SECS2797 Building threat-driven use cases for the real-world with iDefense intelligence

John Rubey
Cyber Defense Manager | Accenture

splunk> .conf19

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.

Agenda

Use Case Overview

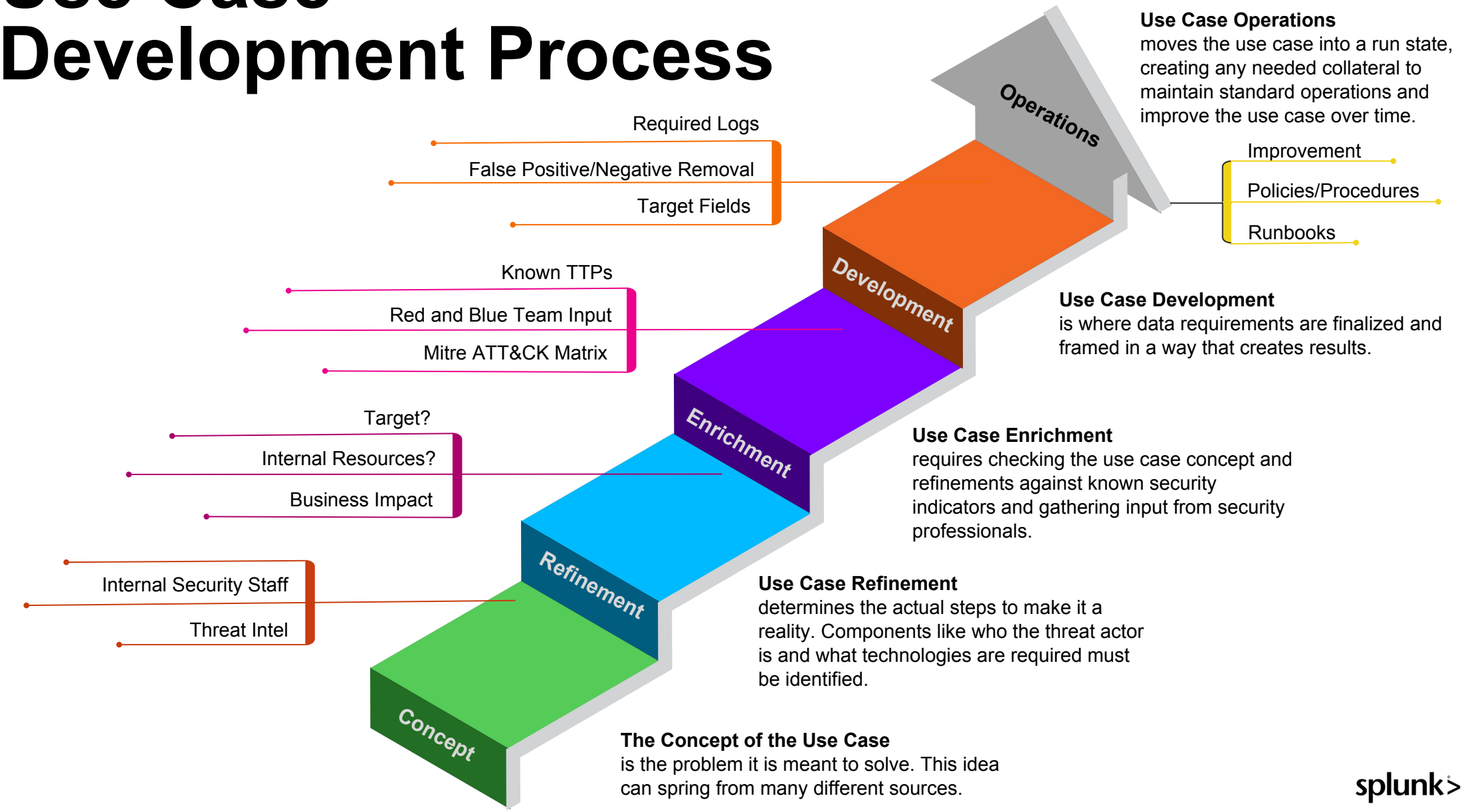
Sample Walkthrough

- Threat Actor Review
- Threat Actor Analysis
- Detailed Use Case Definition
- Use Case Prioritization

Use Case Overview

splunk> .conf19

Use Case Development Process



Use Case Operations
moves the use case into a run state, creating any needed collateral to maintain standard operations and improve the use case over time.

