Splunk .conf18
Connecting the Dots

From Problem Statement to Response Understanding Event Flow Through Security Operations

Brandie Anderson, PhD

May 2018 | Version 1.0

Forward-Looking Statements

During the course of this presentation, we may make forward-looking statements regarding future events or the expected performance 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 could differ materially. For important factors that may cause actual results to differ from those contained in our forward-looking statements, please review our filings with the SEC.

The forward-looking statements made in this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward-looking statements we may make. 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 functionality described or to include any such feature or functionality in a future release.

splunk> .conf18

BRANDIE ANDERSON, PHD

Professional Services Global Security Practice Lead

@ba2trinity

splunk> .conf18

Agenda

01. What is a Use Case

02. Log Sources

03. Operational Flow

04. Key Takeaways

splunk> .conf18

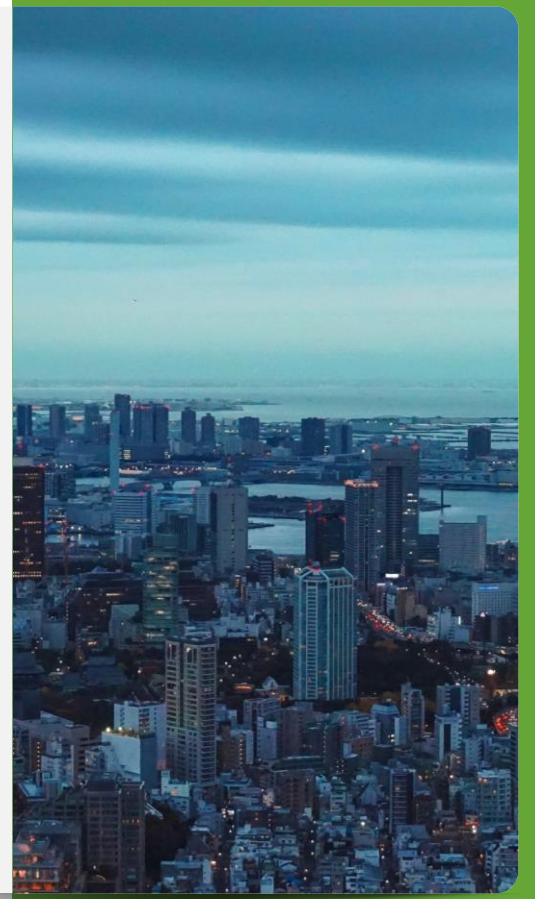
What is a Use Case

What is a Use Case?

Wikipedia: A list of steps, typically defining actions between a role and a system, to achieve a goal.

Splunk: Any search created to solve a specific problem.

- Use cases should address a business purpose
- Use cases should help the user address those purposes



When is a Use Case NOT a Use Case?

Traditional SIEM:

