SEC1545 – Improve Your Cyber Monitoring & Response Strategy

Ed Svaleson
Security Consulting 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.

Session Outcomes

I would like you to take the following away from this session:

Evaluate and clarify the primary objective of your SOC program

Evaluate and refine your definition of *SOC use case*

Assess how comprehensive and effective your use cases are, and try the *detection matrix* recommendation

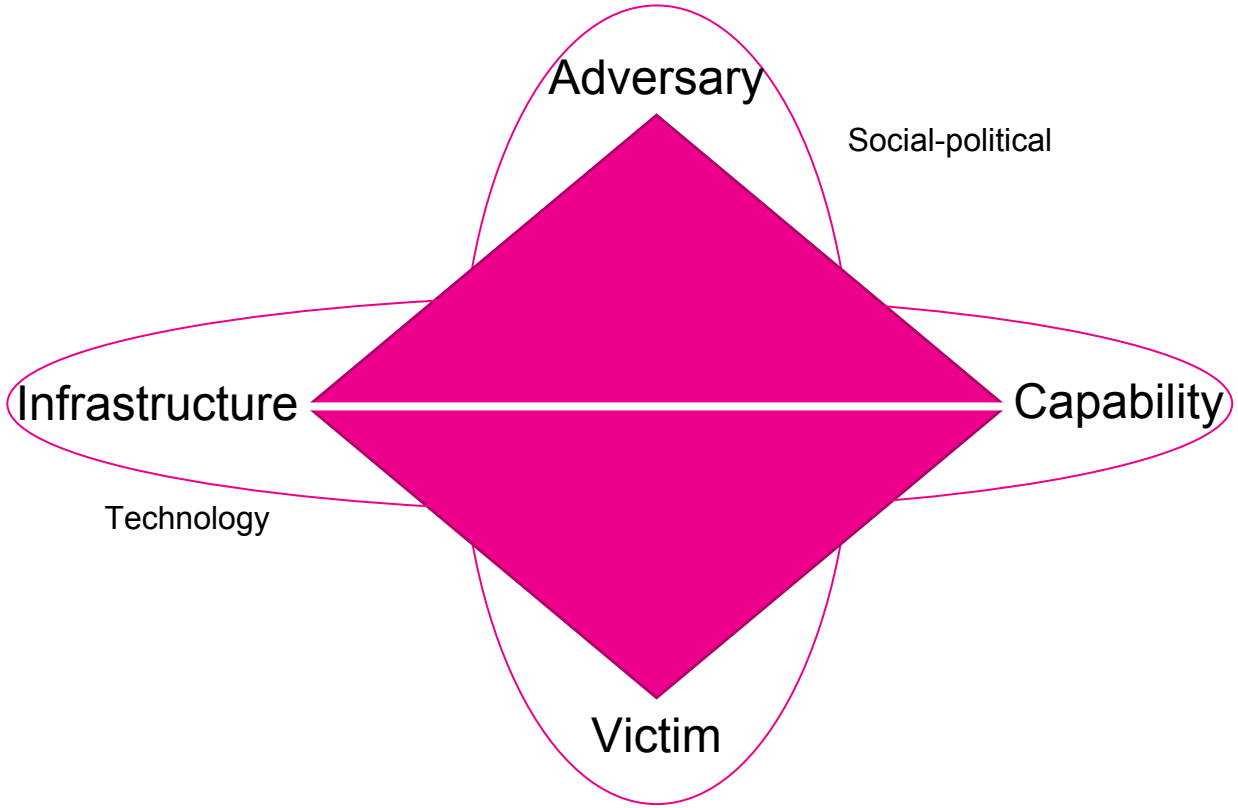
Evaluate your continuous use case improvement lifecycle, and sources of inspiration for your use cases

Strategy Requires an Achievable Objective

Security Operations Objective: Minimize the negative impact an adversary can produce on your organization

"For every intrusion event there exists an adversary taking a step towards an intended goal by using a capability over infrastructure against a victim to produce a result." –*Axiom 1 of the Diamond Model*