Use Case Development
is where data requirements are finalized and framed in a way that creates results.

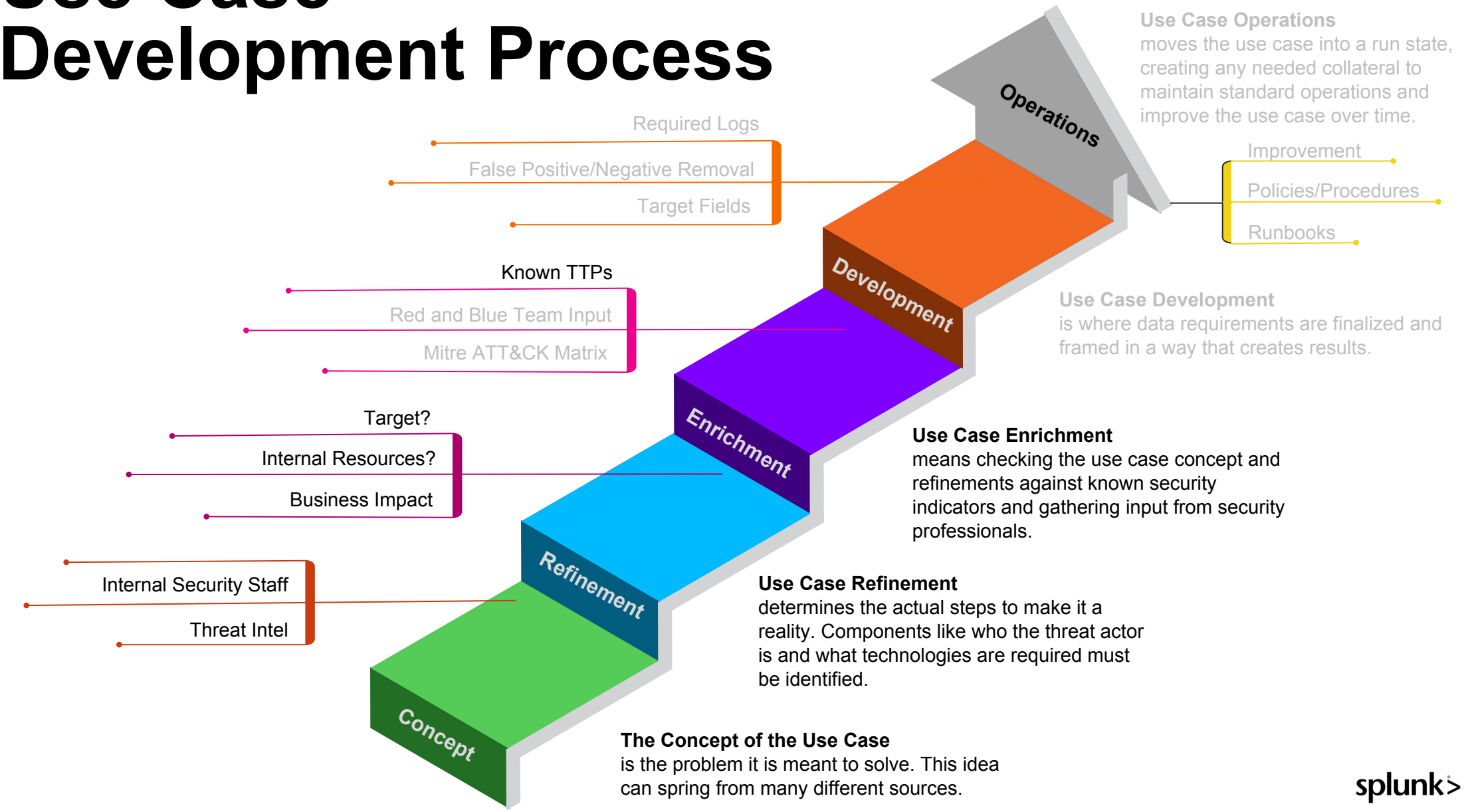
Use Case Enrichment
requires checking the use case concept and refinements against known security indicators and gathering input from security professionals.