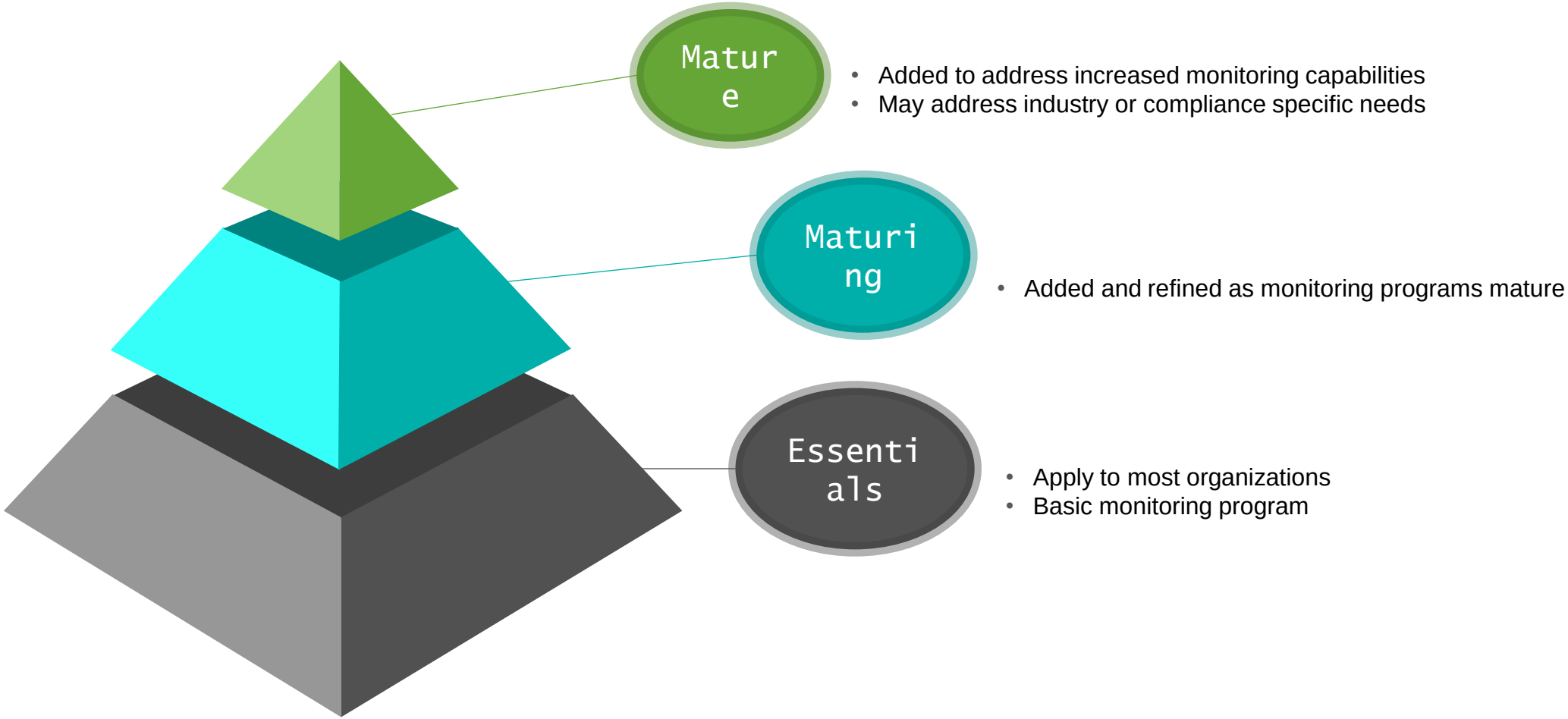
- *TOR exit node activity inbound*
- *TOR exit node suspicious activity allowed*
- *Internal host communication with Lojack C2 Domains*

- *Alert when 5+ failed login attempts are seen in 15 minutes on DB server*
- *Alert when unauthorized Drop All Roles action is seen*
- *Alert when unauthorized Drop All Users action is seen*

Splunk Version:

- *Threat Activity Detected – Alerts when any activity matching threat intelligence is detected*
- *Brute Force Access Behavior – Detects excessive number of failed logins along with a successful attempt*

Professional Services Use Case Categorization



- Added to address increased monitoring capabilities
- May address industry or compliance specific needs