Diamond Model

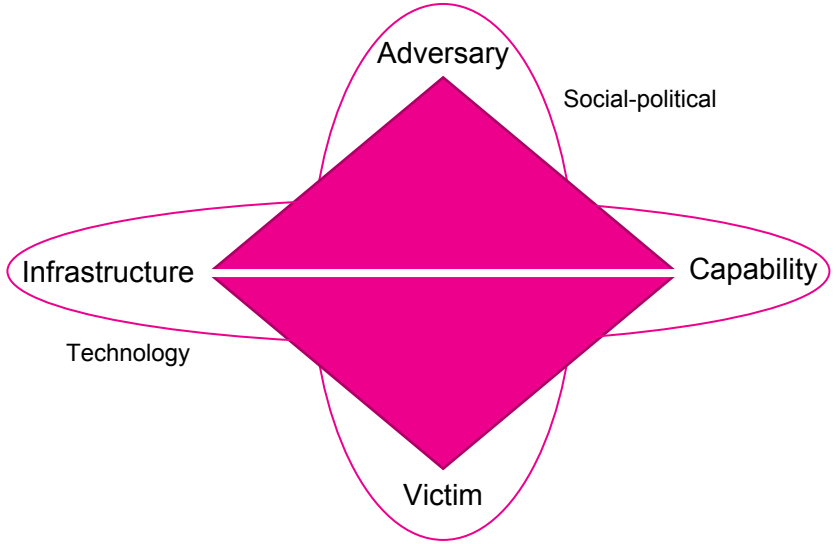


Effective Strategy

An effective strategy continuously addresses these four elements.

Who are our adversaries, and what are their motives and opportunities?

What infrastructure must our adversaries traverse to get to their targets, and what reliable telemetry can we employ to observe this activity?



What Tactics, Techniques, and Procedures do our adversaries employ, and what use cases can we develop to detect and respond to them?

How are we susceptible to being a victim, and what activities are normal vs. anomalous within our infrastructure?

Recommendation – Build a Detection Matrix

To be effective, we must understand where we have use cases to detect adversarial capabilities (i.e. TTP) over what infrastructure, and where we do not have coverage.

For this, build a detection matrix.

Detection Matrix (Use Case Mitre ATT&CK Mapping)

Infrastructure		Devices Reporting			Initial Access	Execution	Persistance	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Compliance	Total
	Servers	2294	2422	95%	2	4	12	4	6	1	9	10	0	2	2	6	56
	Endpoints	13504	31473	43%	0	2	0	0	1	1	0	0	0	0	1	1	5
	Database	205	241	85%	3	0	4	0	2	2	0	2	1	0	0	3	15
	Network	645	673	96%	1	0	0	0	0	0	12	5	0	3	3	0	22
	Application	11	972	1%	0	0	1	0	0	3	0	0	1	0	0	5	9
	Cloud (SaaS/PaaS)	1	13	8%	0	0	0	0	0	1	0	0	0	0	0	0	1
	IoT/ICS	35	241	15%	0	0	0	0	0	0	1	0	0	0	0	0	1
	Total	16695	36035	46%	6	5	16	4	9	7	20	16	2	5	5	15	106

To build matrix:

1. Document all use cases in a spreadsheet.
2. Add two columns to map to Mitre ATT&CK Tactics and to Techniques.
3. Add two columns to map to Infrastructure (categories as shown above) and Data Sources.

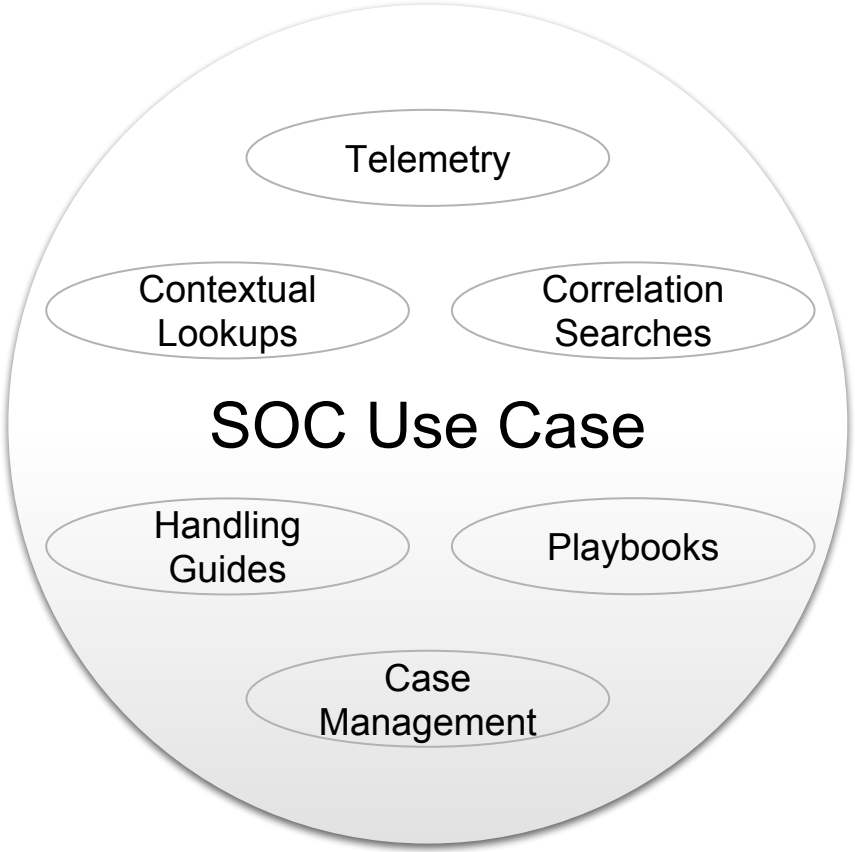
Notes:

