Security Monitoring Using Splunk Cookbook

Proven recipes for improving the security posture

Prabhu Ravi | Mathangi Shanmugam

Verizon

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.

Prabhu Ravi

Principal Consultant | Verizon

splunk> .conf20

Mathangi Shanmugam

Senior Consultant | Verizon

splunk> .conf20

Agenda

1) The Need
I'm hungry!

2) Challenges
Too many options

3) Our Journey
Ingredients

4) Solutions
Recipe

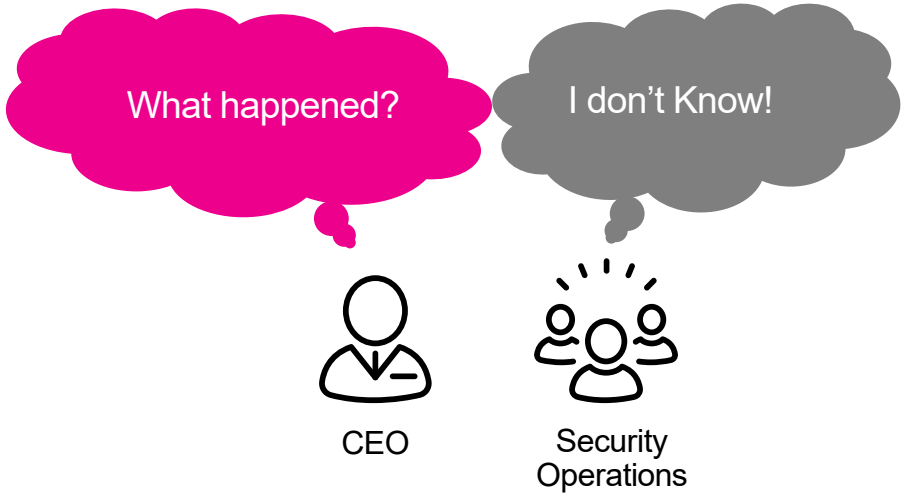
5) Benefits
The Taste

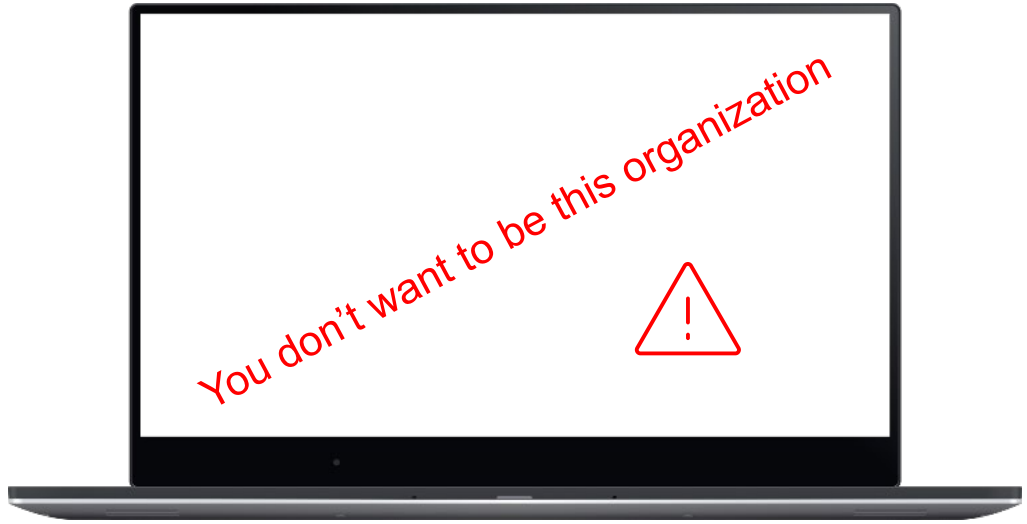
The Need – Why SIEM

Types of Organizations

Breached!

Don't know they have been breached!





That's where Splunk SIEM helps….

Common Myths and Facts

Myth	Fact
Just Network perimeter devices will suffice my security needs	Two thirds of security administrators admit that security intelligence platform is required. **SIEM solution has become mandatory to protect network from attacks**
Enterprise Security is only about compliance requirement for yearly audit	Top enterprises believe that security goes beyond yearly audit reports **Continuous monitoring is essential to secure the Enterprise systems**