- Added and refined as monitoring programs mature

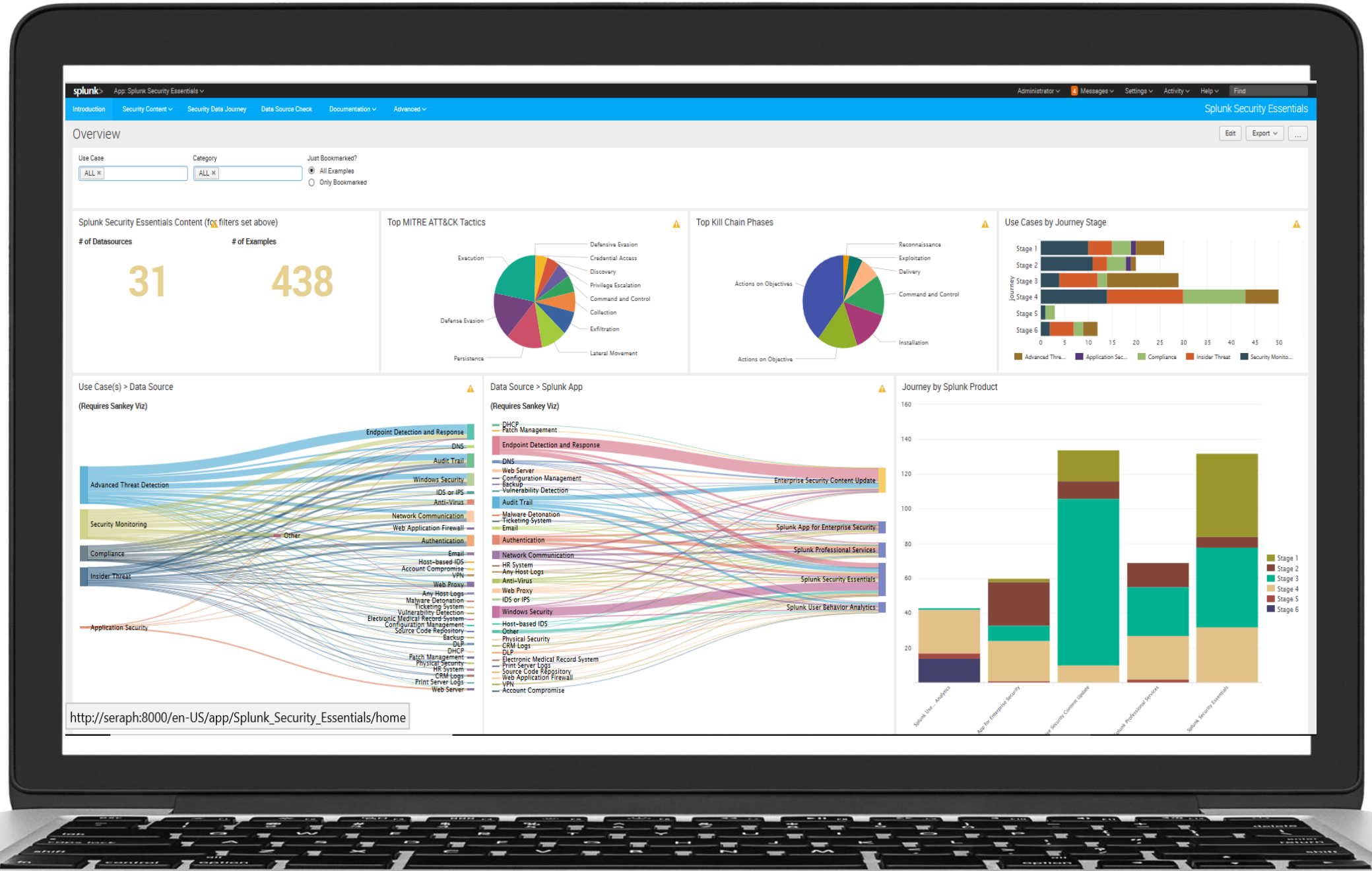
- Apply to most organizations
- Basic monitoring program

VPN Monitoring Example Use Case

- What is the problem we are trying to solve?
  - Violations by remote users
- What are some interesting items we might care about?
  - X# of failed logins on VIP account
  - Failed/Successful logins from geographically infeasible locations
  - X# of disabled accounts in Y time period

