Eliminate your alert fatigue

Risk Based Alerting

Johan Bjerke
Security Strategist | Splunk SURGe
June 2023

splunk> turn data into doing®

Johan Bjerke

Principal Security Strategist
Splunk SURGe

SURGe by Splunk

/bin/whoami

Spent most of my career in London, UK

Relocated to Stockholm, Sweden in 2021

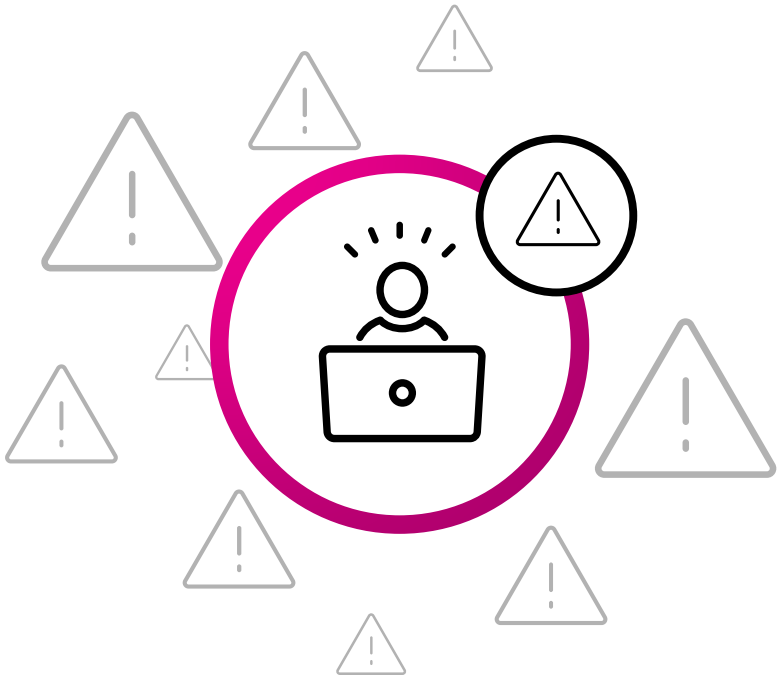
Member of SURGe, Splunk's strategic security research team

Responsible for European coverage of Rapid Response events

Lead contributor to Splunk Security Essentials (#1 app on Splunkbase)

Alert Volumes Are Overwhelming SOCs

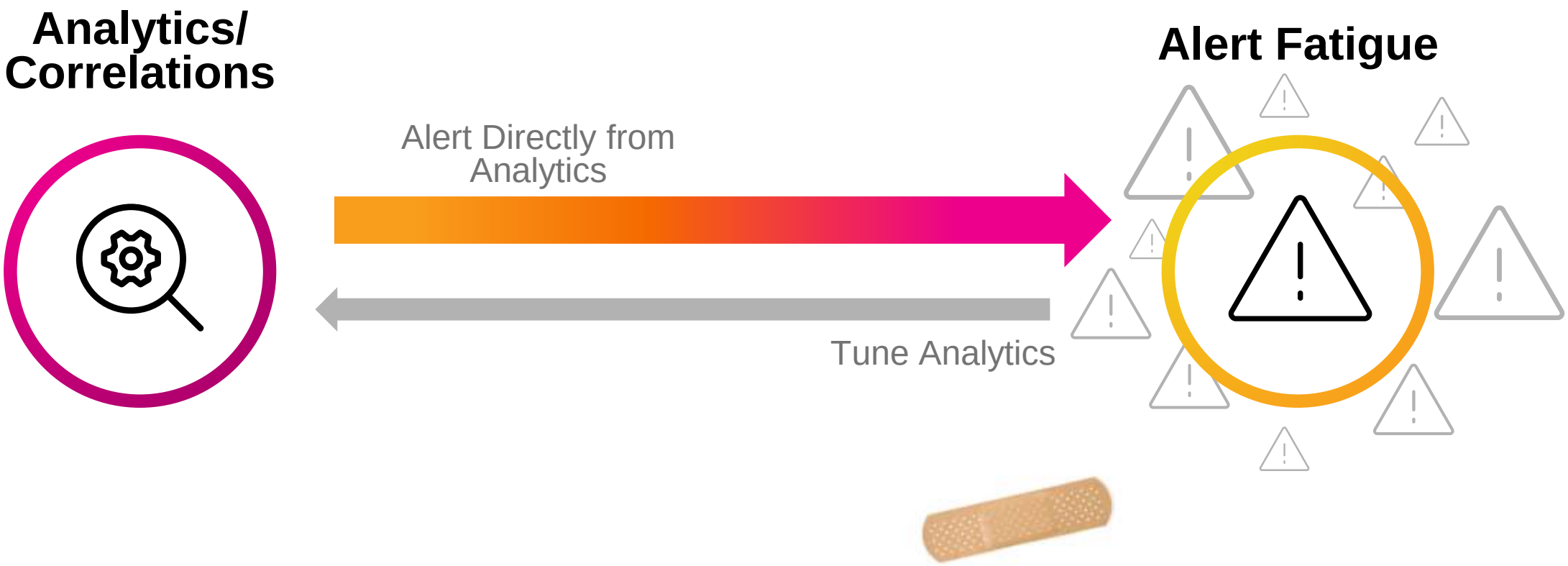
Over 40% of orgs receive 10,000+ alerts per day; experience 50%+ false positives



