

Forward-Looking Statements



This presentation may contain forward-looking statements regarding future events, plans or the expected financial performance of our company, including our expectations regarding our products, technology, strategy, customers, markets, acquisitions and investments. These statements reflect management's current expectations, estimates and assumptions based on the information currently available to us. These forward-looking statements are not guarantees of future performance and involve significant risks, uncertainties and other factors that may cause our actual results, performance or achievements to be materially different from results, performance or achievements expressed or implied by the forward-looking statements contained in this presentation.

For additional information about factors that could cause actual results to differ materially from those described in the forward-looking statements made in this presentation, please refer to our periodic reports and other filings with the SEC, including the risk factors identified in our most recent quarterly reports on Form 10-Q and annual reports on Form 10-K, copies of which may be obtained by visiting the Splunk Investor Relations website at www.investors.splunk.com or the SEC's website at www.sec.gov. The forward-looking statements made in this presentation are made as of the time and date of this presentation. If reviewed after the initial presentation, even if made available by us, on our website or otherwise, it may not contain current or accurate information. We disclaim any obligation to update or revise any forward-looking statement based on new information, future events or otherwise, except as required by applicable law.

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. We undertake no obligation either to develop the features or functionalities described or to include any such feature or functionality in a future release.

Splunk, Splunk>, Data-to-Everything, D2E and Turn Data Into Doing are trademarks and registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names or trademarks belong to their respective owners. ©2021 Splunk Inc. All rights reserved.

Accenture's Journey to Risk Based Alerting with Splunk Enterprise Security and Beyond

SEC1249A

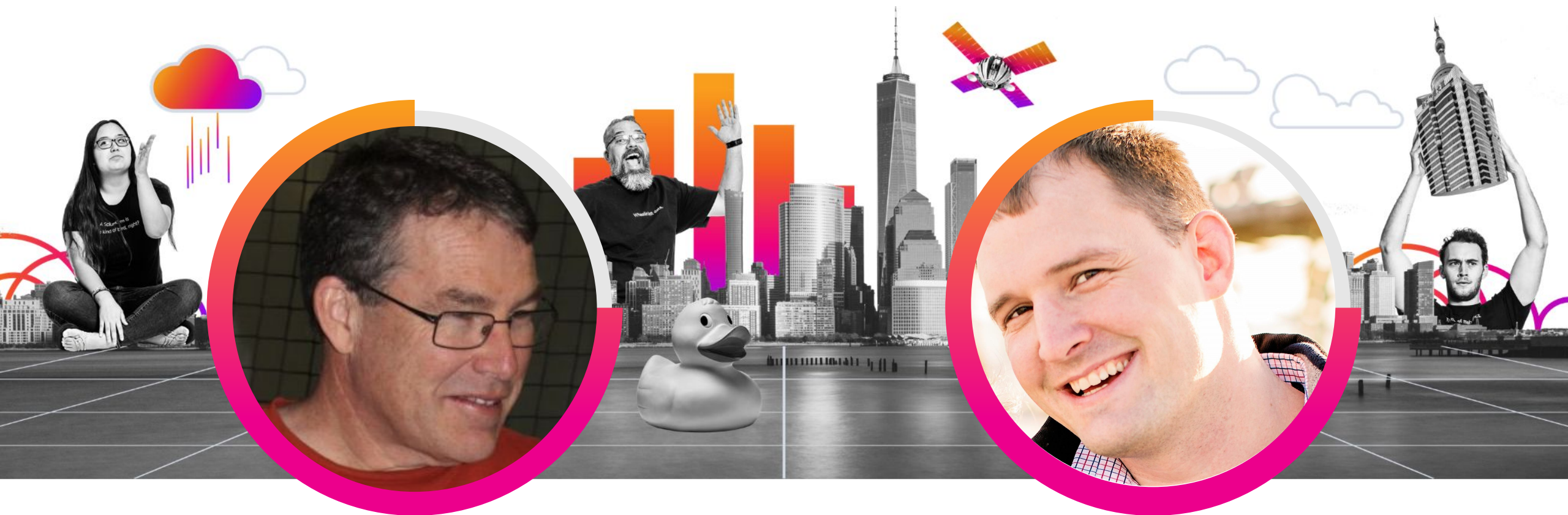
Chip Stearns

Partner | Keos Technology

Marcus Boyd

Manager | Accenture





Chip Stearns

Partner | Keos Technology

Marcus Boyd

Manager | Accenture

Risk-Based Alerting (RBA)