Use Case Refinement
determines the actual steps to make it a reality. Components like who the threat actor is and what technologies are required must be identified.

The Concept of the Use Case
is the problem it is meant to solve. This idea can spring from many different sources.

splunk> .conf19

Use Case Development Process



Use Case Operations
moves the use case into a run state, creating any needed collateral to maintain standard operations and improve the use case over time.

Improvement
Policies/Procedures
Runbooks

Use Case Development
is where data requirements are finalized and framed in a way that creates results.

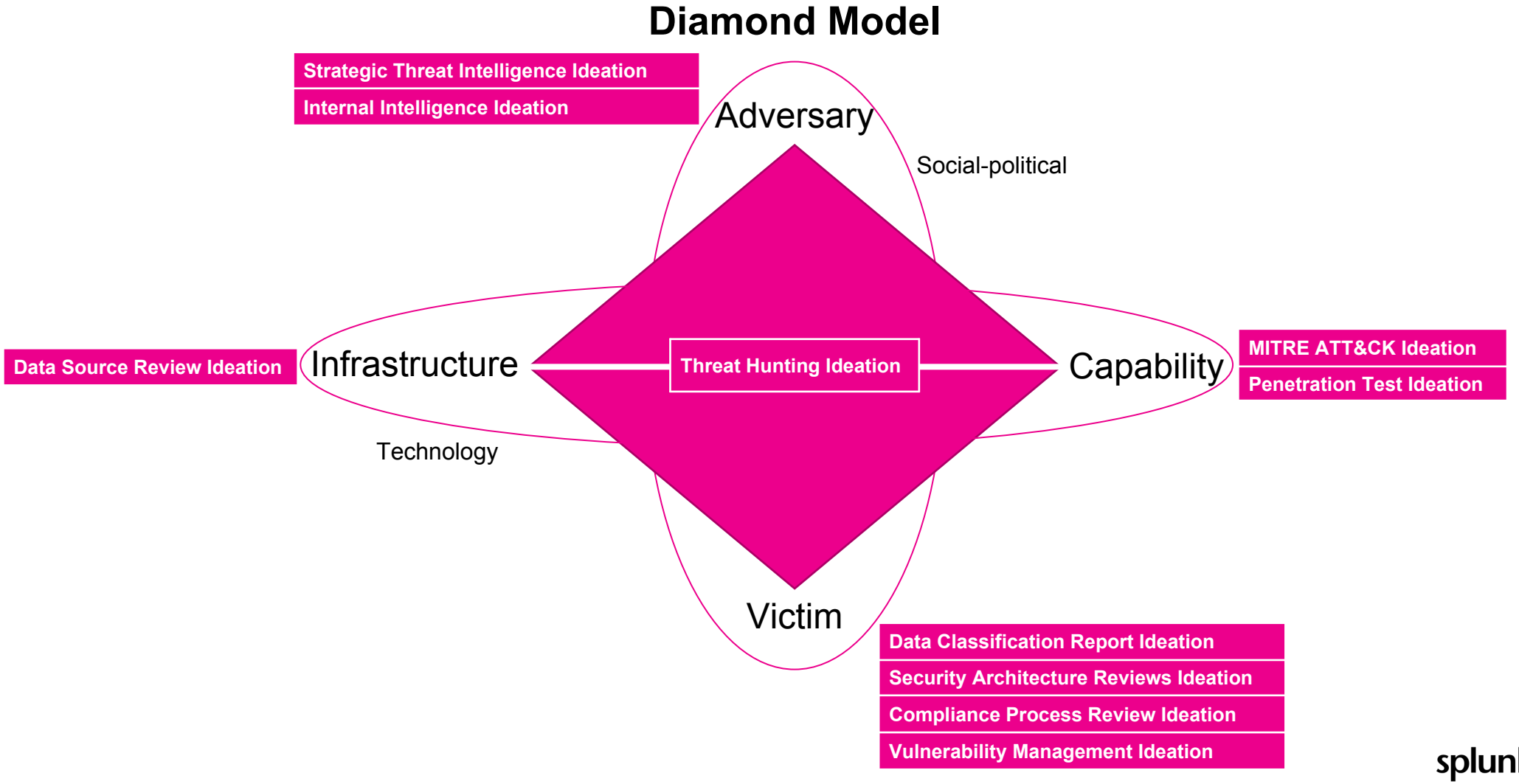
Use Case Enrichment
means checking the use case concept and refinements against known security indicators and gathering input from security professionals.