- Abandoned alerts
- Suppressed alerts
- Slow detection / response
- Analyst burnout

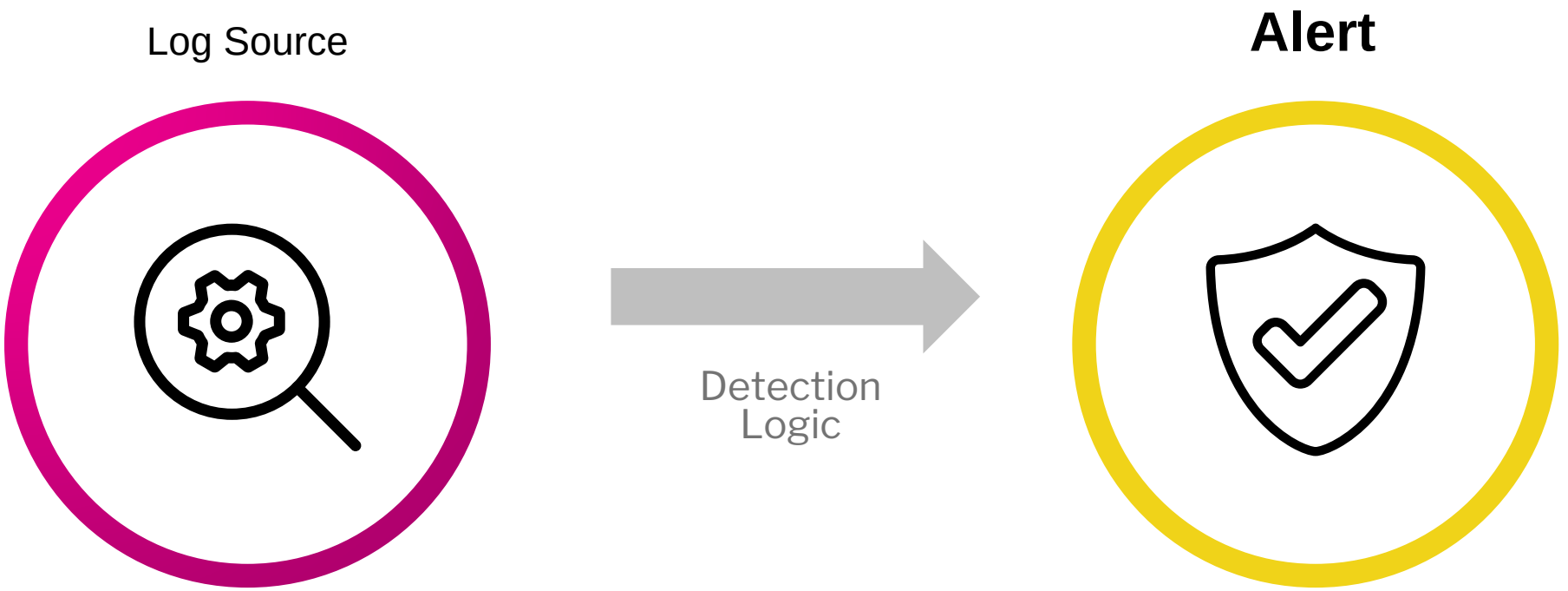
But What Alternatives Do SOCs Have?