- 1) Why we did this, and why now
- 2) How we did it
- 3) How we know it worked...and is still working
- 4) What we learned along the way



Accenture's footprint

The largest and most diversified group of strategy, digital, technology and operations professionals in the world delivering on the promise of technology and human ingenuity every day

**569K**

Employees

200Cities with Accenture locations and operations, across **50** countries**6,000+**Clients served in **120+** countries**\$44.3B**

(US) Revenues

More than 50 delivery centers across five continents, offering services in 39 languages

Splunk + Accenture Security



Accenture's SIEM footprint

Let's begin with the end in mind

Splunk Cloud

12.5TB
of daily ingest



3
Search Heads



2
Tenants

Teams



SOC Monitoring



CIRT



SOC Eng.



Network Admins

Data Source



65K
Network Devices



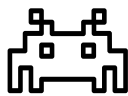
45K
Server Devices



250
Applications



4K
Cloud accounts across
AWS, Azure, GCP

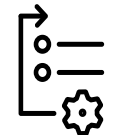


2
Threat Intel Feeds

Content



52
Traditional UCs by end of FY21



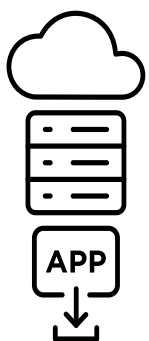
60
RBA UCs by end of FY21



1
SOAR Instance

splunk> .conf21

Our Best Laid Plans



Our Plan for FY21

40%

Increase in data
volume

2x

Increase in use cases
under monitor

Problem Statement:

How can we optimize to handle new data volume & added scope while keeping SOC headcount stable?

Our Approach:

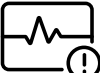
- ≡  Tweak ingestion, to reduce unneeded data
- ≡  Tune use cases
- ≡  Train users for ongoing maintenance

...but the CISO had other plans

The CISO's priorities:

 Louder alarms for high priority assets

 Map use cases against an accepted security framework to assess coverage/identify gaps

 Reduce high False Positive rates

...but the CISO had other plans

The CISO's priorities:



Louder alarms for high priority assets →



Map use cases against an accepted security framework to assess coverage/identify gaps →



Reduce high false positive rates →

Our New Plan:

Implement Urgency Framework

Map current & future use cases to MITRE ATT&CK Framework (Enterprise Matrix)

Let's try this new RBA feature...

Now for the charts
so we can show you how
we did this

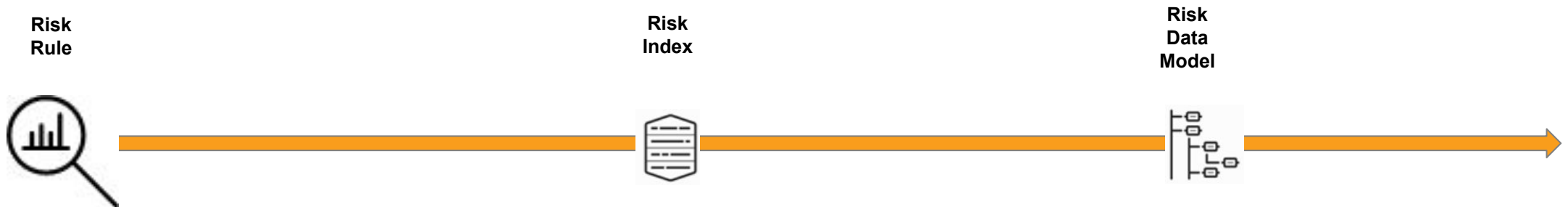
The Risk Based Alerting Flow

...with multi-cloud sources and an adaptive feedback loop



RBA Alerting - Advanced Topics

1



Identify risk object types

- Look beyond “user” and “system”
- Consider: accountID, subscriptionID, storageID, resourceGroup, office

Make ample use of anomaly detection

- box-and-whisker
- must throttle with “recent” due to size of search window

Pass-thru events

- Dynamically assign MITRE IDs

Dynamically derive the severity in SPL

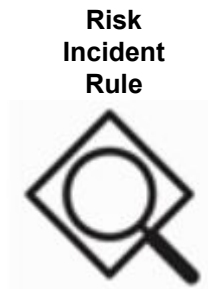
- e.g. “| eval severity = case()”
- Drives “urgency” in the IR dashboard