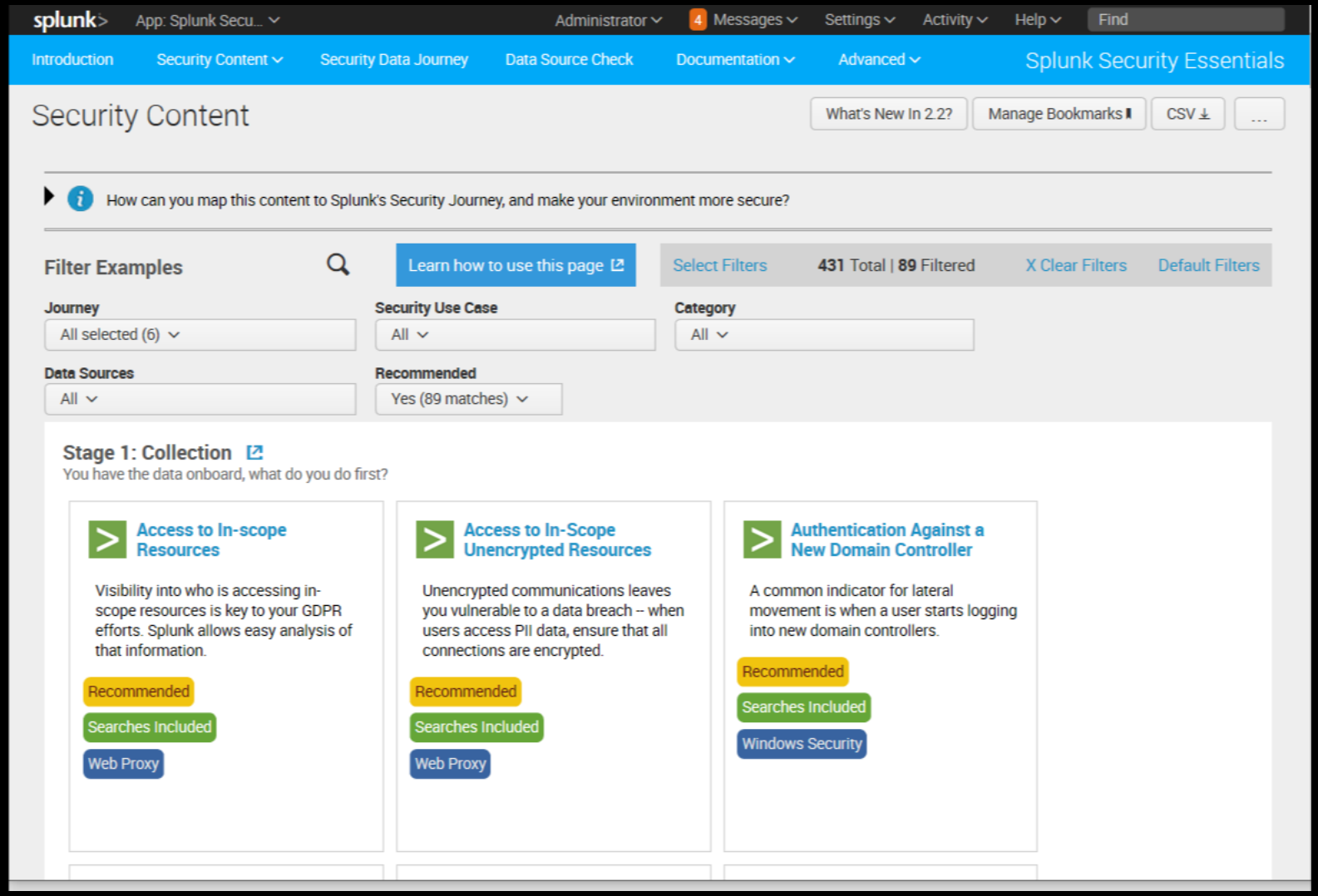
Example Use Case – User Behavior Monitoring

- What is the problem we are trying to solve?
  - Detection of malicious or compromised user activity
- What are some interesting items we might care about?
  - Manual login to a NHA
  - Account groups or roles changed
  - Actions performed by a user of group Y are anomalous to typical group Y users



