScript through a trusted Windows utility. Image=".Image.".parent_process_path:".parent_process_path
| eval testmode=0
| eval threat_object=Image
| eval threat_object_type="commandline"
risk_score_system(src,5)
`risk_score_user(user,5)`
Updated Risk Data Model

**Score Calculation**

Scores are calculated via factors during DMA.

**Additional MITRE ATT&CK Enrichment**

Additional MITRE ATT&CK enrichment.

**Risk & Threat Object Support**

Risk & Threat Object Support.

### Calculated Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>description</td>
<td>String</td>
</tr>
<tr>
<td>object</td>
<td>String</td>
</tr>
<tr>
<td>object_type</td>
<td>String</td>
</tr>
<tr>
<td>risk_score</td>
<td>Number</td>
</tr>
<tr>
<td>threat_object_type</td>
<td>String</td>
</tr>
<tr>
<td>risk_factor_add</td>
<td>Number</td>
</tr>
<tr>
<td>risk_factor_add_matched</td>
<td>Number</td>
</tr>
<tr>
<td>risk_factor_mult</td>
<td>Number</td>
</tr>
<tr>
<td>risk_factor_mult_matched</td>
<td>Number</td>
</tr>
<tr>
<td>risk_score_matched</td>
<td>Number</td>
</tr>
</tbody>
</table>
SA-RBA to ES
Auto-Enrichment Of ATT&CK data

|eval mitre_technique_id="T1170"
|lookup mitredict mitre_technique_id OUTPUTNEW mitre_tactic_id
|eval risk_message="Possible use mshta.exe to proxy execution of VBScript through a trusted Windows utility. Image=".Image.".parent_process_path=".parent_process_path
|eval testmode=0
|eval threat_object=Image
|eval threat_object_type="commandline"
`risk_score_system(src,5)`
`risk_score_user(user,5)`
Updated Risk Data Model

Risk events are now auto-enriched for any data model searches and risk index searches.
Updated Risk Analysis Dashboard Panels

New panels showing risk modifiers by ATT&CK technique

<table>
<thead>
<tr>
<th>risk_object</th>
<th>risk_type</th>
<th>risk_score</th>
<th>source</th>
<th>count</th>
<th>risk_score</th>
<th>risk_objects</th>
<th>count</th>
</tr>
</thead>
<tbody>
<tr>
<td>127.0.0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>arn:aws</td>
<td></td>
<td>160.0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.2.3.4</td>
<td></td>
<td>140.0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>i-0a0c</td>
<td></td>
<td>120.0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>i-061b</td>
<td></td>
<td>120.0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>i-0b7f58d0486c75c8</td>
<td></td>
<td>120.0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>system</td>
<td></td>
<td>120.0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>user</td>
<td></td>
<td>100.0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>system</td>
<td></td>
<td>80.0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **Risk Score By Object**
- **Most Active Sources**
  - Endpoint - Should Timesync Host Not Syncing - Rule
  - Network - Unroutable Host Activity - Rule
  - Audit - Personally Identifiable Information Detection - Rule
  - Threat - AWS Guard Duty Alert - Rule
  - Threat - Many Unauthorized AWS Operations - Rule
  - Endpoint - Code42 Rule Match - Rule
  - Endpoint - Host Sending Excessive Email - Rule

Graphs showing risk modifiers over time and by annotations.
Thank You

“Live long, and prosper.” — Spock

Please provide feedback via the SESSION SURVEY