There are no perfect correlation searches; alert fatigue seems inevitable

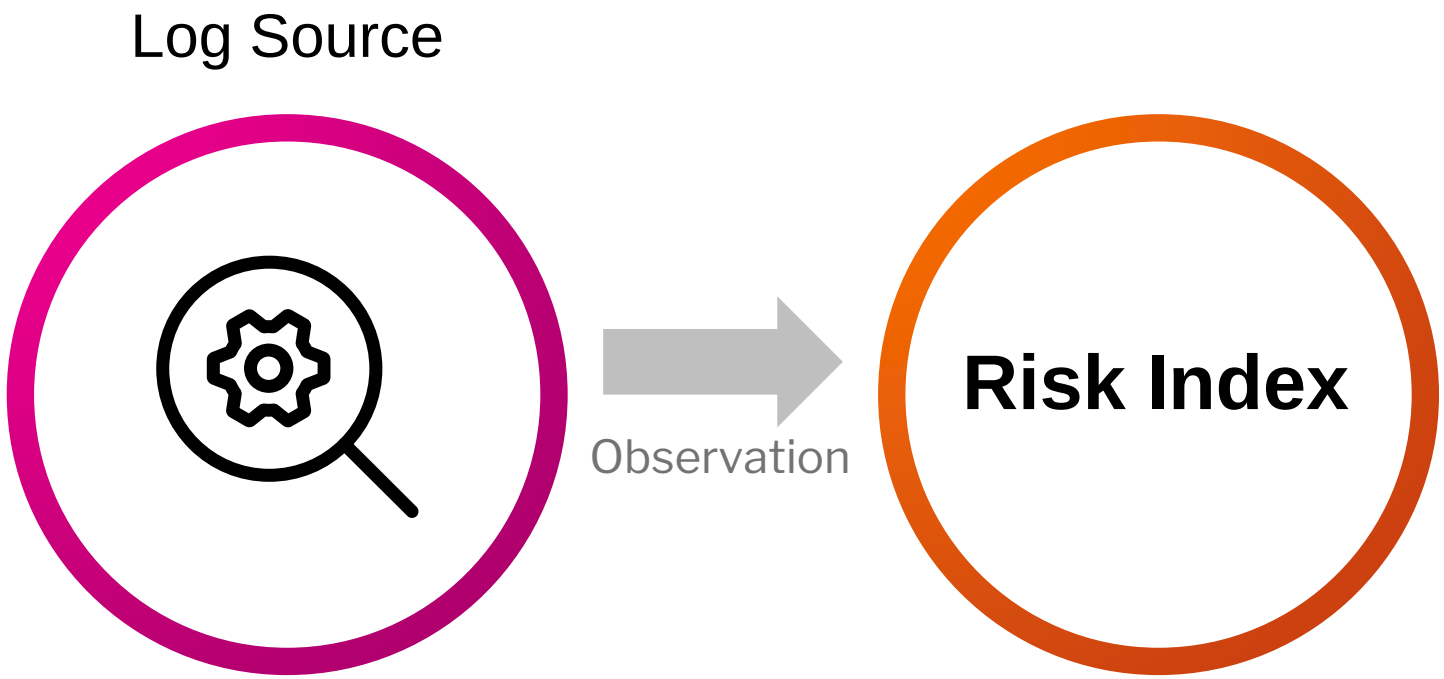


How can SOCs **reduce alert volumes** while **improving their security** coverage?