Use Case Refinement
determines the actual steps to make it a reality. Components like who the threat actor is and what technologies are required must be identified.

The Concept of the Use Case
is the problem it is meant to solve. This idea can spring from many different sources.

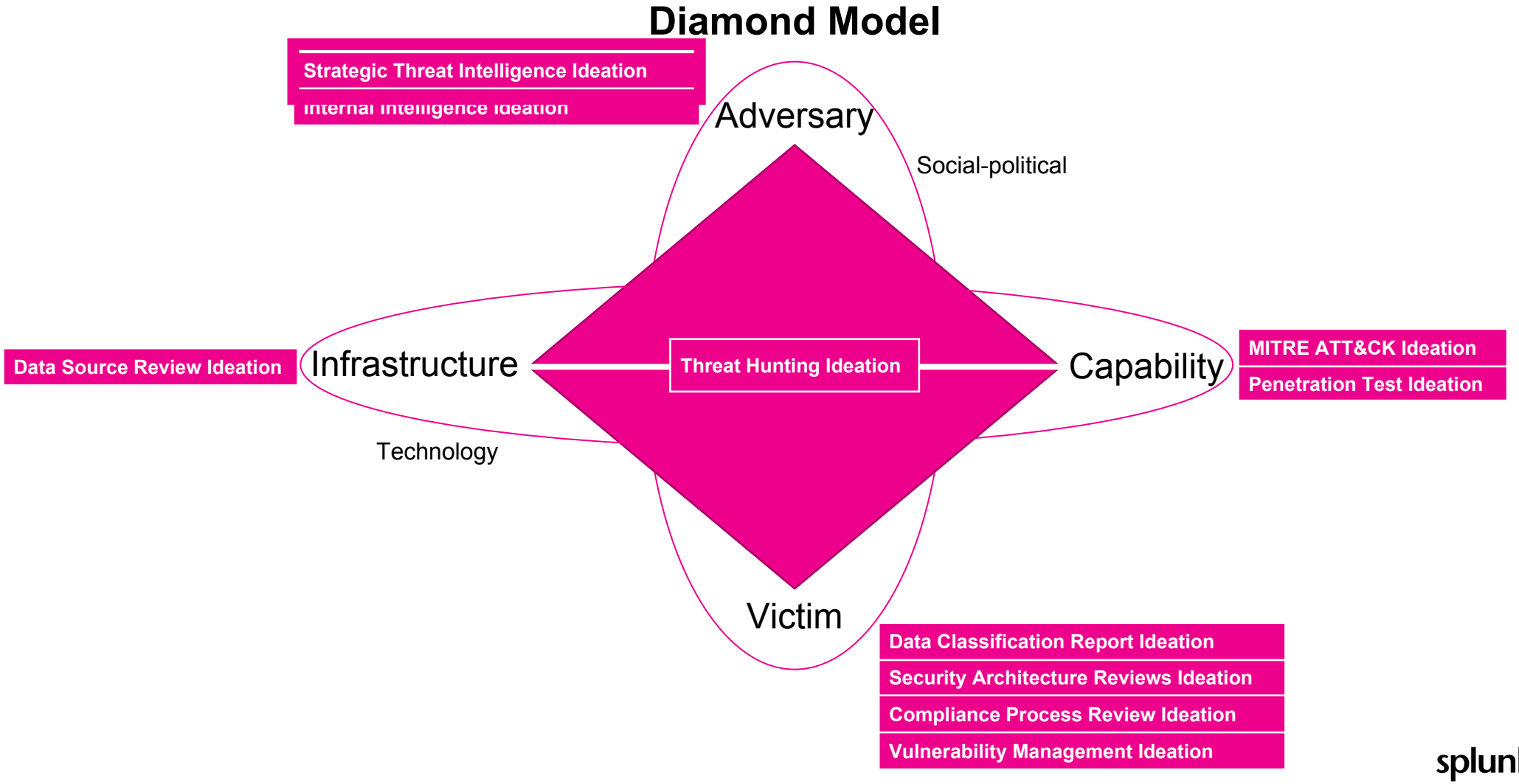
10 Sources of Use Case Inspiration

Look to understand the vertices of the Diamond Model within your organization to find sources of inspiration of your use case ideation.



10 Sources of Use Case Inspiration

Look to understand the vertices of the Diamond Model within your organization to find sources of inspiration of your use case ideation.



Example Walkthrough

splunk> .conf19

Process Overview

Develop industry-threat focused use cases

- Identify the threat actors relevant to industry
- Review threat actor-specific tactics, techniques, and procedures
- Identify use cases relevant to the business
- Map use cases to both existing and new data sources
- Prioritize implementation based on the specific threats

splunk> .conf19

HOGFISH Threat Actor

Sample threat actor analysis

The HOGFISH threat group has been operational since 2009. HOGFISH actors have conducted supply-chain focused attacks, where the initial action on objective is to compromise an MSP in order to subsequently gain access via legitimate, compromised user credentials to their client's networks for exfiltration of sensitive information.

Initial Compromise	Execution	Persistence	Defense Evasion	Credential Access	Discovery	Lateral Movement
• Spear Phishing Campaign • Malware attached to email	• Powersploit to inject code into PowerShell	• Autorun registry keys for malware persistence	• Utilized base-64 encoded content	• Mimikatz • pwdump	• Used net use to check for connectivity to machines • Scripts to enumerate IP ranges	• RDP

RECOMMENDED USE CASES

1. Monitor for malicious start-up tasks
2. Monitor for external emails from unknown domains with attachments
3. Monitor for common hacker tools

Use Case Sample

Sample use case for HOGFISH Persistence

Use Case Name:	Malicious Start-up Tasks
Threat Scenario	Threat establishes scheduled tasks, startup items or cronjobs to maintain persistence
Objective	Prevent competitors and malicious entities from creating malicious start-up tasks to establish malware persistence
Stakeholders	SOC
Tools	Splunk, Cylance, Carbon Black
Data Requirements	Windows, CrowdStrike, Cylance, Carbon Black, CyberArk
Logic	Alert on: • Unknown startup items • Unknown cron jobs • schtasks usage • Run registry key changes