Enable Adaptive Feedback

- Lookup tables to whitelist selected objects
- Lookup tables for assigning risk scores

Risk Incident Rule - Advanced Topics

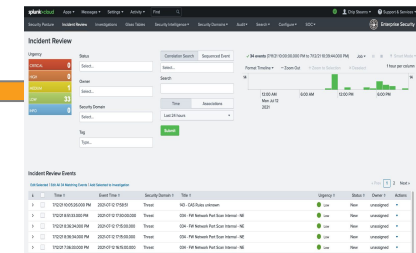
2



Notable Event



Incident Review Dashboard



How many RIRs?

- user
- system
- account
- office
- MITRE

Leverage High Value Targets (HVT) lookup table to drive Urgency

- Find the object in an HVT table
- Increment score once per risk object
- This determines the "priority"

Enable Adaptive Feedback

- Lookup tables for thresholds

Populate ES keywords

- score
- object_type
- severity
- priority
- risk_object

Update IR Dashboard

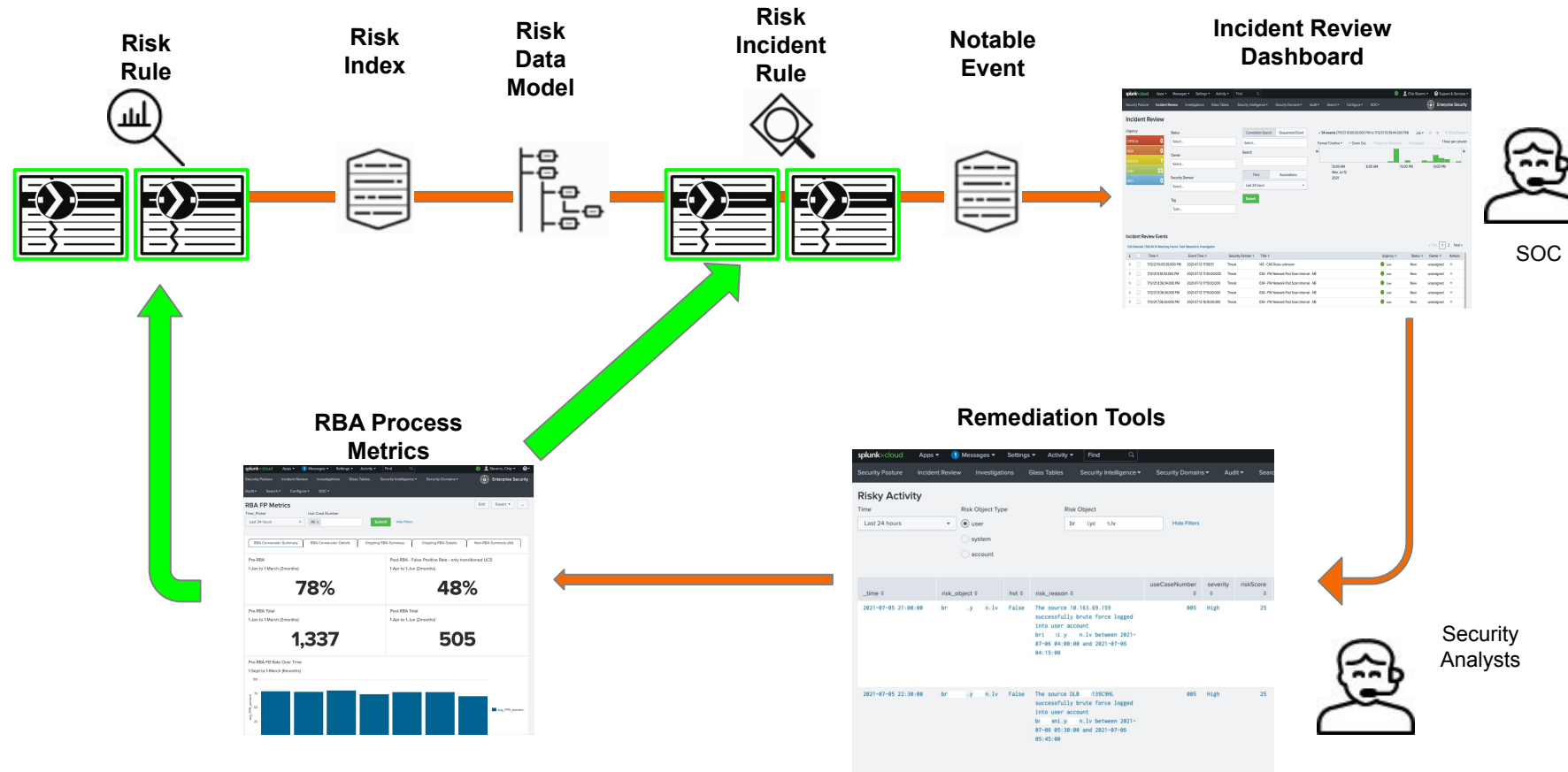
- Add HVT
- Threshold
- List of triggered Risk Rules
- Add workflow actions