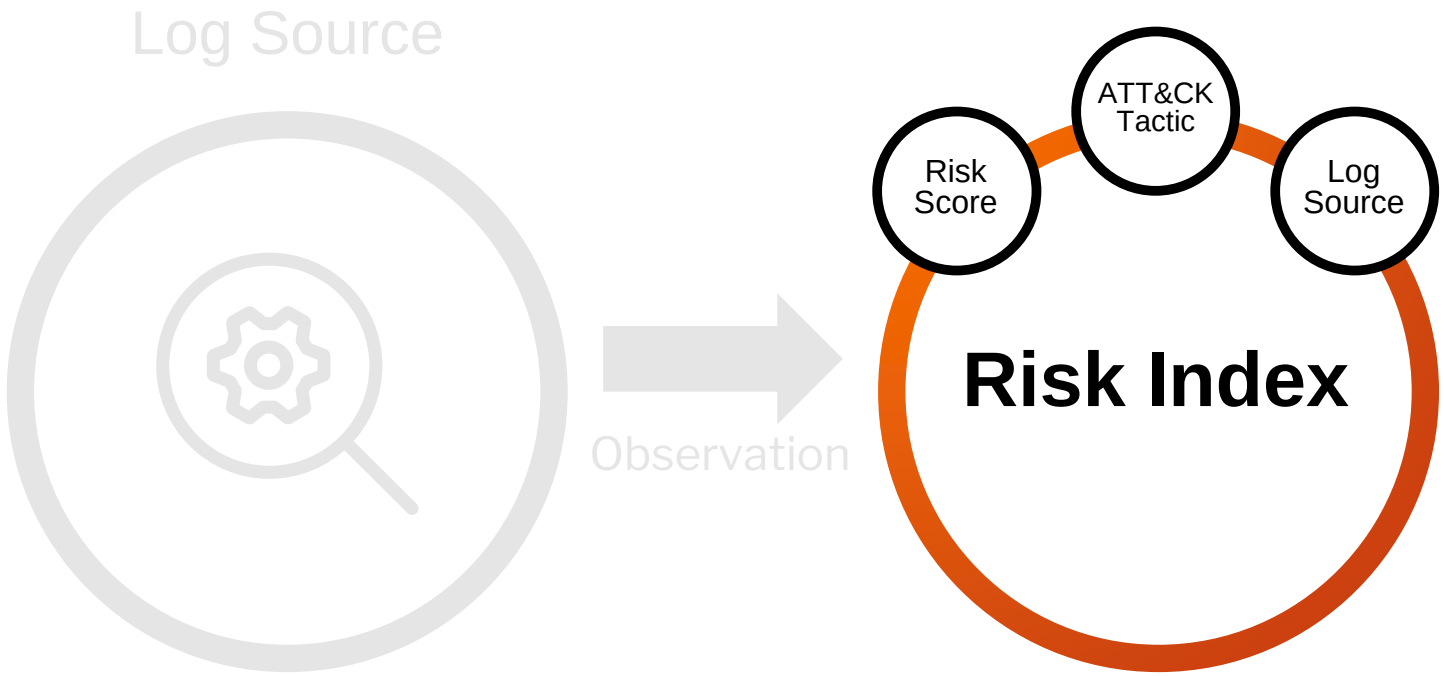
Detection Methodology for Too Long



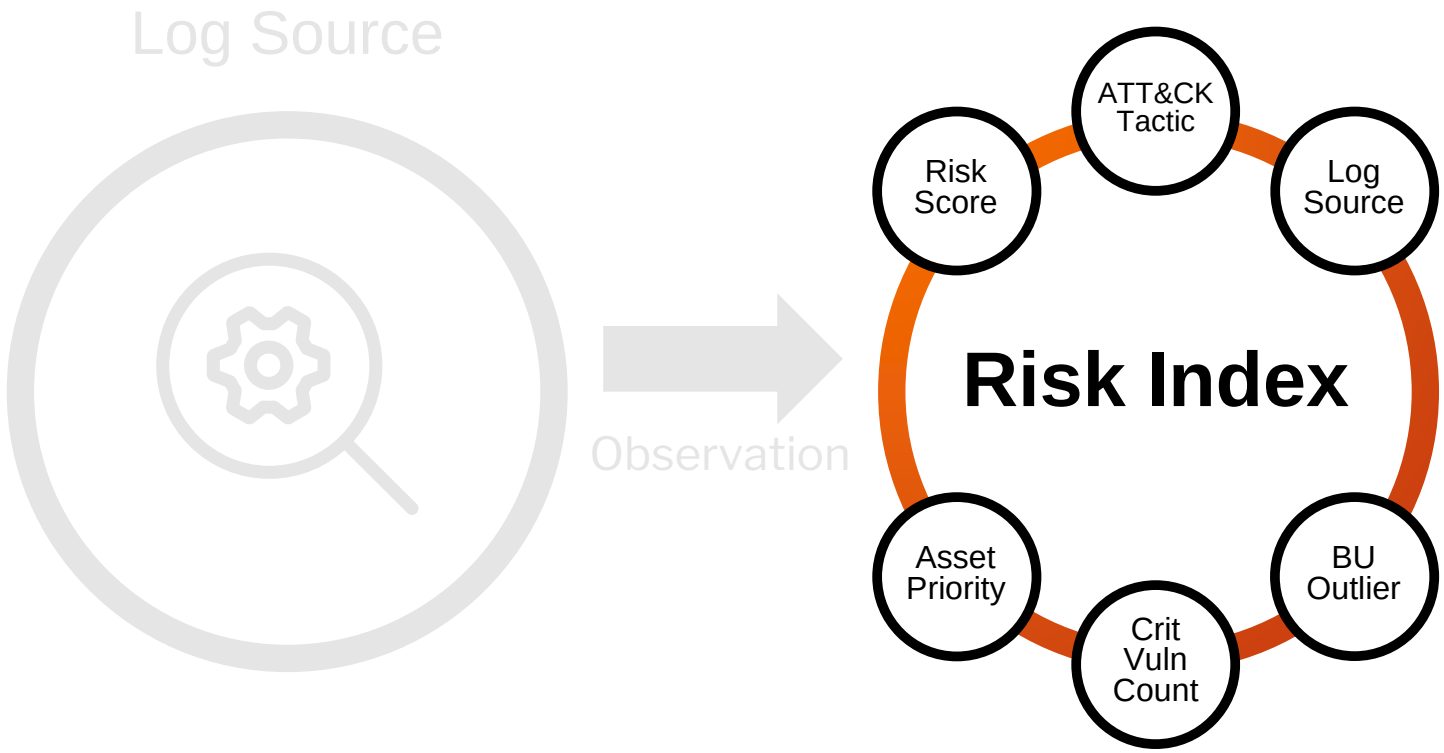
Risk Based Alerting



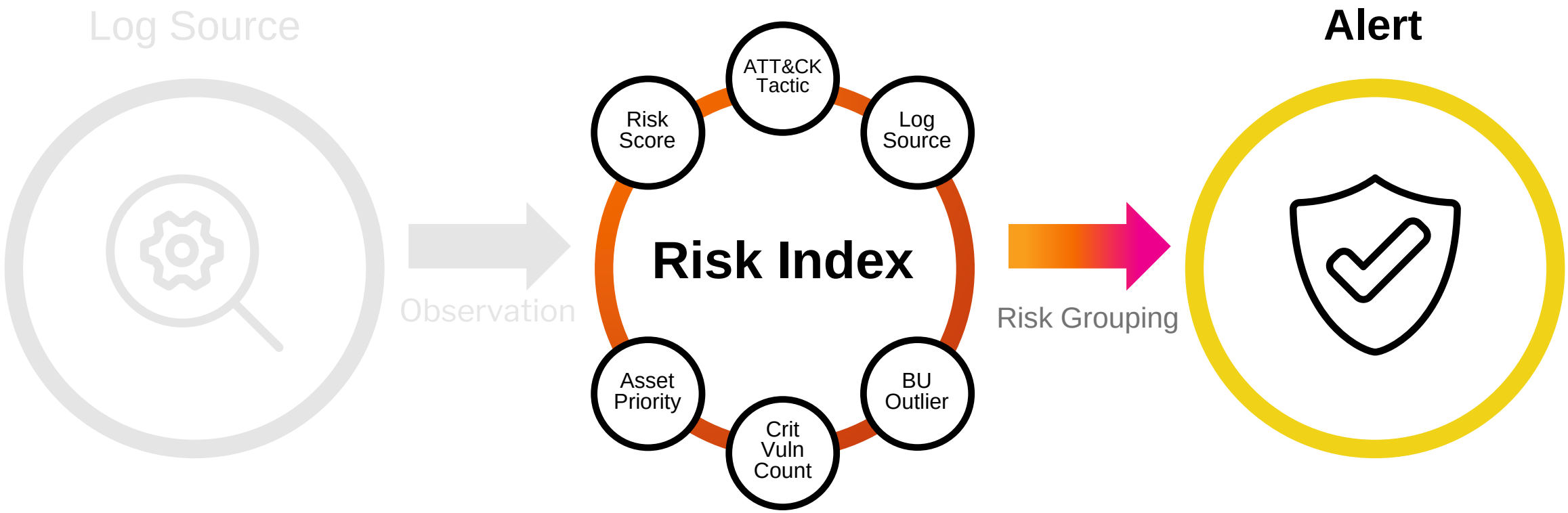
Risk Based Alerting



Risk Based Alerting

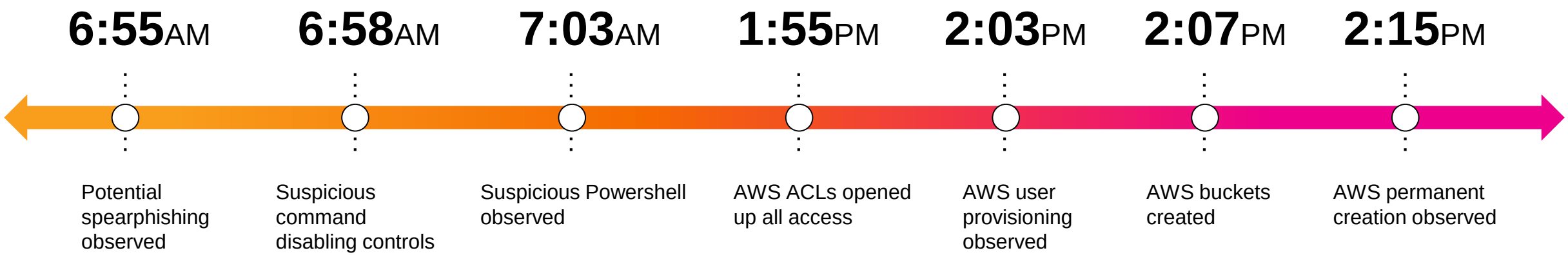