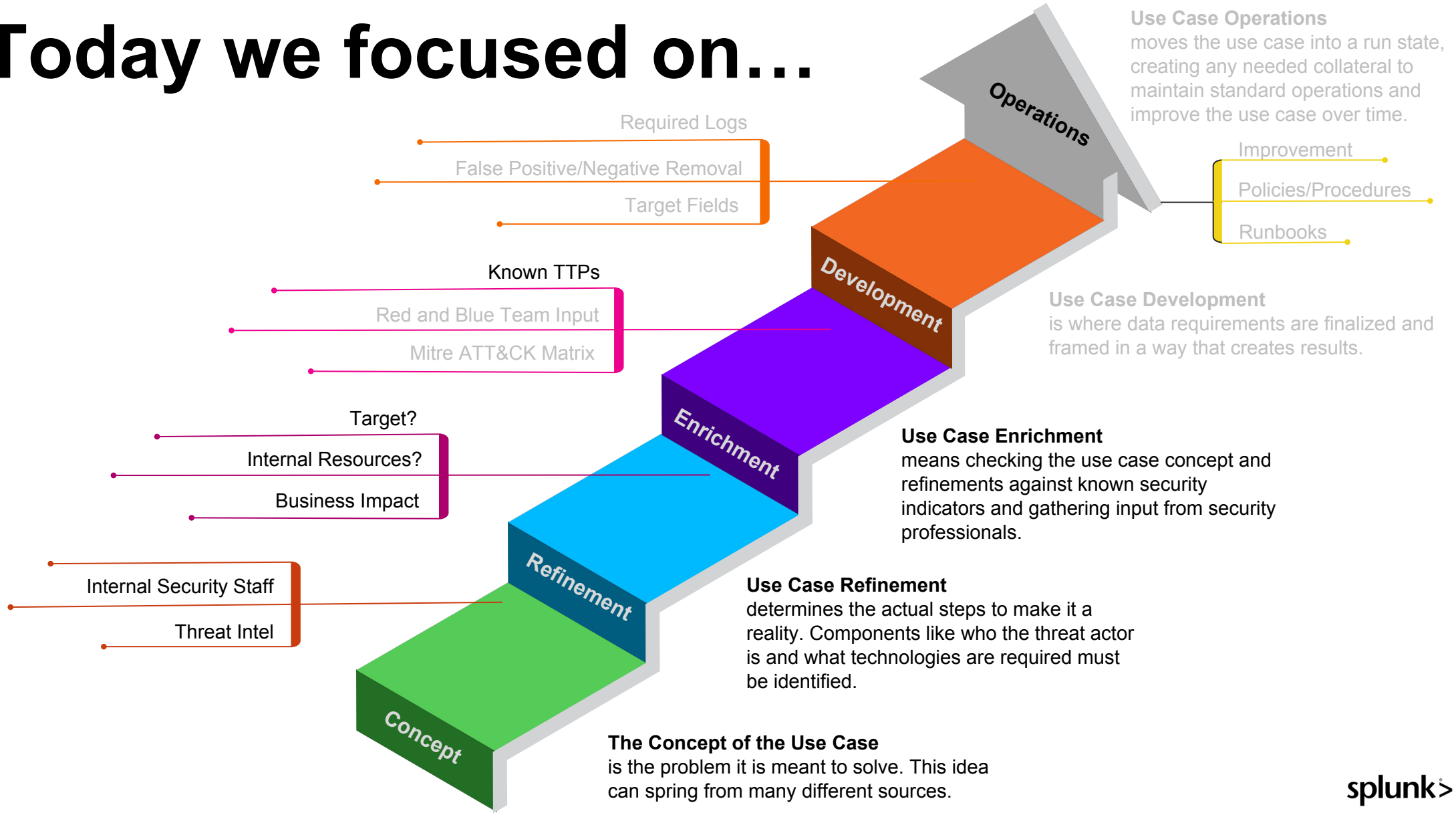
Prioritize Use Cases

- How severe is the threat? What is the impact to the business?
- Is the required data already available? How difficult will it be to get the required data?
- Are there existing compensating controls to prevent this activity?
- Do you have existing detection content for similar TTPs?
- Are there clear actions to investigate and respond to the use case?

Recap

splunk> .conf19

Today we focused on…



Use Case Operations
moves the use case into a run state, creating any needed collateral to maintain standard operations and improve the use case over time.

Improvement
Policies/Procedures
Runbooks

Use Case Development
is where data requirements are finalized and framed in a way that creates results.

