Streamlining Analysis of Security Stories with Risk-based Alerting

SEC1113A

Haylee Mills

Sr. Security Developer | Charles Schwab

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.

Haylee Mills

Sr. Security Developer | Charles Schwab

splunk> .conf20

Agenda

1) Risk Based Alerting (RBA) Review

2) Analysis Dashboard Preview

3) Structural Elements

4) Design Principles

5) Dashboard Design

RBA Review

Putting the big alert pipeline to pasture

isolated security **EVENTS** → contextual security **STORIES**

RBA Review

Putting the big alert pipeline to pasture

isolated security **EVENTS** → contextual security **STORIES**

Noise → Context

RBA Review

Putting the big alert pipeline to pasture

isolated security **EVENTS** → contextual security **STORIES**

Noise → Context

Alerts → Risk Rules → Risk Objects → Risk Incident Rules

RBA Review

Putting the big alert pipeline to pasture

how to tell a STORY

RBA Review

Putting the big alert pipeline to pasture

how to tell a STORY

What is worth knowing to make analysis decisions?

What is the analyst going to check anyway?

What would be nice to know?

Structural Elements

Lenses

Different **TEAMS** need different **STORIES**

Structural Elements

Lenses

Different **TEAMS** need different **STORIES**

Review board

Risk incident rules (RIRs)

Investigation dashboard

Structural Elements

Lenses

Different **TEAMS** need different **STORIES**

Review board

Risk incident rules (RIRs)

Investigation dashboard

```
eval SOC_Core="1"
```

```
eval Insider_Core="1"
```

Structural Elements

Dynamic Impact / Confidence

```
| lookup RRadjustment-Threat_Intel_Hit dest user user_bunit OUTPUT impact confidence

| eval impact = case(
match(feed, “alert*”) AND match(fidelity_score,”high”),”medium”,
match(feed, “alert*”) AND match(fidelity_score,”low”),”low”,
isnull(impact),”informational”)
```

Structural Elements

Dynamic Impact / Confidence

```
| lookup RRadjustment-Threat_Intel_Hit dest user user_bunit OUTPUT impact confidence

| eval impact = case(
match(feed, “alert*”) AND match(fidelity_score,”high”),”medium”,
match(feed, “alert*”) AND match(fidelity_score,”low”),”low”,
isnull(impact),”informational”)
```

Lookup definitions with WILDCARD(fieldname)

Structural Elements

Dynamic Impact / Confidence

```
| lookup RRadjustment-Threat_Intel_Hit dest user user_bunit OUTPUT impact confidence
```

```
| eval impact = case(
match(feed, “alert*”) AND match(fidelity_score,”high”),”medium”,
match(feed, “alert*”) AND match(fidelity_score,”low”),”low”,
isnull(impact),”informational”)
```

Lookup definitions with WILDCARD(fieldname)

Case statements for **DAYS**

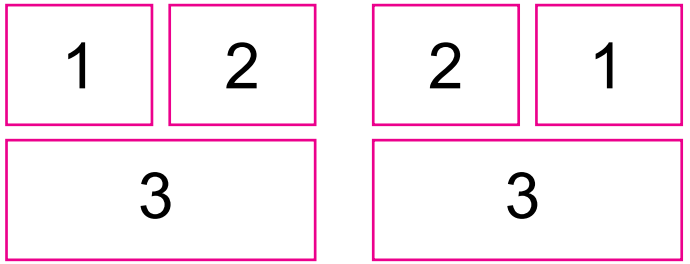
Design Principles

Good design reduces **COGNITIVE LOAD** – ***quicker*** analysis, better ***thinking***

Design Principles

Good design reduces **COGNITIVE LOAD** – ***quicker*** analysis, better ***thinking***

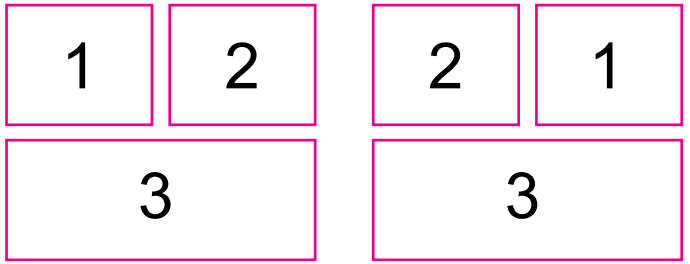
ORDER



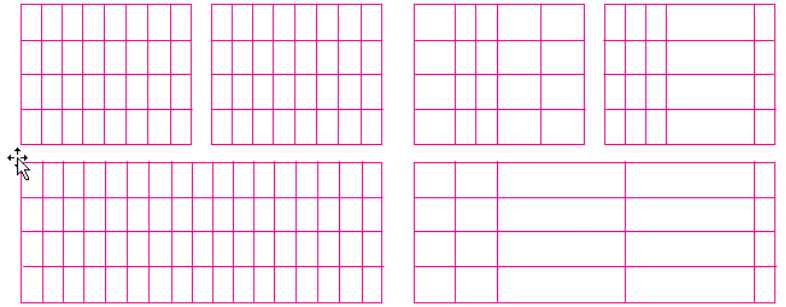
Design Principles

Good design reduces **COGNITIVE LOAD** – ***quicker*** analysis, better ***thinking***

ORDER



DISPLAY



Dashboard Design

Depends / Reject

```
<panel / table / chart depends="$token$">
```

Dashboard Design

Depends / Reject

```
<panel / table / chart depends="$token$">
```

Search for *everything* with a baseSearch

Dashboard Design

Depends / Reject

```
<panel / table / chart depends="$token$">
```

Search for *everything* with a baseSearch

All data is loaded, just hidden with depends

Dashboard Design

Depends / Reject

```
<panel / table / chart depends="$token$">
```

Search for *everything* with a baseSearch

All data is loaded, just hidden with depends

Selectively display panels based on user action

Dashboard Design

Drilldowns

```
<drilldown target="_blank">
<condition match="match('click.value2', &amp;quot;click&amp;quot;)">
<link>$row.drilldown_link|n$</link>
</condition>
<condition>
<set token="filterValue1">$click.value2$</set>
<set token="filterField1">$click.name2$</set>
</condition>
</drilldown>
```

Allows eval's match() logic, but must use URL-encoding

Dynamic actions based on what was clicked!

Agenda

1) Risk Based Alerting (RBA) Review

2) Analysis Dashboard Preview

3) Structural Elements

4) Design Principles

5) Dashboard Design

Risk-Based Alerting Talks

- **SEC1479:** Say Goodbye to Your Big Alert Pipeline, and Say Hello to Your New Risk-Based Approach
  Jim Apger / Stuart McIntosh
- **SEC1803:** Modernize and Mature Your SOC with Risk-Based Alerting
  Jim Apger / Jimi Mills
- **SEC1538:** Getting Started with Risk-Based Alerting and MITRE
  Bryan Turner
- **SEC1908:** Tales From a Threat Team: Lessons and Strategies for Succeeding with a Risk-Based Approach
  Stuart McIntosh
- **SEC1556:** Building Behavioral Detections: Cross-Correlating Suspicious Activity with the MITRE ATT&CK Framework
  ME!

Thank You

Please provide feedback via the

SESSION SURVEY