Risk Based Alerting



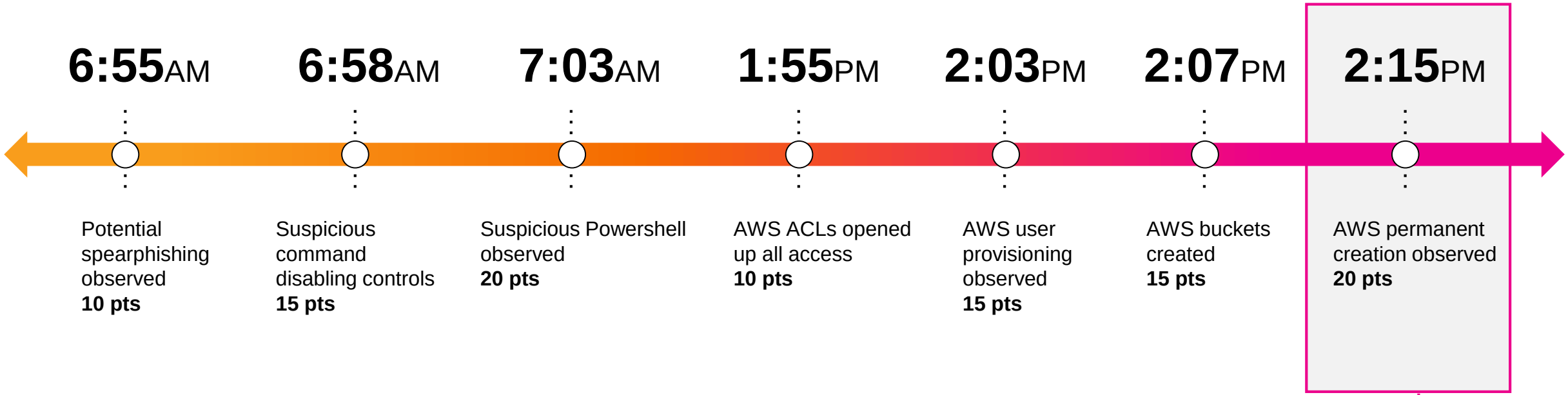
How Does This Look in Practice?

Traditionally, the events below would be considered too noisy and would be abandoned



How Does This Look in Practice?

With risk-based alerting, these events become