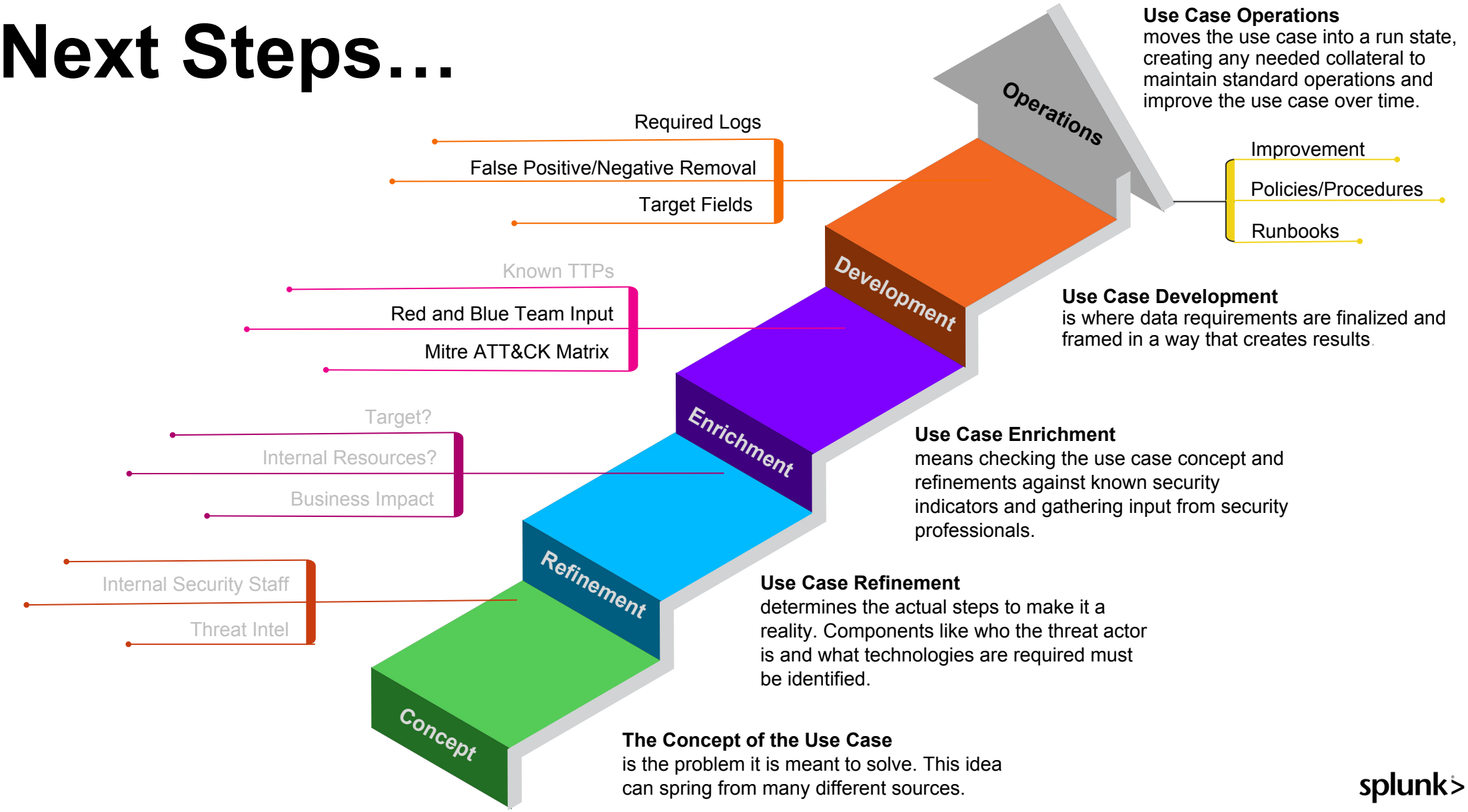
Use Case Enrichment
means checking the use case concept and refinements against known security indicators and gathering input from security professionals.

Use Case Refinement
determines the actual steps to make it a reality. Components like who the threat actor is and what technologies are required must be identified.

The Concept of the Use Case
is the problem it is meant to solve. This idea can spring from many different sources.

splunk> .conf19

Next Steps…



Use Case Operations
moves the use case into a run state, creating any needed collateral to maintain standard operations and improve the use case over time.

Use Case Development
is where data requirements are finalized and framed in a way that creates results.

Use Case Enrichment
means checking the use case concept and refinements against known security indicators and gathering input from security professionals.

Use Case Refinement
determines the actual steps to make it a reality. Components like who the threat actor is and what technologies are required must be identified.

The Concept of the Use Case
is the problem it is meant to solve. This idea can spring from many different sources.

splunk> .conf19

Key Takeaways

1. There are multiple sources of use case ideation to proactively detect threats
   - ACTION: review your current ideation processes for additional use case sources

2. Threat intelligence serves as a valuable source of detection content beyond simple indicator matching
   - ACTION: review your latest threat intel briefs to identify attacker TTPs for potential use cases

3. Security use cases require response to be effective
   - ACTION: validate your current detection rules are aligned to response processes

.conf19

splunk>

Thank You !

Go to the .conf19 mobile app to

RATE THIS SESSION