- Spawn from drilldowns from the IR dashboard
- Workflow actions carry over RIR populated fields to auto populate the dashboard

- What contributing Risk Rules and associated scores caused this risk object to cross the threshold?
- What was the threshold?
- Find the risk object in the CMDB and decorate
- Show all the raw log events associate with the triggered notable event

- RBA Risk Weights tables
- RBA Allowance table
- RIR High Value Asset table
- RIR Threshold table

.... and back again





How We Know it Worked

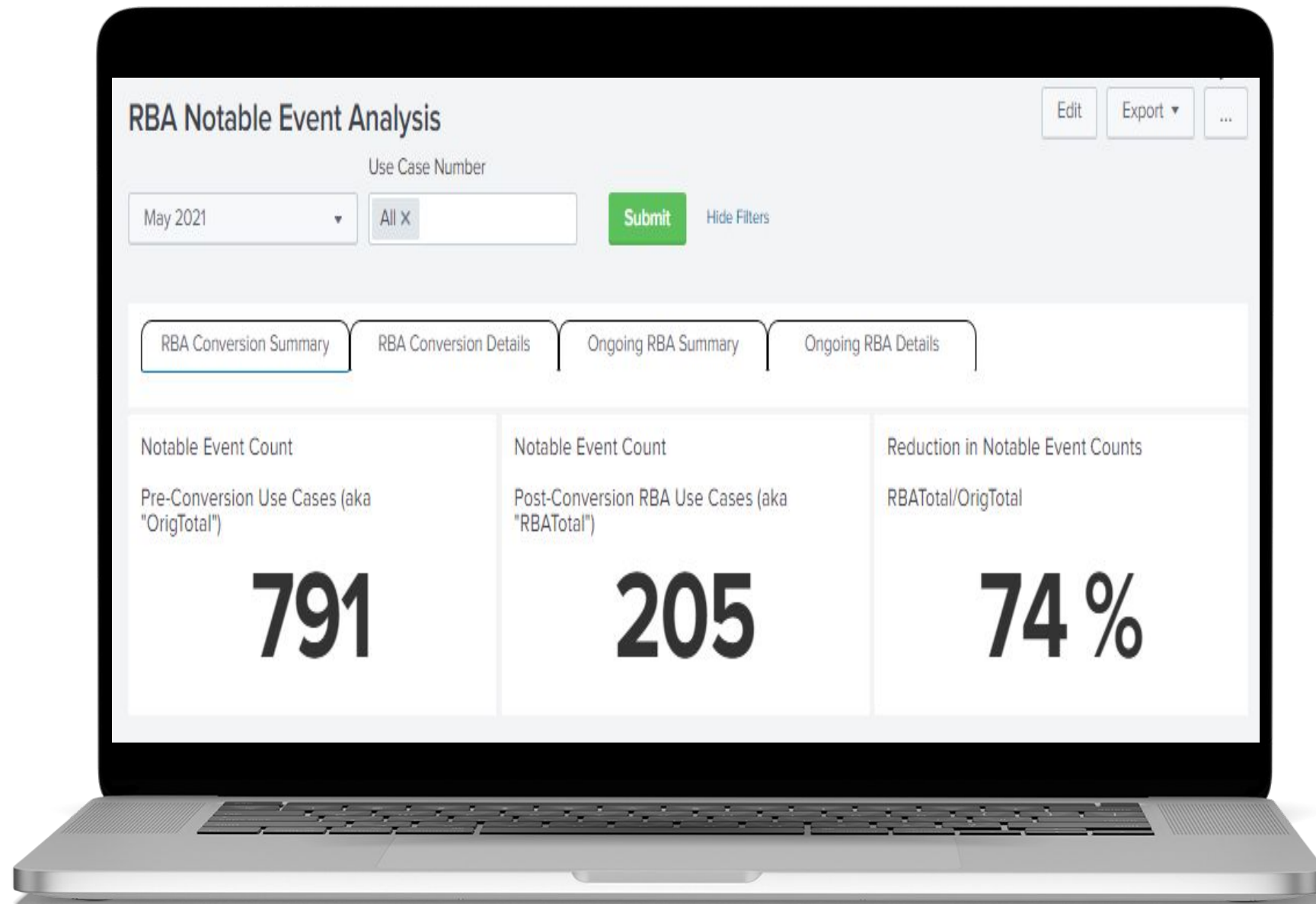
It worked!