context that informs high-fidelity alerts



With one click, view all of the risk events that contribute to the alert

ALERT

Risk Notable

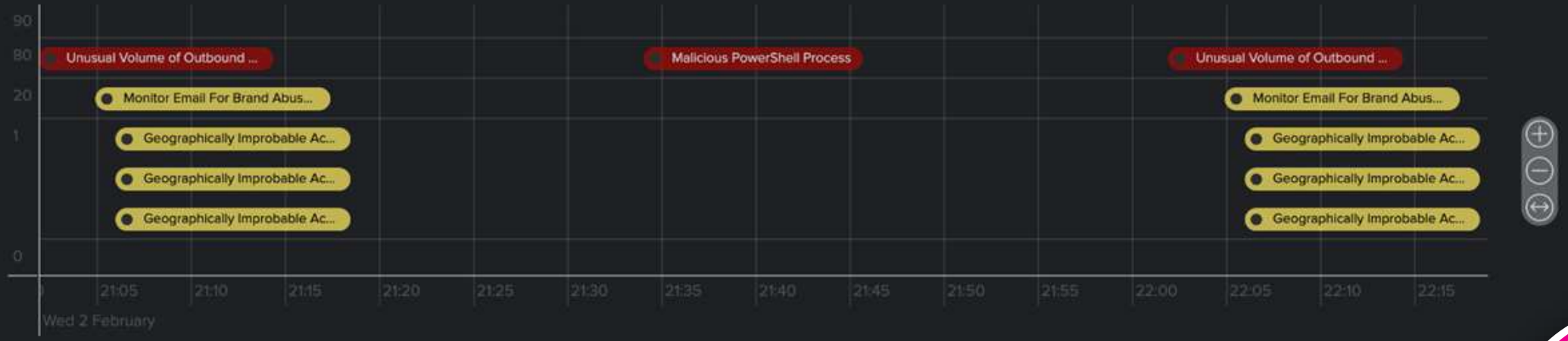
Generate alert for any user or system that exceeds a risk score of 100 in a 24 hour period