- A single use case often maps to multiple tactics, techniques, data sources, and infrastructure categories.
- You may also want to add device counts (x of y reporting) to describe how many devices are actually sending correct data.
- Since use cases map to multiple tactics and infrastructure, you have to total those against the entire dataset.

Advantages of building Detection Matrix:

- ✔ To date, the Mitre ATT&CK matrix is the most comprehensive set of TTP to represent the spectrum of adversarial capabilities.
- ✔ Understand where you have coverage and where you do not.
- ✔ Understand the natural bias you/your team has (i.e. if you have an I&AM background, most of your use cases are likely I&AM related).
- ✔ The mapping exercise by itself will help you understand your use cases on a deeper level, and you will likely get additional ideas just doing the mapping.
- ✔ Asking others to get involved in mapping typically sparks debate and also leads to additional ideas on how to increase coverage.
- ✔ Mapping use cases to data requirements also set the requirements for data health monitoring.

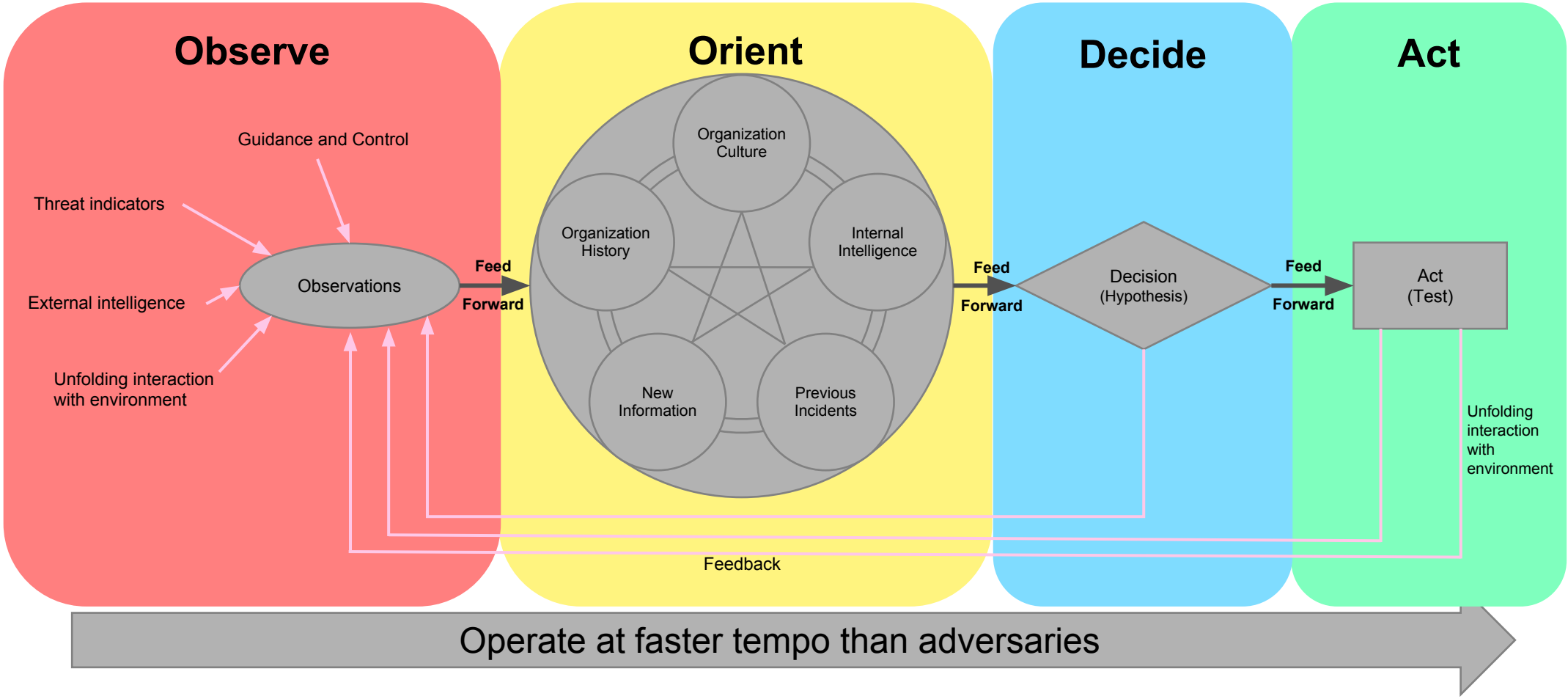
Definition: *SOC Use Case*



An *operational function* to detect **and** respond to one or more adversarial capabilities.