Data Breach Statistics

Size of the problem

71%

Data breaches were financially motivated

52%

Breaches featured hacking

4.1B

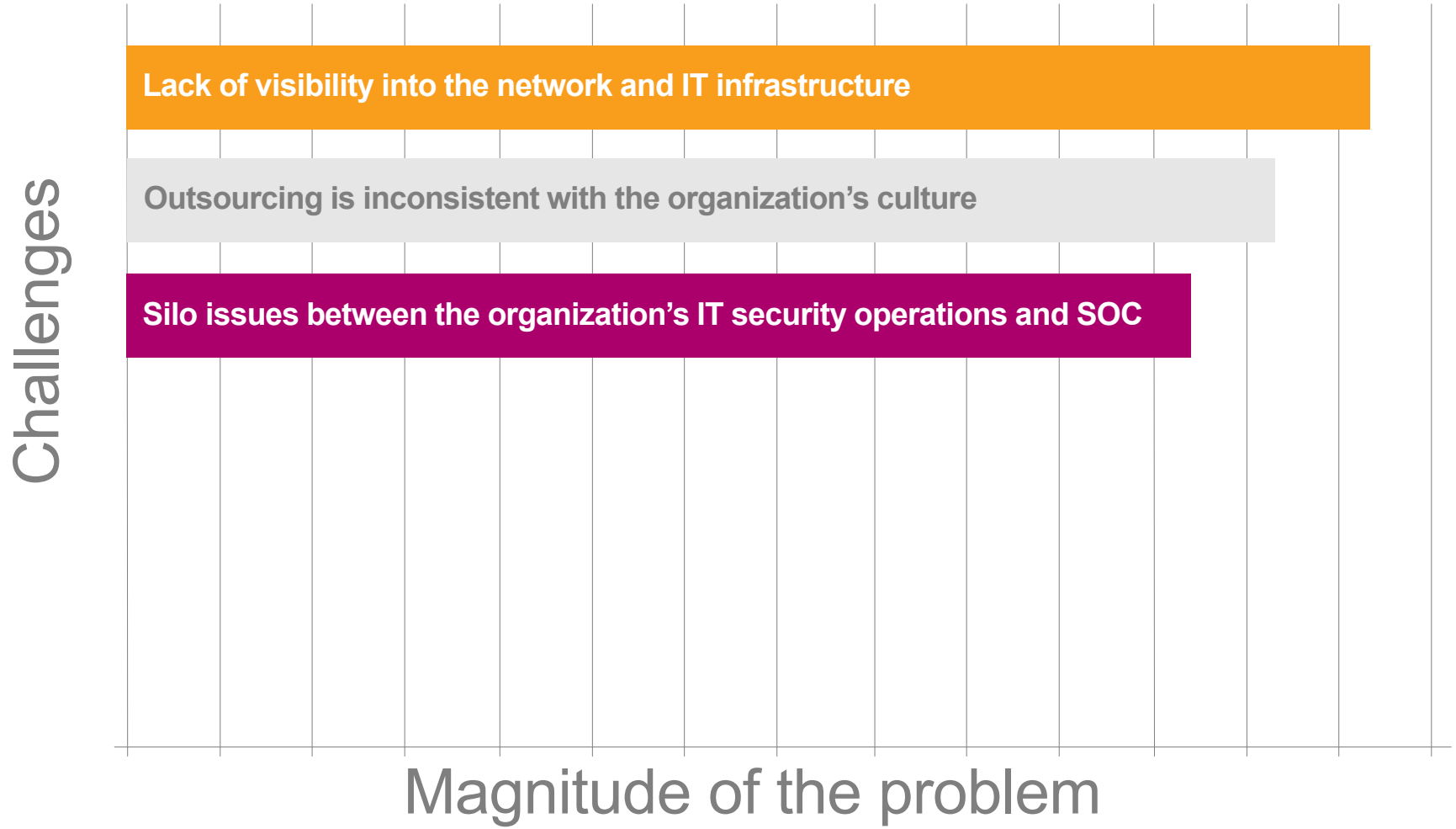
Records exposed by data breaches

3.92M

Average cost of a data breach

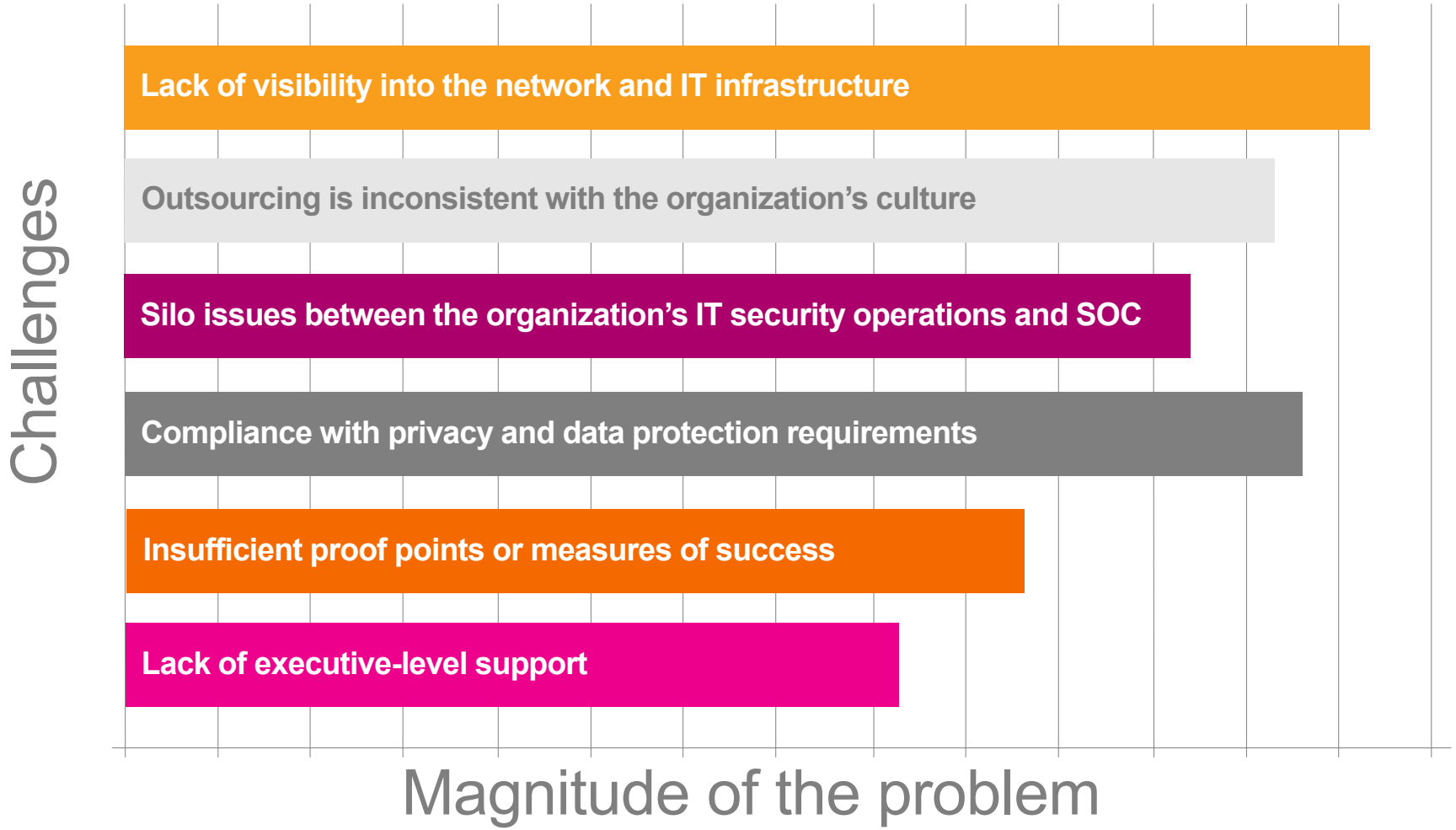
Challenges and the Need to Address Them

Problems in the general security set up



Challenges and the Need to Address Them

Problems in the general security set up



Our Journey and Experience

Observations and lessons learnt

Choose on-premise or cloud
Ample third part connectivity options

Plan for required license & storage
Importance relative to feasibility & affordability

No luxury to on-board everything
Not just a log management arena

Decide Most Valuable Resources
On-board them first

Our Journey and Experience

Observations and lessons learnt

Choose on-premise or cloud
Ample third part connectivity options

Plan for required license & storage
Importance relative to feasibility & affordability

No luxury to on-board everything
Not just a log management arena

Decide Most Valuable Resources
On-board them first

Add context & use frameworks
Assets, Identities, Threat Intelligence, Risk, etc.

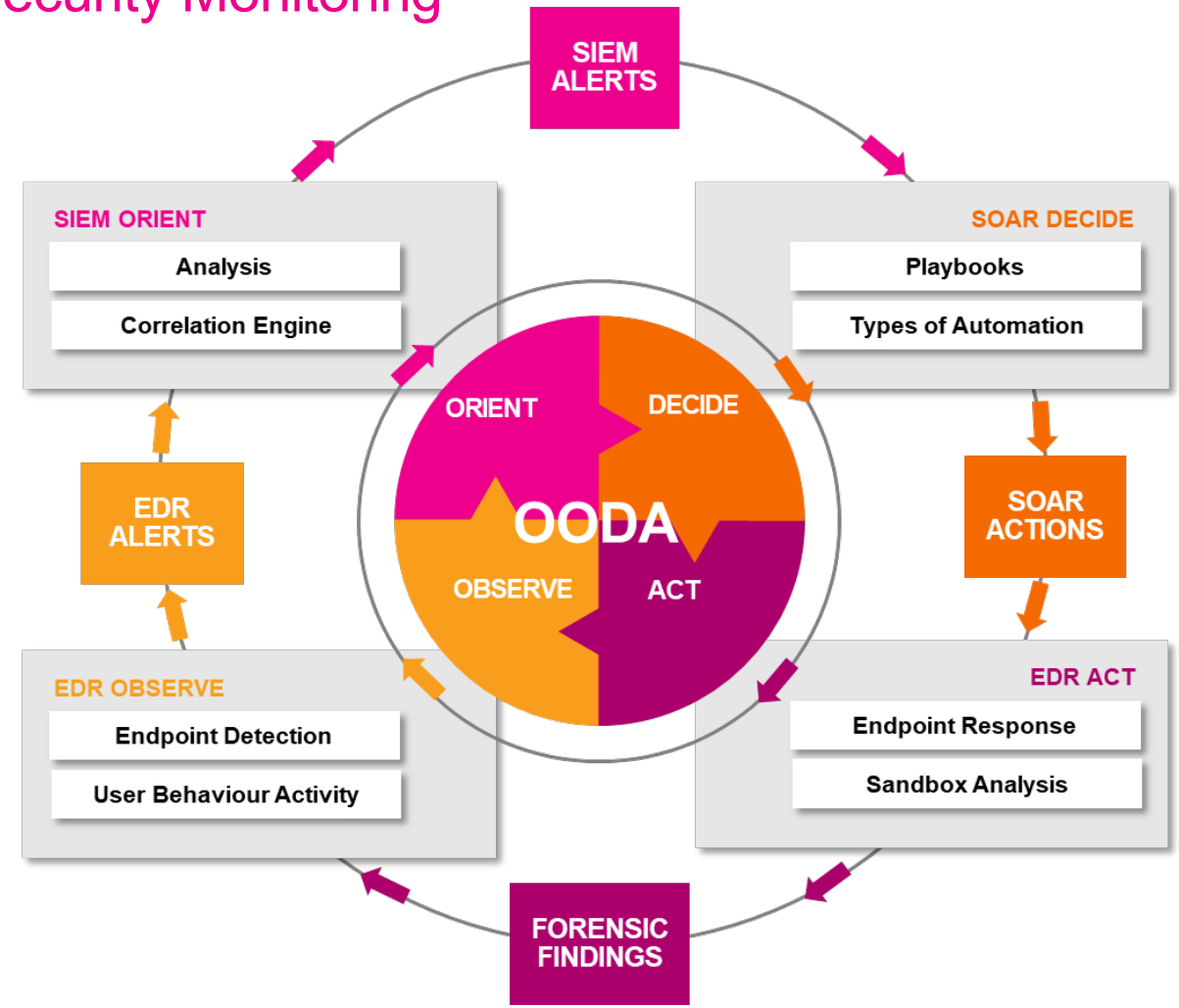
Identify crucial use case scenarios
Wider coverage versus depth