Aggregated user risk score **>100**

splunk> turn data into doing

Risk Events

fyodor@froth.ly Risk Score: [redacted] Event Count: 32



Contributing Risk Events

filter

Time	Risk Rule	Risk Score	Annotations	Threat Object
Yesterday, 11:31 PM	Network - Unusual Volume of Outbound Traffic By Src - Rule	80	T1030, TA0010 2	10.0.1.4 1
Yesterday, 10:34 PM	ESCU - Malicious PowerShell Process - Encoded Command Demo - Rule	80	T1059.001, TA0002 2	"C:\Windows\System32... 2
Yesterday, 8:34 PM	ESCU - Malicious PowerShell Process - Encoded Command Demo - Rule	80	T1059.001, TA0002 2	"C:\Windows\System32... 2
Yesterday, 7:34 PM	ESCU - Malicious PowerShell Process - Encoded Command Demo - Rule	80	T1059.001, TA0002 2	"C:\Windows\System32... 2
Yesterday, 11:34 PM	ESCU - Malicious PowerShell Process - Encoded Command Demo - Rule	80	T1059.001, TA0002 2	"C:\Windows\System32... 2
Yesterday, 10:01 PM	Network - Unusual Volume of Outbound Traffic By Src - Rule	80	T1030, TA0010 2	10.0.1.4 1
Yesterday, 9:34 PM	ESCU - Malicious PowerShell Process - Encoded Command Demo - Rule	80	T1059.001, TA0002 2	"C:\Windows\System32... 2

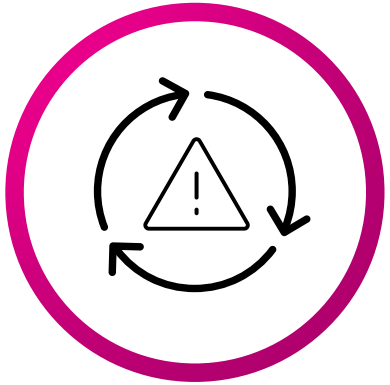
Up to 80%
drop in Security alerts

Up to 30%
reduction in false positives

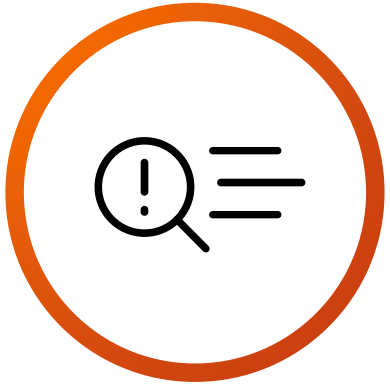
RBA Reduces Alerts, and Much More

RBA initially reduces alert volumes (and fast) but ultimately streamlines the entire SOC

Reduce Alerts

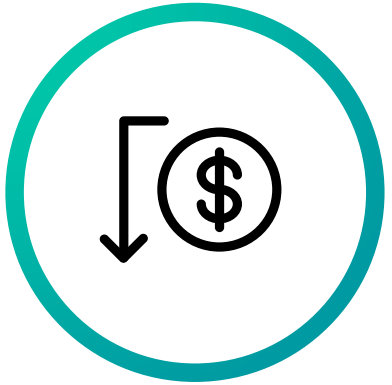


Improve Detections



Quantify SOC Maturity

Reduce Operational Costs



Before & After

Big Alert Pipeline

thousands of alerts per month

very low alert fidelity

- disconnected security events
- heavy alert fatigue
- limited application for smaller, specialized teams