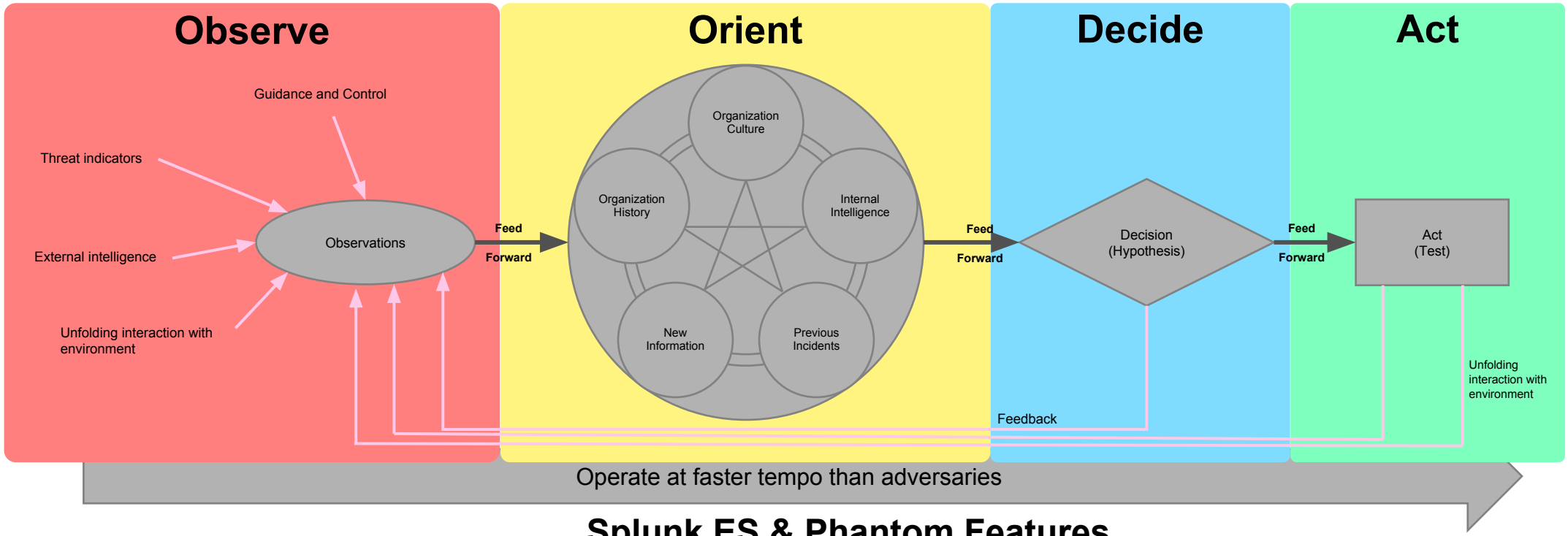
Understand End-to-End Cyber Response

To efficiently respond to cyber threats, Analysts must be able to observe, orient, decide, and act to disrupt kill chains faster than the adversary can rebuild them.



Cyber Security Use Cases Must Account for SOEL

To achieve this efficiency, we must expand the definition of security use cases from detection alerts to the end-to-end Security Operations Event Lifecycle, and evaluate how to make each step in the decision process faster.



Splunk ES & Phantom Features

- Correlation Searches
- Dashboards and Visualizations
- Tactical Threat Intelligence Integration
- Glass Tables (aggregated KPI views)
- Real-time Event Data
- Scripted Inputs
- Asset and Identity Lookups
- CSV Lookups and KVstores
- Notable Events Store
- Investigative Journal
- Contextual Logs (VM, DNS, DHCP)
- Workflow actions
- Incident Response Workflow
- Statistical Commands
- Machine Learning
- SOAR Playbooks
- Adaptive Response Actions
- ITSM Integration
- SOAR Action Playbooks

splunk> .conf19

Tactical Guidance on Efficient Operations

Orchestration first – First start with understanding your detection and response processes and how to orchestrate them, then focus on automation

Prioritize your process engineering –

- Identify the processes you operate the most, and which response processes are most business critical (e.g. ransomware response)
- Prioritize your process engineering on the above and level of effort to make changes