Watch Splunk Security Domains
Content updates is a starting point

Choose the battles
Be a Security advisor first

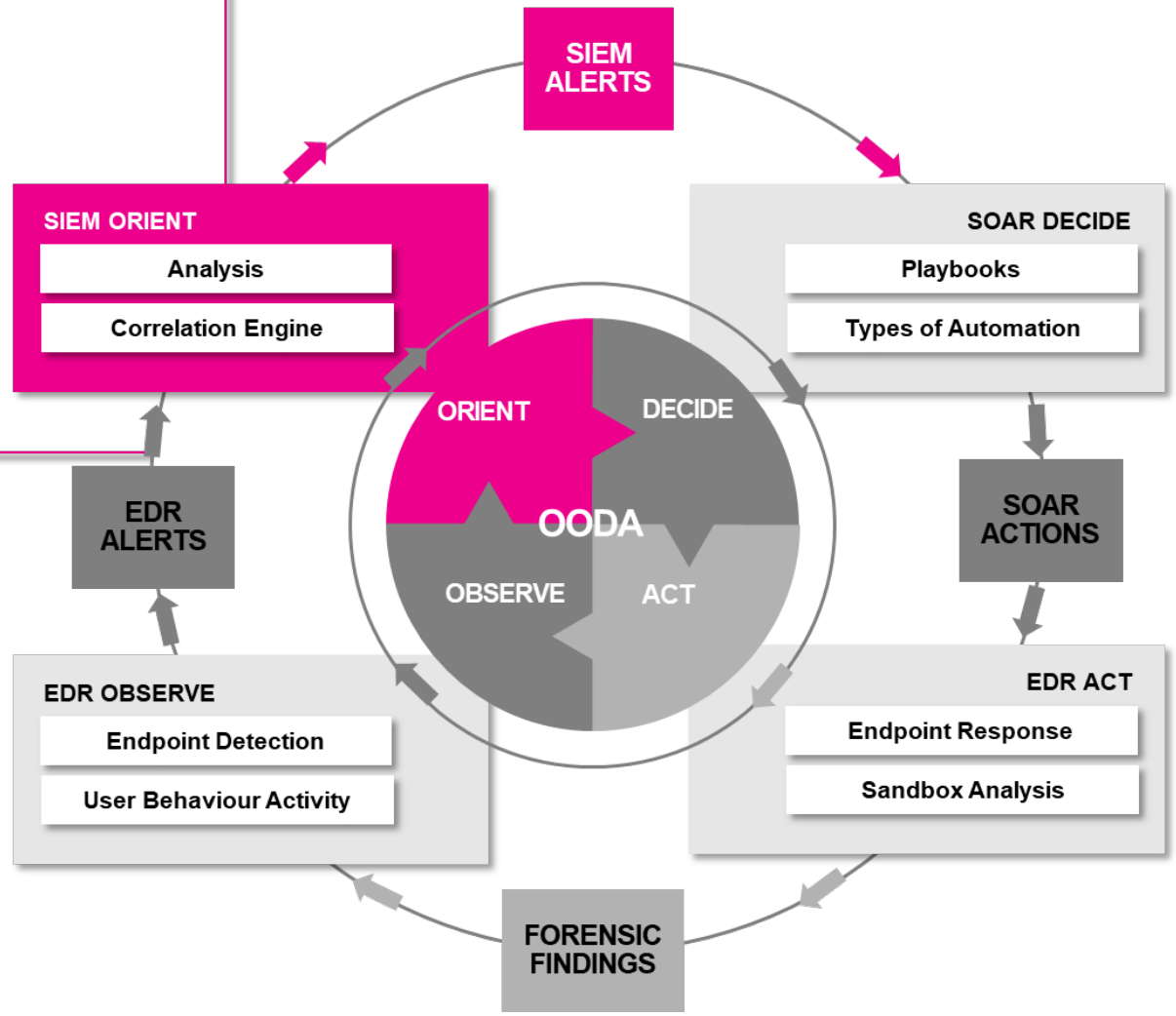
Decision Making Methodology

Applying OODA to Security Monitoring

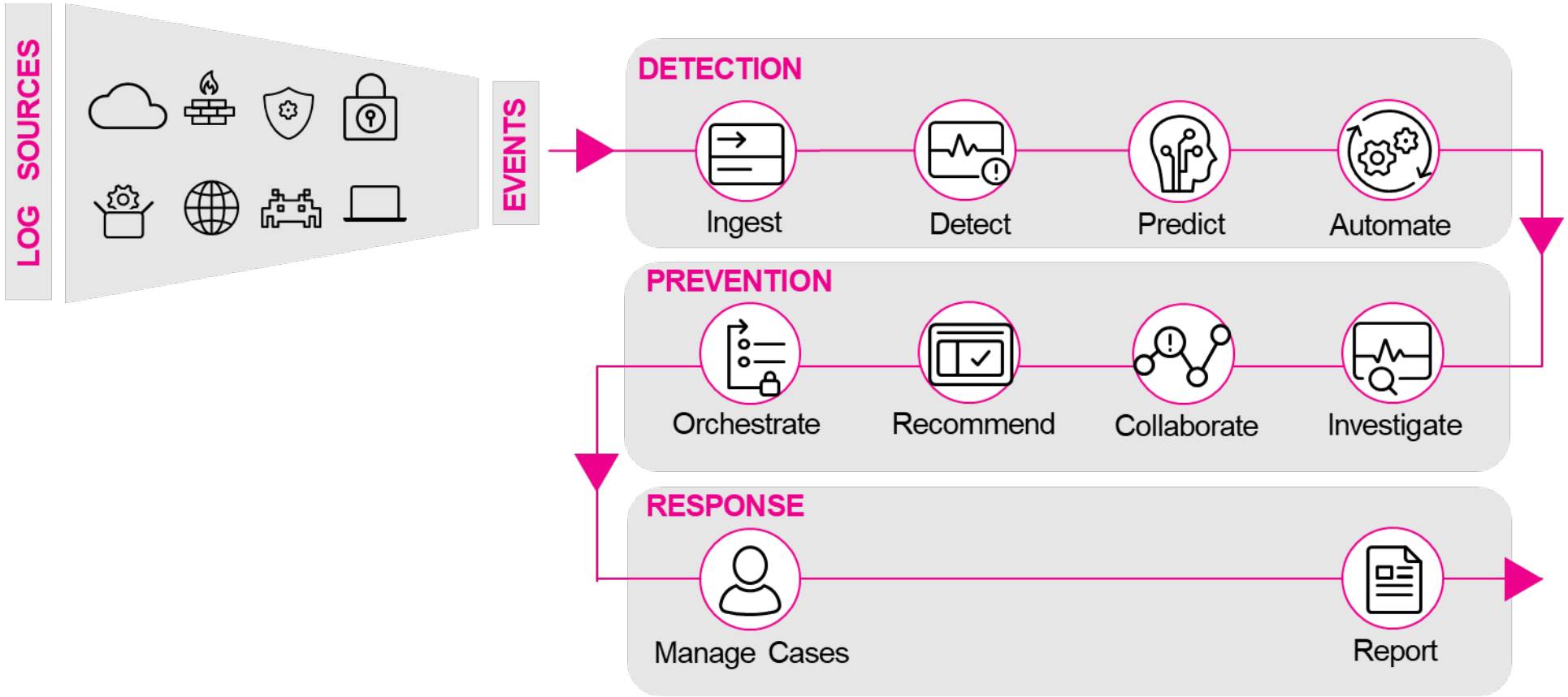


… with Focus on SIEM

- Security analytics
- Use case management
- Incident management
- Threat Intelligence
- Adaptive response
- Log Source Correlation
- User Behaviour Analytics
- Vulnerability Management