Notable Events counts dropped between 30% & 80+% depending on the use case

////////////////////

Secret sauce ingredients:

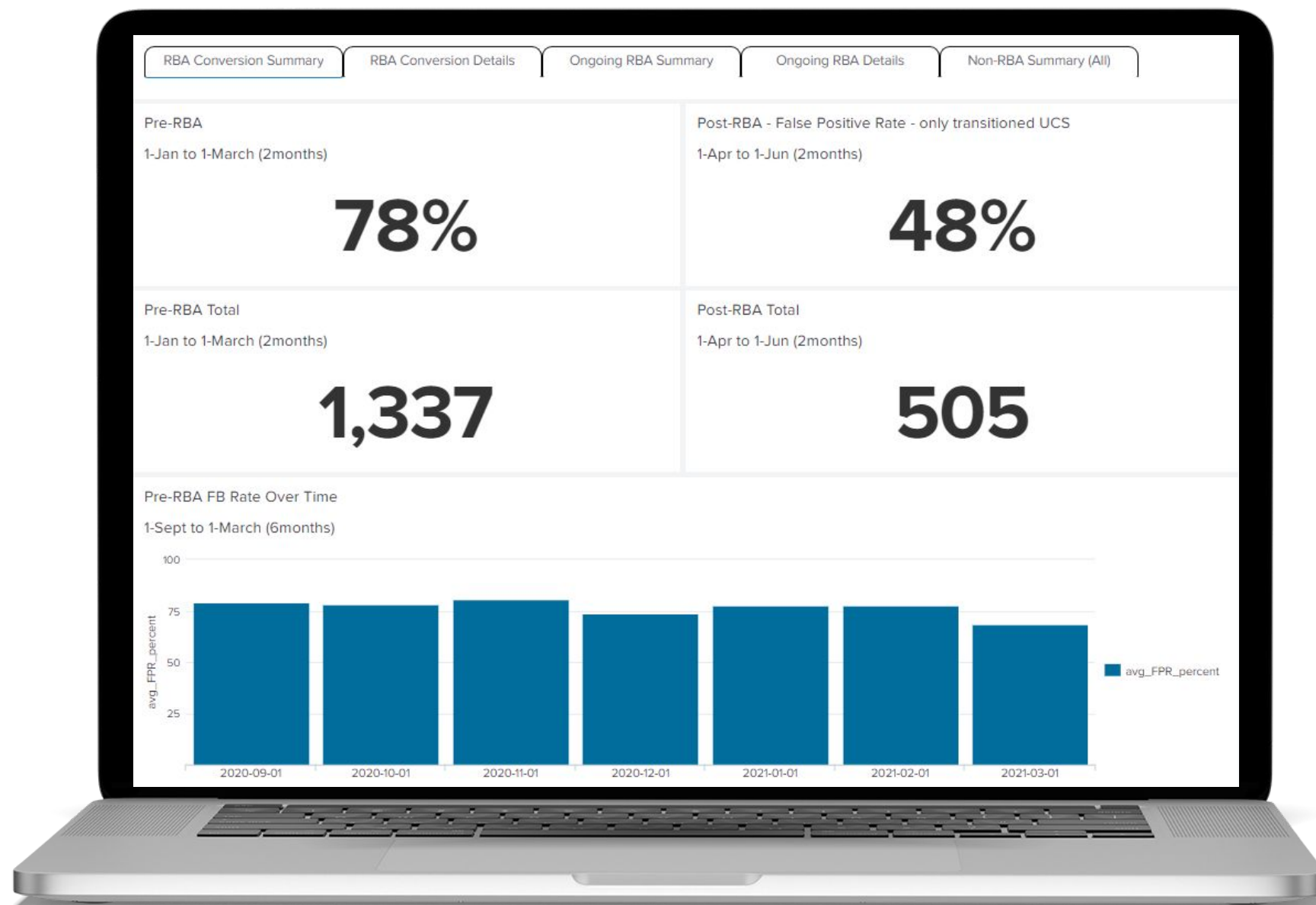
- Keep old use cases running during comparison period
- How to get “apples to apples”? Compare Pre-RBA NE count with Post-RBA contributing event count