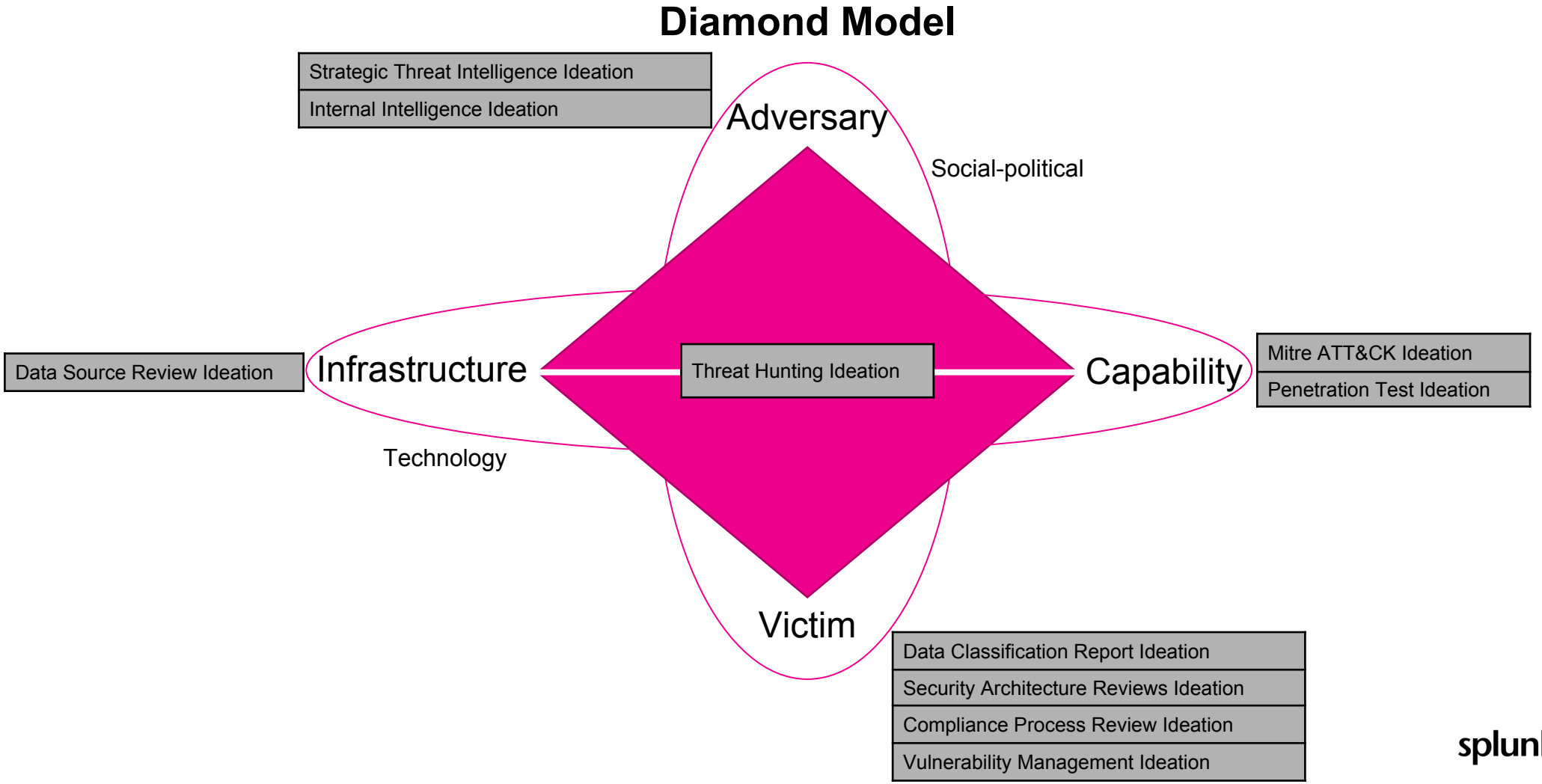
Modular automation – Identify specific sub-processes that are good candidates for automation (i.e. lock use account, gather information on IP address, etc.), and develop reusable modular automation scripts that can be called across your orchestrated processes

Close the loop between operations and engineering –

- Your engineering team can onboard new data, integrate with system to contextually enrich your response and/or automate response actions, but their efforts need to be prioritized on the needs of your operations team
- Recommendation: Update your post incident reports to include process improvement ideas (i.e. what data sources would have been helpful, what additional data were needed to provide context to make decisions, etc.)

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.



.conf19

splunk>

Thank You !

Go to the .conf19 mobile app to

RATE THIS SESSION