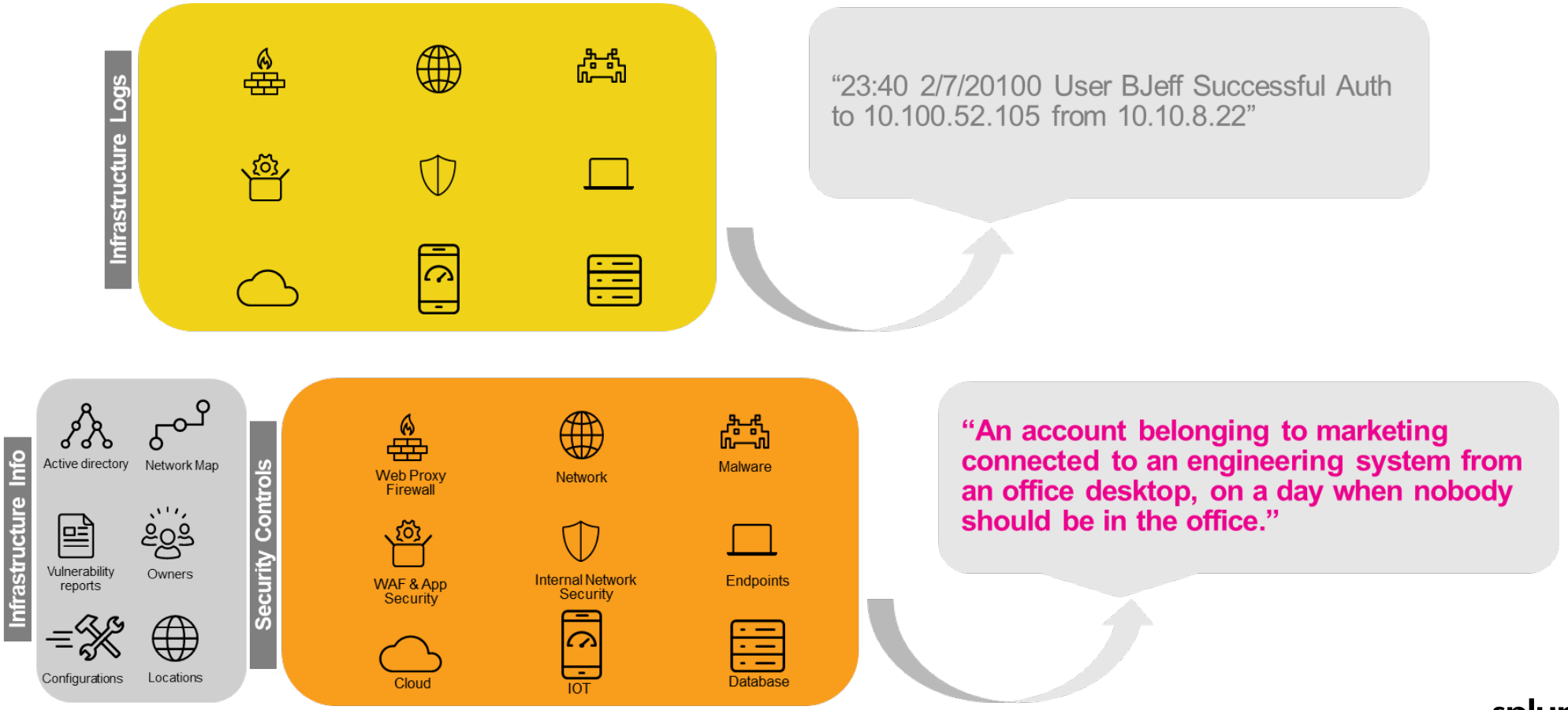


10 Building Blocks of Detection & Response



Logs, Alerts and Context to it

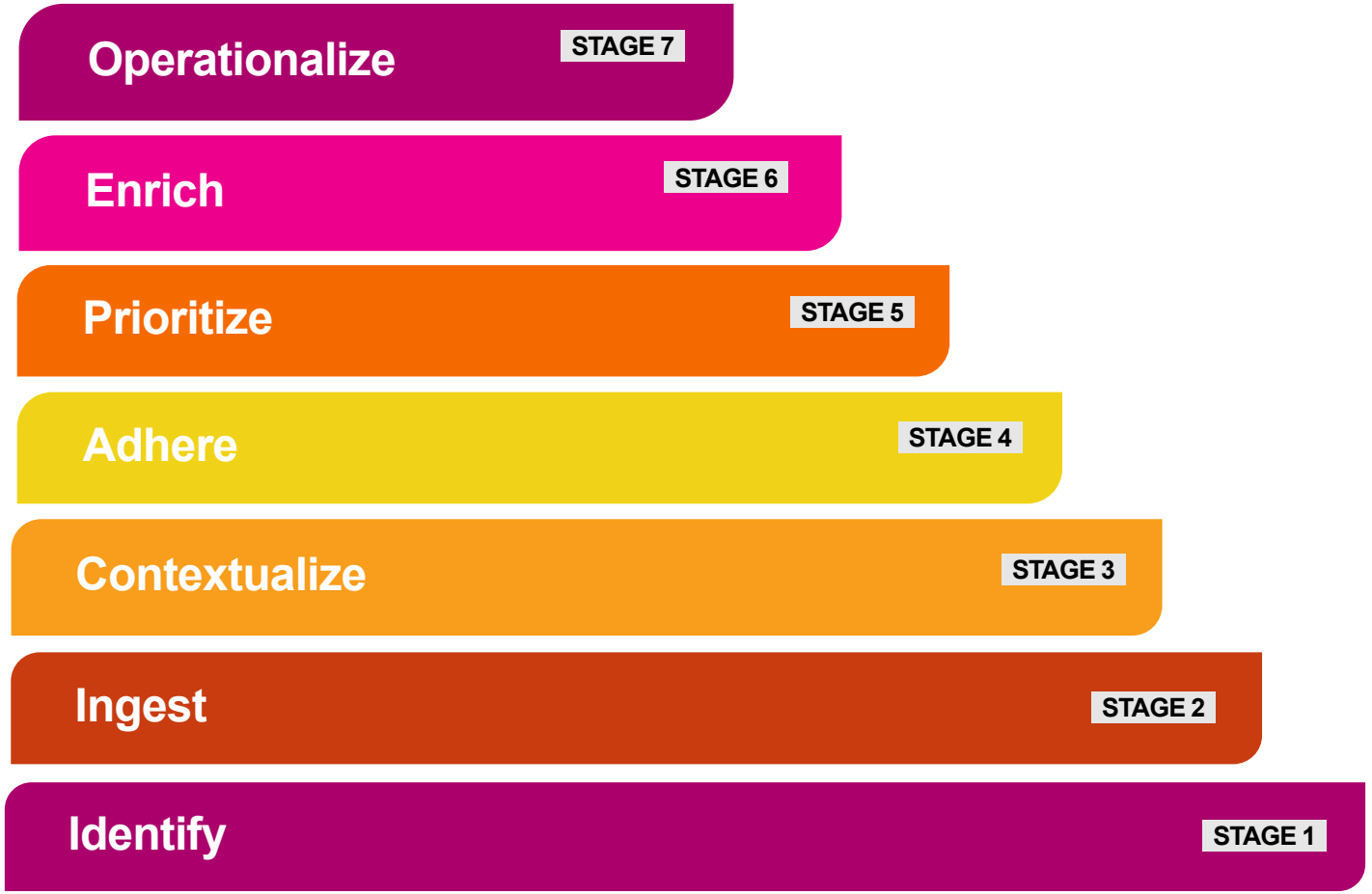
Adding clarity to detection of ‘An anomalous authentication event’