...but wait, there's more!

////////////////////

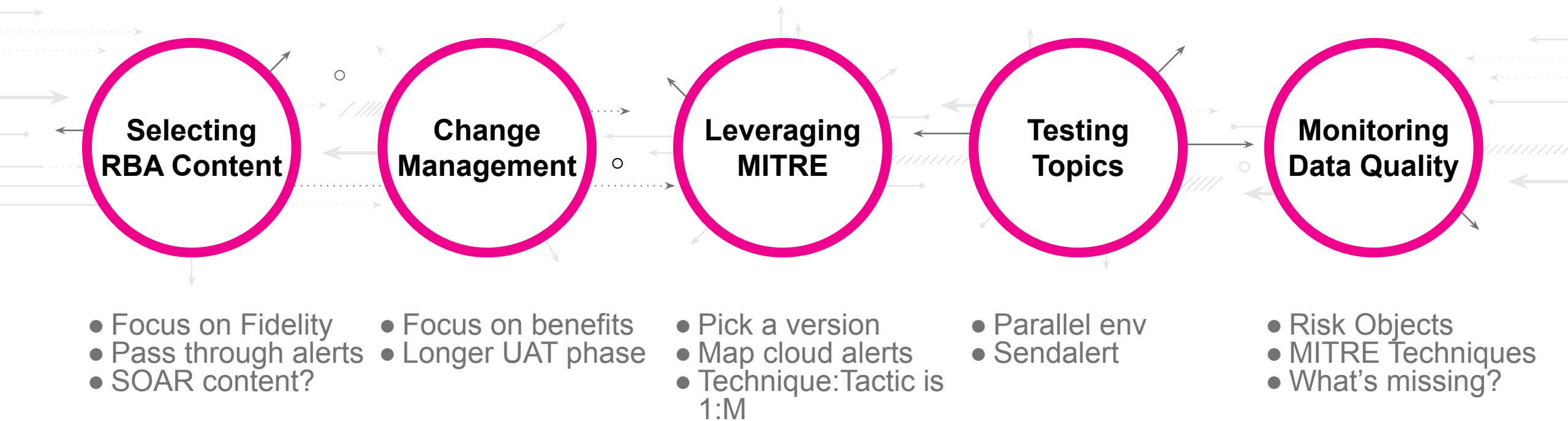
False Positive Rate
reduced by 30%



Sage wisdom we will impart to you from our journey



A Few Final Thoughts



Keep in Touch!

For more information on...

Risk-Based Alerting:

- Marcus Boyd, marcus.boyd@accenture.com
- Chip Stearns, chip@keostech.com
- Splunk's RBA Slack Channel:
outpost-frontline.slack.com

Splunk Professional Services:

- info@keostech.com

SOC Transformations:

- Rob Boyce, r.boyce@accenture.com
- Michael Sloan, michael.sloan@accenture.com



Risk-Based Alerting (RBA) at .conf21

SEC1249A - Accenture's Journey to RBA with Splunk Enterprise Security and Beyond

SEC1163A - Proactive Risk Based Alerting for Insider Threats

SEC1162A - Supercharge Your Risk Based Alerting (RBA) Implementation

SEC1271 - What's New in Splunk Enterprise Security?

SEC1590C - Augmented Case Management With Risk Based Analytics and Splunk SOAR

SEC1800A - Implementing Zero Trust: From Hype to Reality

SEC1466A - A Deep-Dive Into How Zoom Is Building Its World-Class Detection Pipeline in Response to the Zoom-Boom!



Thank You

Please provide feedback via the
SESSION SURVEY