Risk Based Alerting

50-90% alert reduction

increased alert fidelity

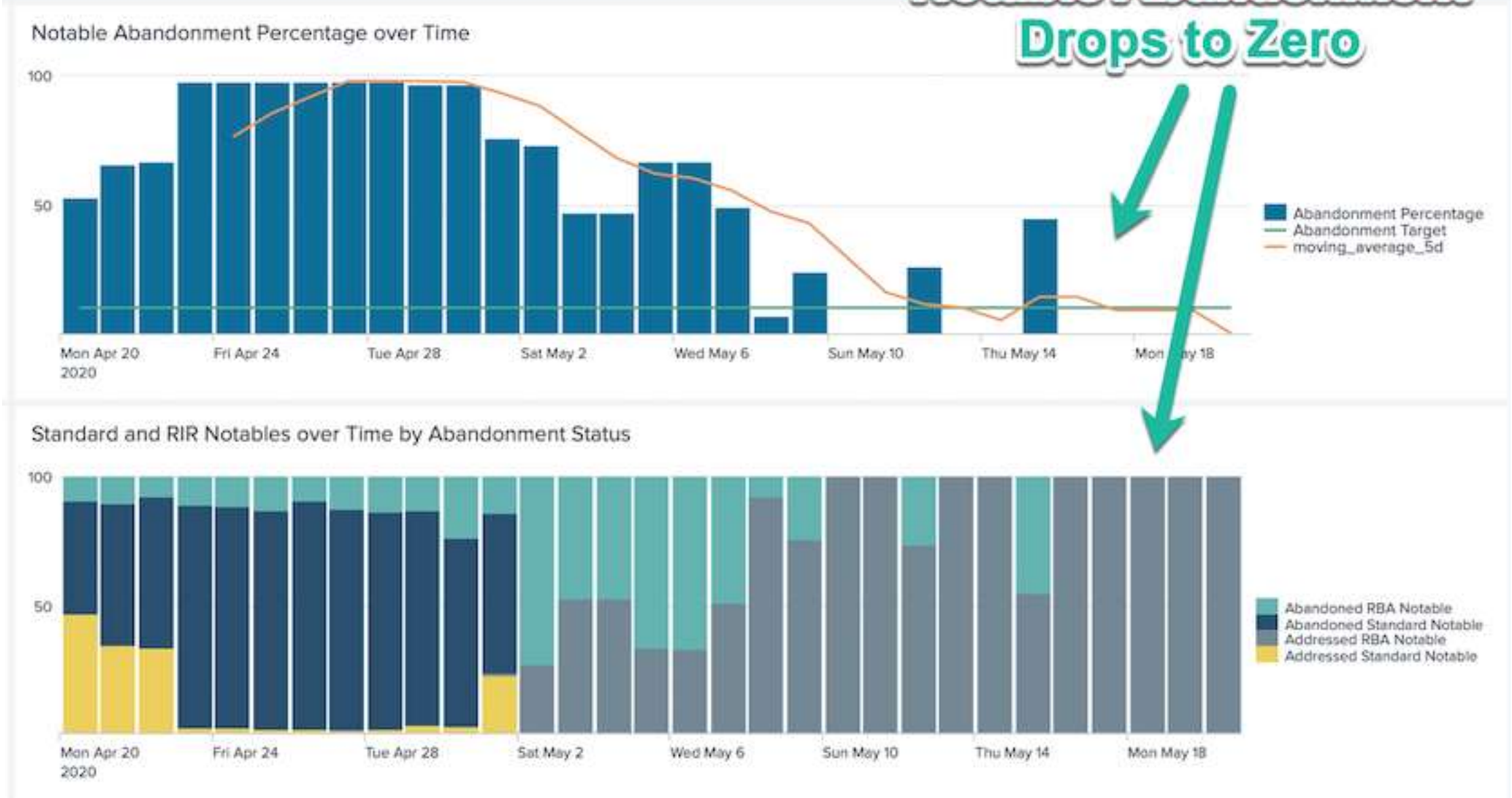
- improved investigation workflows
- significant time freed for SOC projects
- framework relevant for Insider Risk, Fraud, etc.

Real World examples

splunk> turn data into doing

Provided by Viasat and the Viasat CSOC

Notable Abandonment Drops to Zero



Provided by Viasat and the Viasat CSOC

Jun 2020 ▾ Hide Filters

Average Event Abandonment

Notable Abandonment Below 10% Target

Notable Event Trends

Daily Notables Reduced by 10x

Provided by Viasat and the Viasat CSOC

Outcome

- 80% Alert reduction
- 2x Alert fidelity
- 90% Less time for investigation

Provided by Viasat and the Viasat CSOC

Want to know more?

splunk> turn data into doing

Essential Guide to Risk-Based Alerting E-Book

almost **100** pages!

easy to follow!

Haylee Mills

“**I PROMISE!**”

splunk> turn data into doing

.conf talks

supplementary information for various crowds

SEC1479 - Say Goodbye to Your Big Alert Pipeline, and Say Hello to Your New Risk-Based Approach

The original talk by Jim Apger and Stuart McIntosh explains the approach and benefits.

SEC1803 - Modernize and Mature Your SOC with Risk-Based Alerting

Jim Apger reviews RBA structure and benefits, then Jimi Mills offers a *detailed* timeline of Texas Instruments' RBA evolution.

SEC1113A - Streamlining Analysis of Security Stories with Risk-Based Alerting

Haylee Mills explains how to design intuitive dashboards, and shows off what she built for Charles Schwab.

SEC1908 - Tales From a Threat Team: Lessons & Strategies for Succeeding with a Risk-Based Approach

Stuart McIntosh delivers handy lessons learned, metrics, and approaches from running RBA in production for over a year.

SEC1163A - Proactive Risk Based Alerting for Insider Threats

Incredible talk from Matt Snyder at VMware about how they revolutionized their Insider Threat program with RBA.

SEC1538 - Getting Started with Risk-Based Alerting and MITRE

Bryan Turner reviews RBA structure and benefits, then guides building detections and aligning to ATT&CK.

links to all RBA relevant talks in slide notes

Thank you!