splunk> .conf20

Choose Critical Yet Achievable Scenarios

7 stages to choose achievable scenarios



Choice of Security Use Case Scenarios

Limit numbers and reduce alert fatigue

Major business risks to be addressed

Response mechanisms available

Availability of Logs & Security events

Use Case Scenario Selection

Ideal approach

Business Needs

- Splunk Security Domains
- Framework Mapping

Feasibility

- Available Logs
- Relevant events

Use Case Scenario Selection

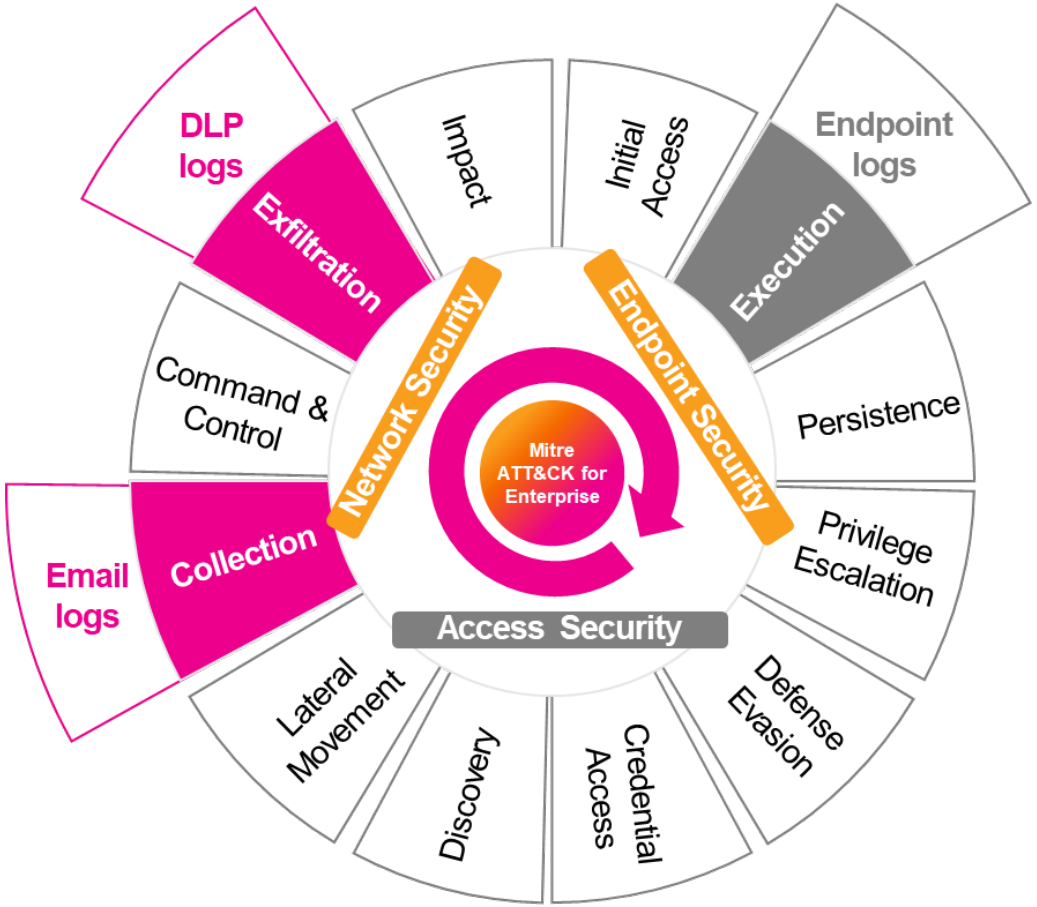
Ideal approach

Business Needs

- Splunk Security Domains
- Framework Mapping

Feasibility

- Available Logs
- Relevant events



Use Case Scenario Selection

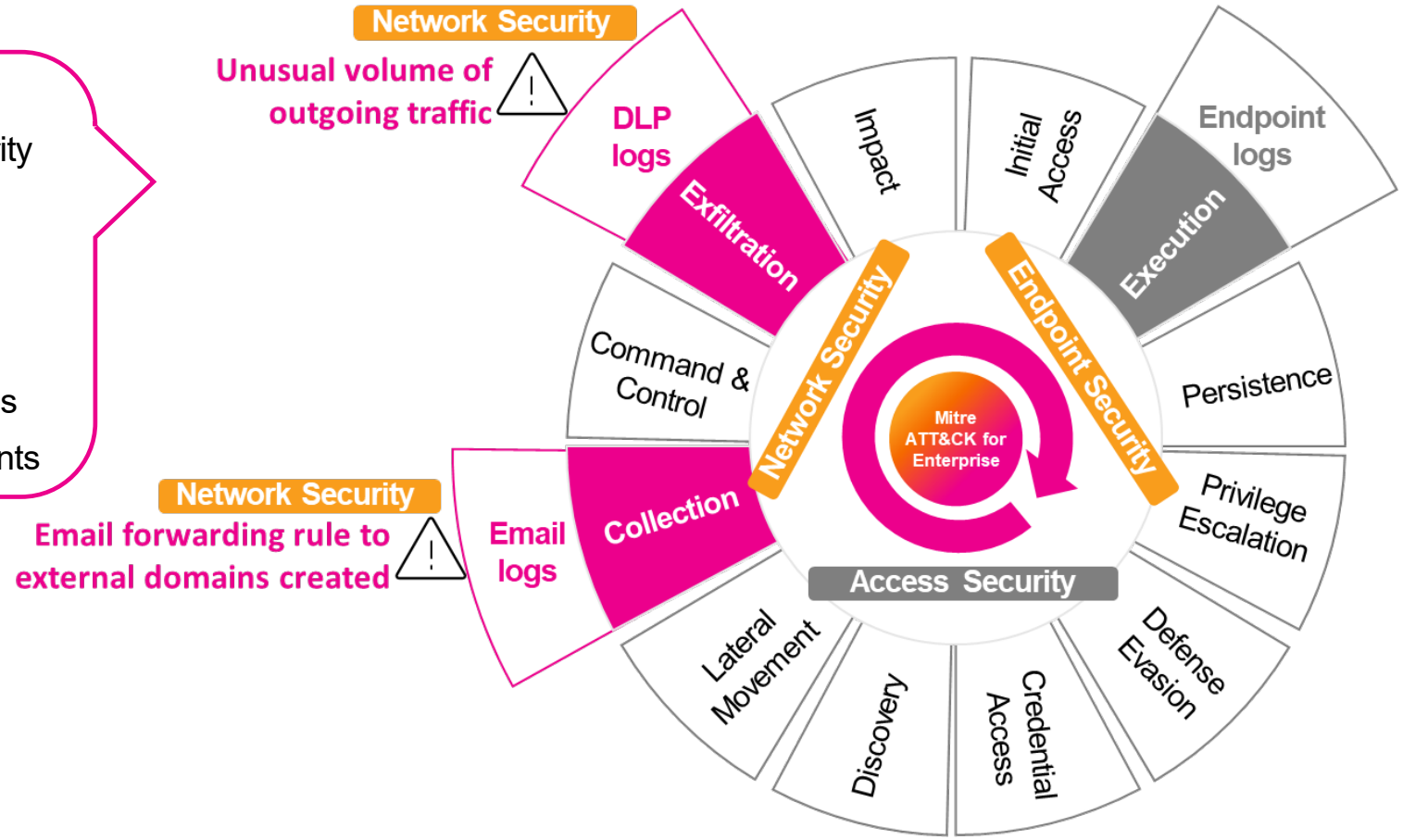
Ideal approach

Business Needs

- Splunk Security Domains
- Framework Mapping

Feasibility

- Available Logs
- Relevant events



Security Posture Key Indicators

Threat Activity

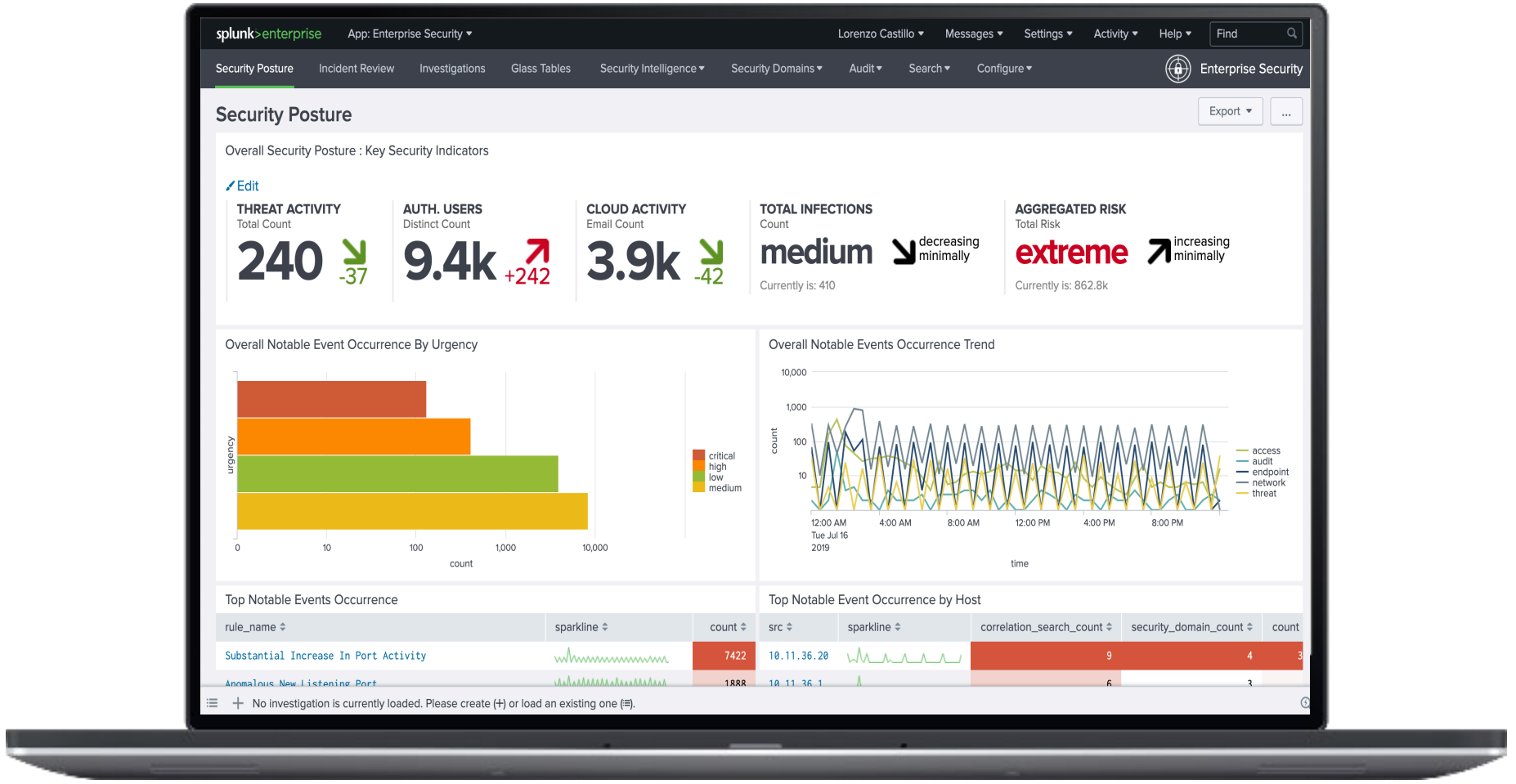
Affected users

Endpoint Activity

Network Activity

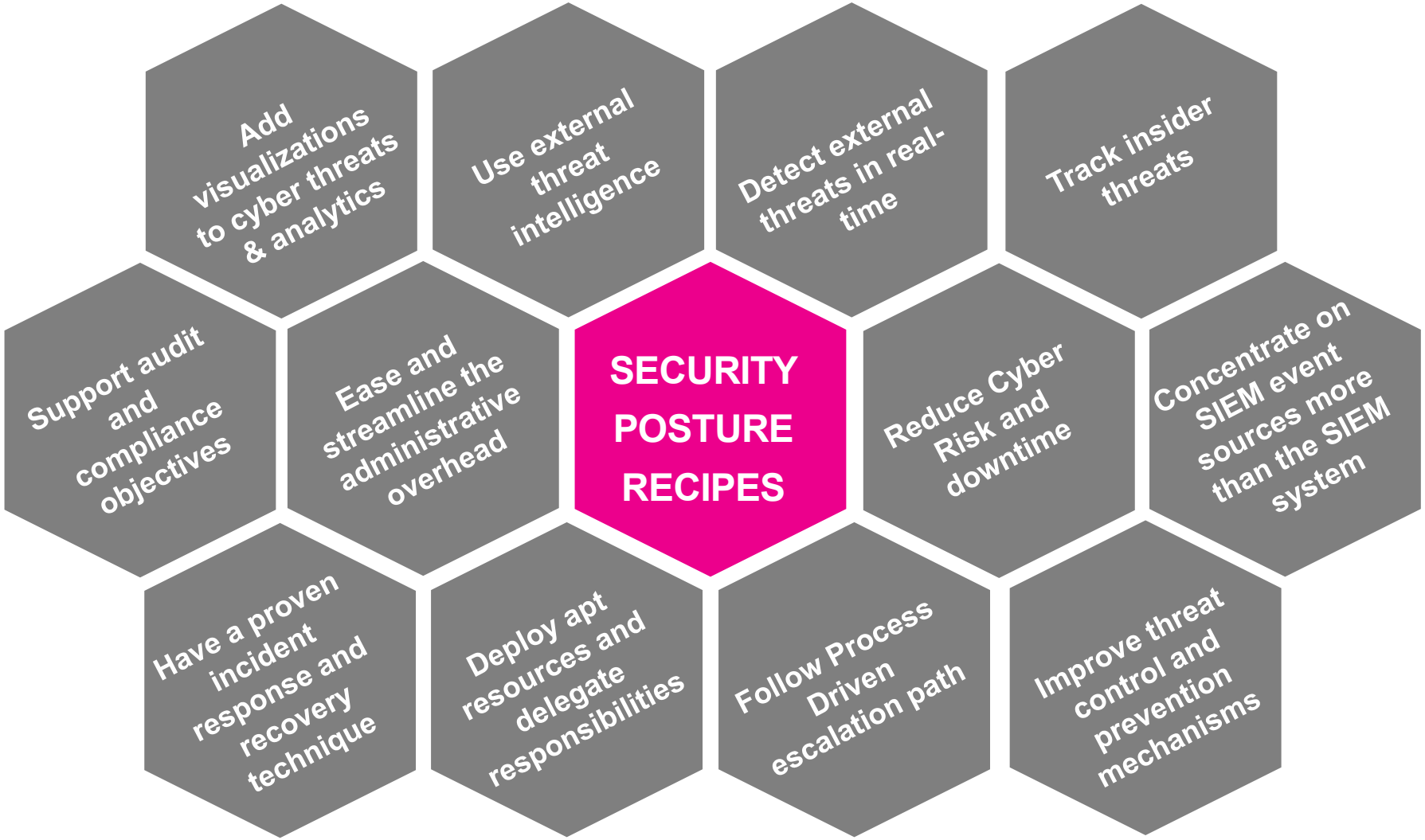
Audit events

Notables

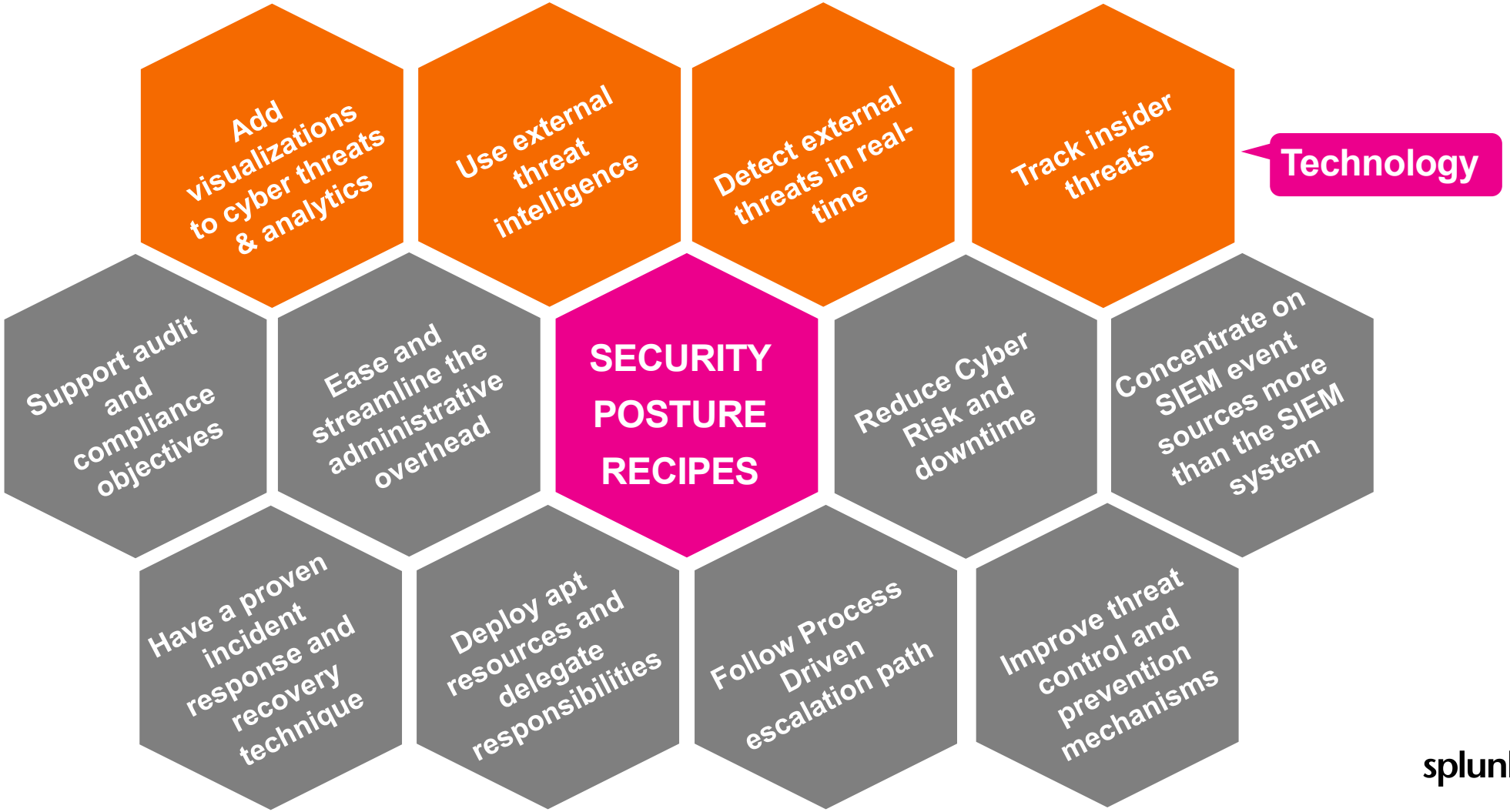


splunk> .conf20

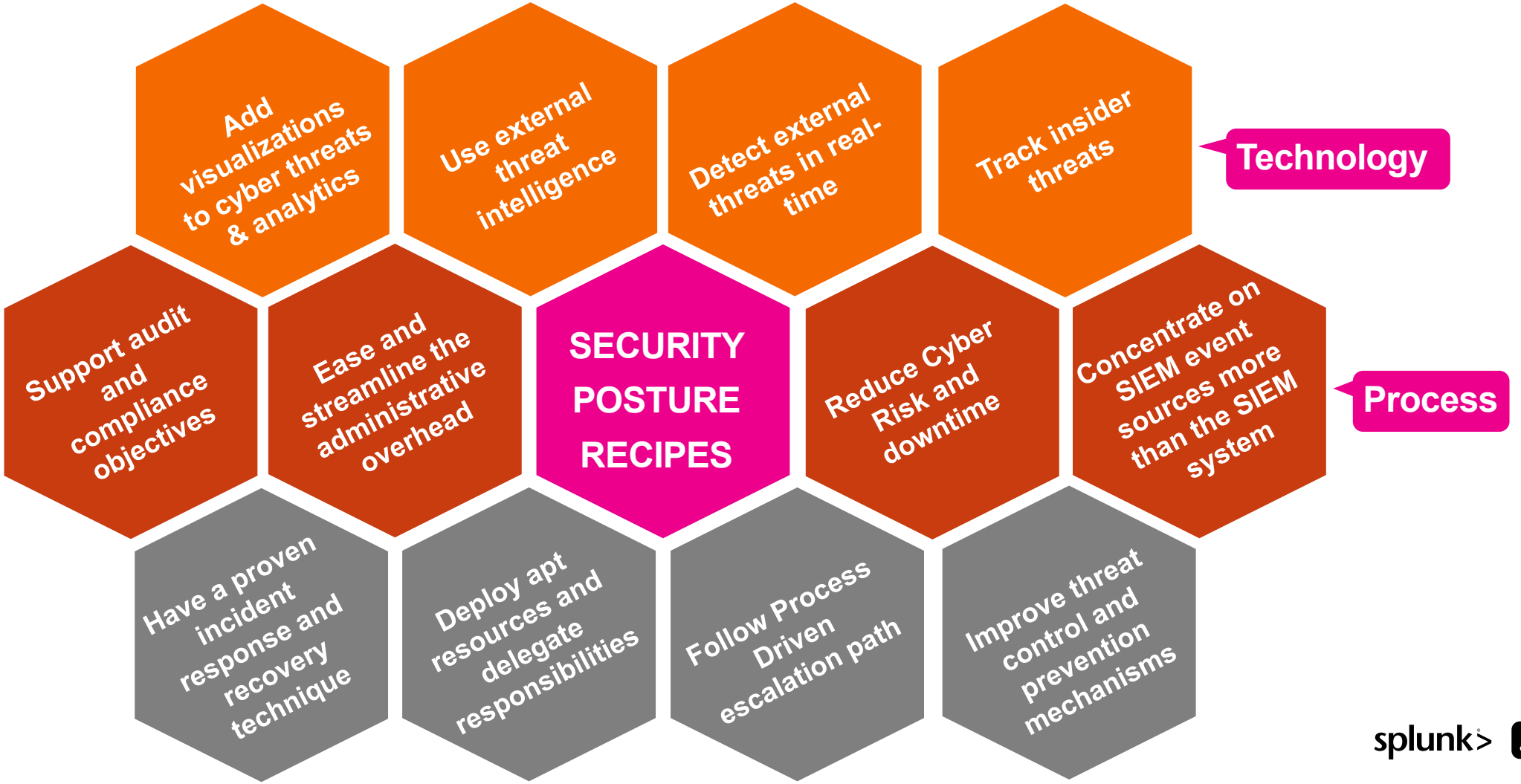
Security Posture – Recipes



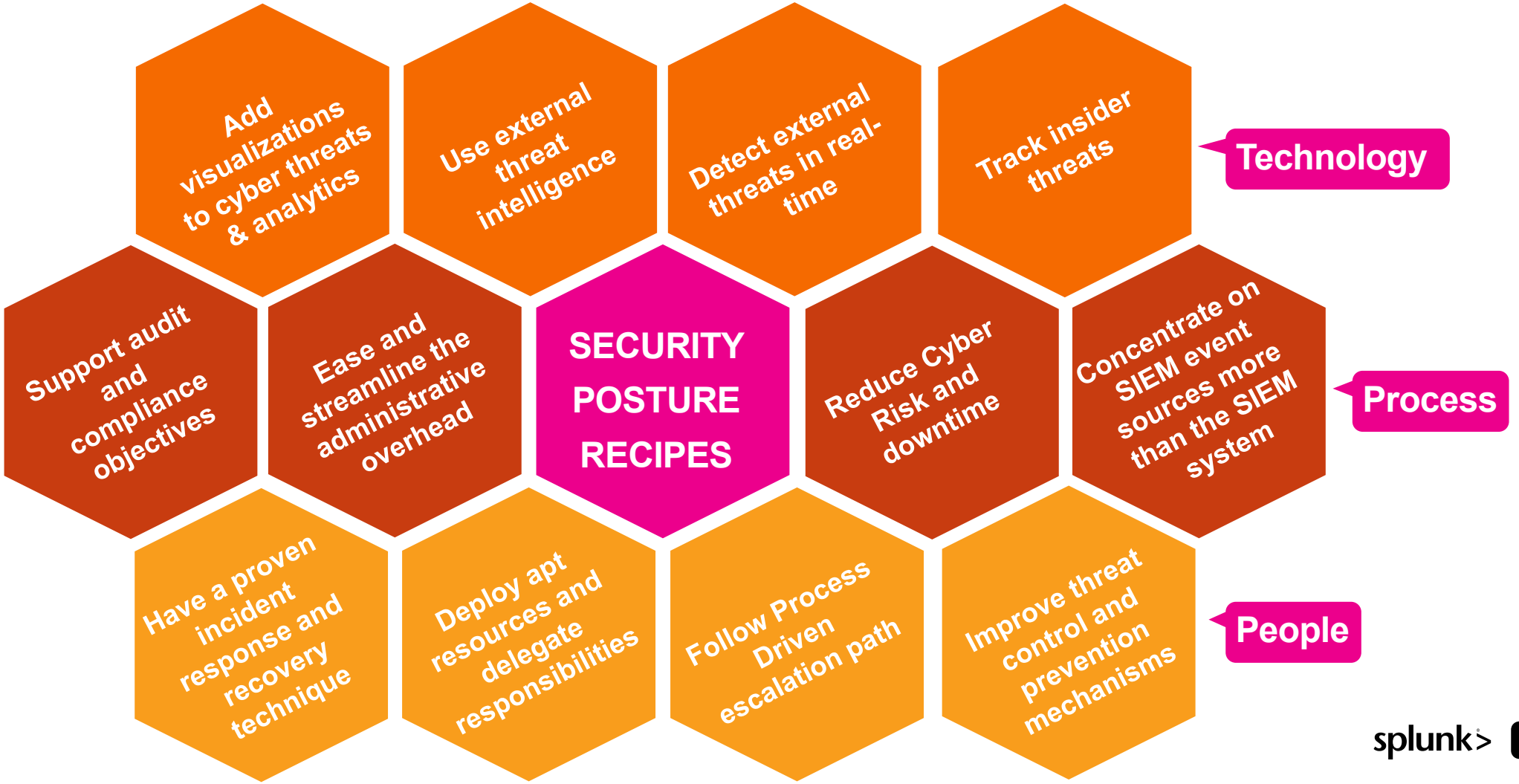
Security Posture – Recipes



Security Posture – Recipes

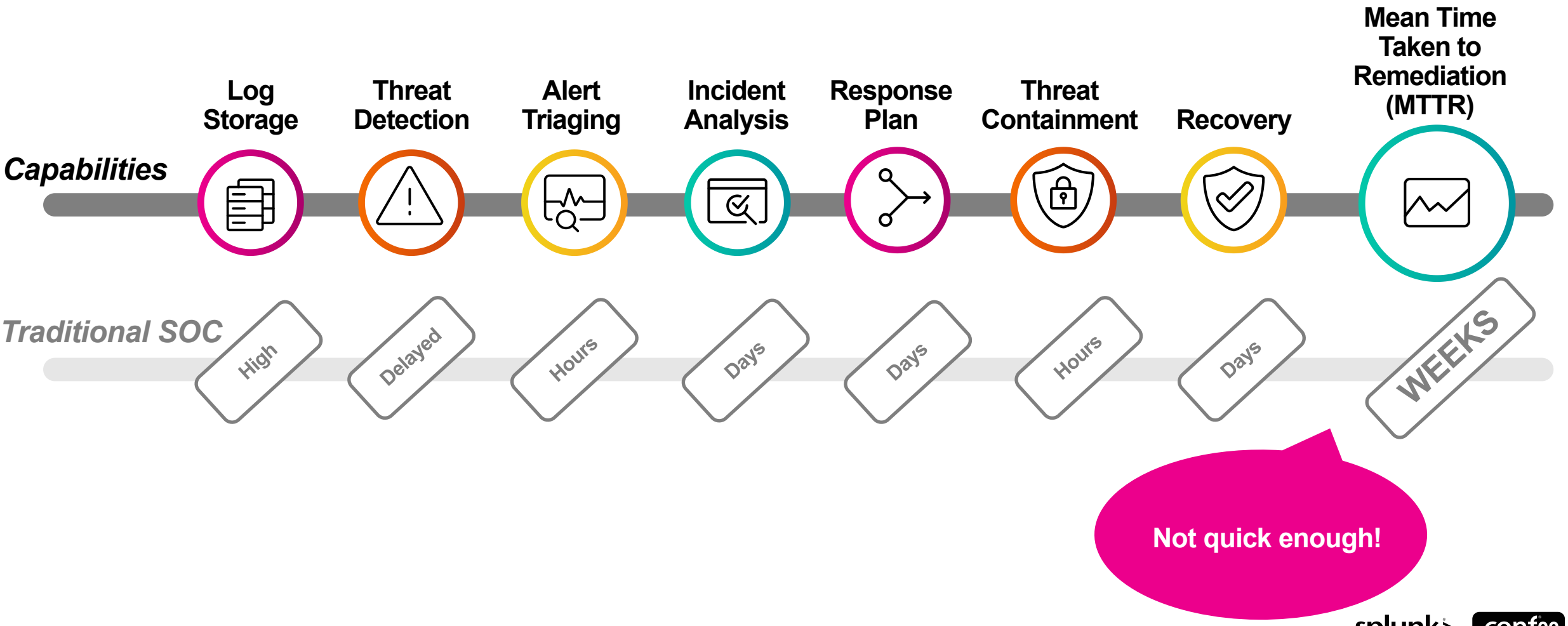


Security Posture – Recipes

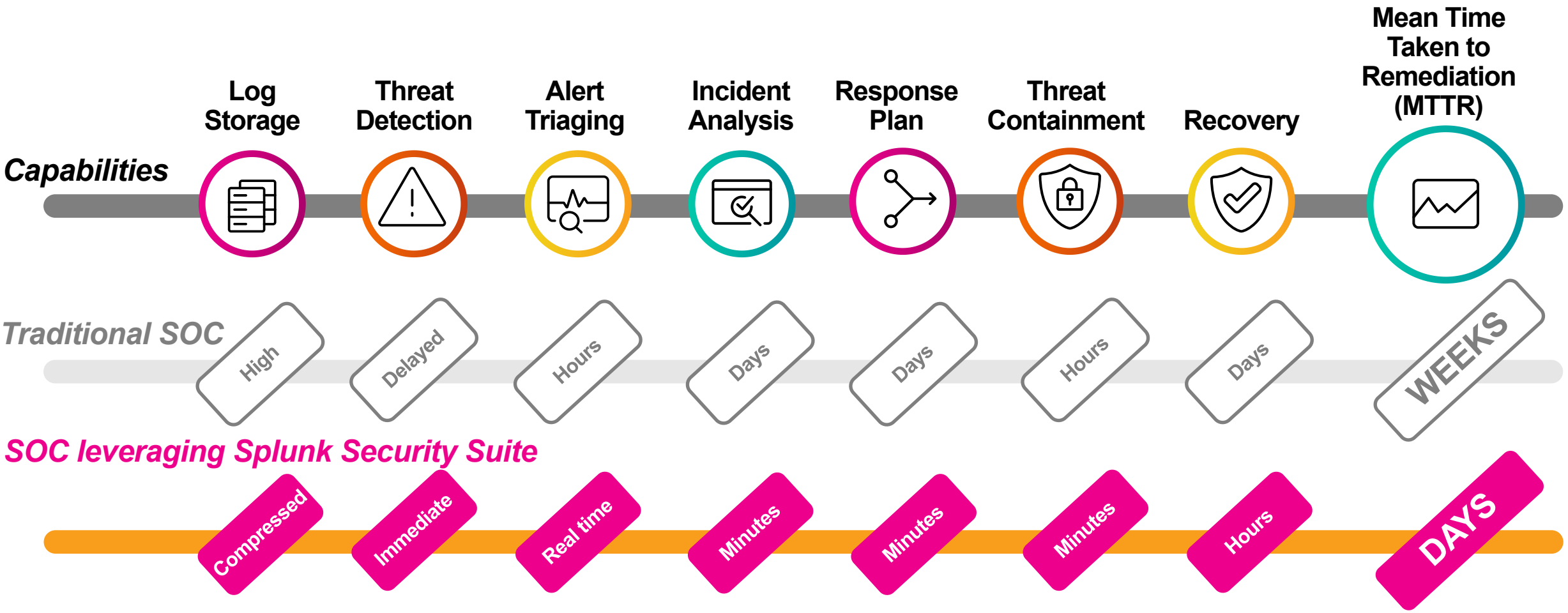


Benefits of Using the Recipe

Benefits of Using the Recipe



Benefits of Using the Recipe



Food for Thought

We have detected, to some level also responded to threats. What next?

UEBA – Unknown Unknowns (Splunk UBA)

SOAR – Automate & Orchestrate (Splunk Phantom)

Threat Intel – Intelligence driven cyber security solutions (Verizon Threat Research & Advisory Center)

Global SOC – Cater to better Response & Recover

Forensics – Cyber security evidence & procedure

Strengths that complement our solutions – Verizon SIEM Services, DBIR, VTRAC, Forensics labs, SOC & CSIRT

References

For more information

https://enterprise.verizon.com/en-gb/resources/reports/dbir/

https://pages.riskbasedsecurity.com/2019-midyear-data-breach-quickview-report

https://securityintelligence.com/posts/whats-new-in-the-2019-cost-of-a-data-breach-report/

https://en.wikipedia.org/wiki/OODA_loop

https://attack.mitre.org/matrices/enterprise/

https://www.nist.gov/cyberframework

https://docs.splunk.com/Documentation

Thank You

Please provide feedback via the

SESSION SURVEY