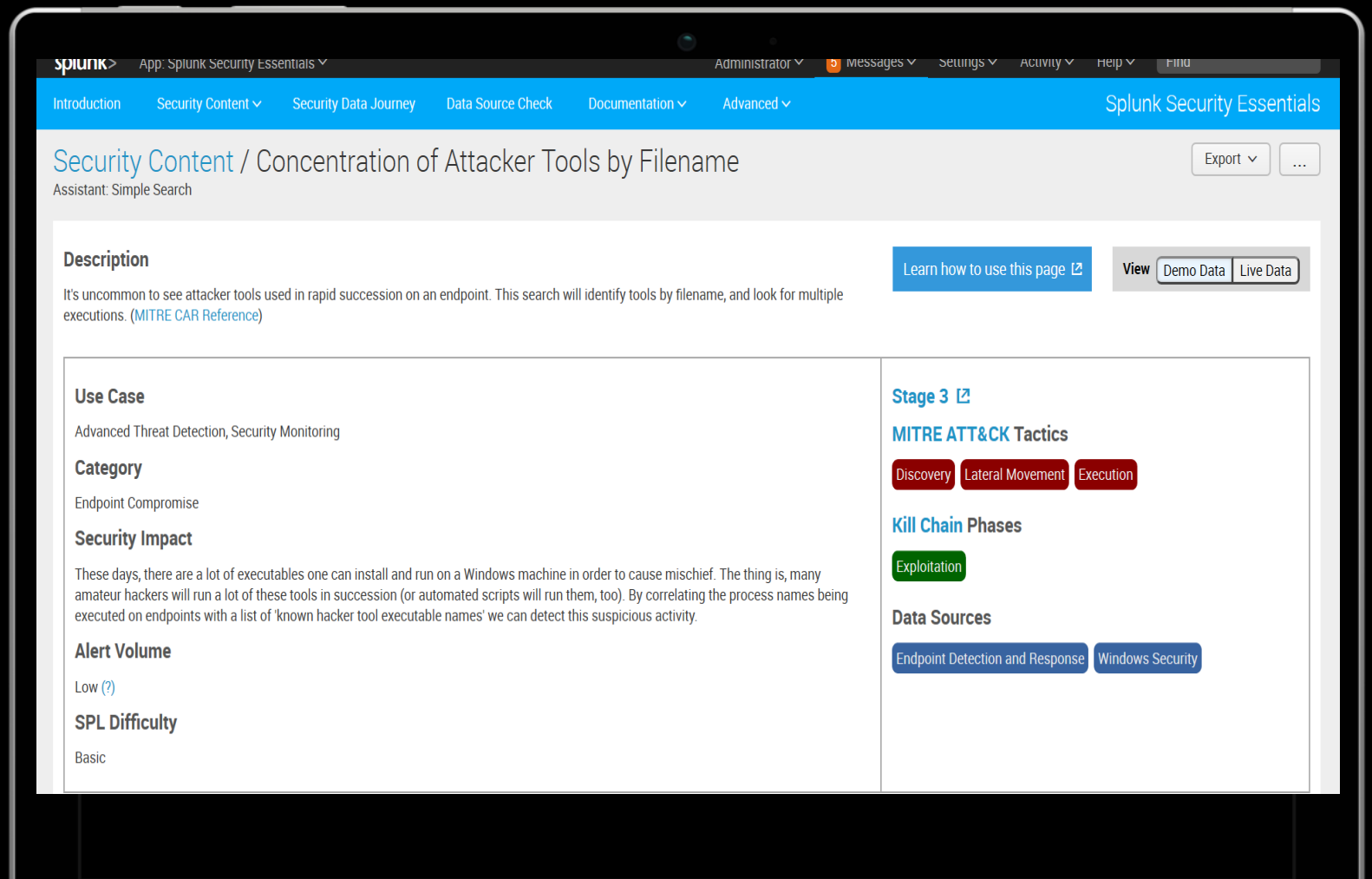
Security Essentials

Security Content Tab



Security Essentials Use Case Example

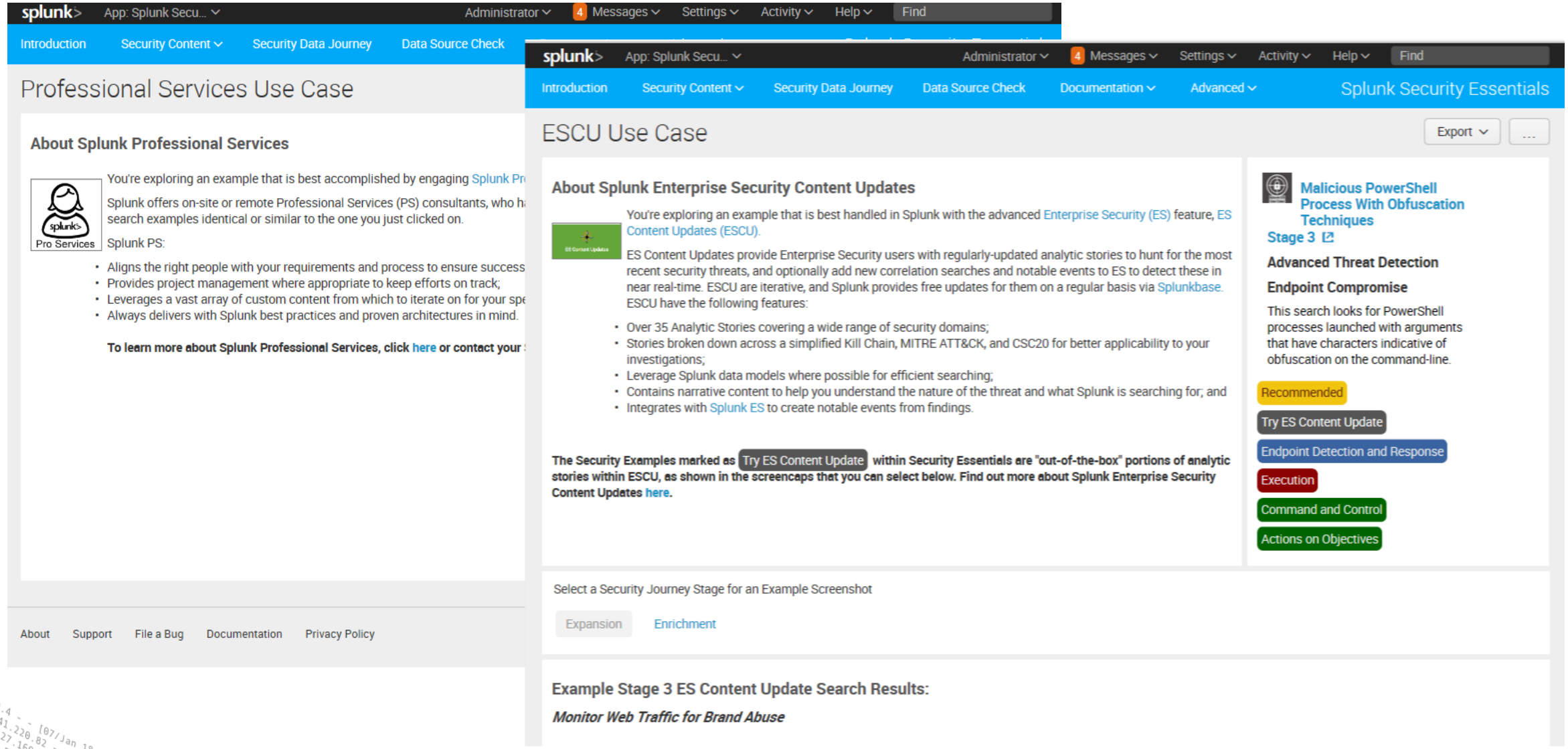
Concentration of Attacker Tools by Filename



- Name
- Description
- Use Case Type
- Category
- Security Impact
- Alert Volume
- SPL Difficulty
- MITRE ATT&CK
- Kill Chain
- Data Sources

splunk> .conf18

Use Case Examples



splunk> .conf18

Use Case Template

Documentation is like sex: when it is good it is very, very good, when it is bad, it is still better than nothing. – Dick Brandon

Use Case Template

Version x

Name: (Add a number if desired)

Description: (Who, What, Why) <1-2 sentences explaining the business purpose>

Use Case Type: <Advanced Threat Detection, Security Monitoring >

Security Impact: <Describe potential impact directing Use Case creation>

Attack Information: <MITRE ATT&CK, Kill Chain, Internal Scale>

Data Sources: <What data sources are necessary for detection>

Search Logic: <Pseudo code of what the Use Case is searching>

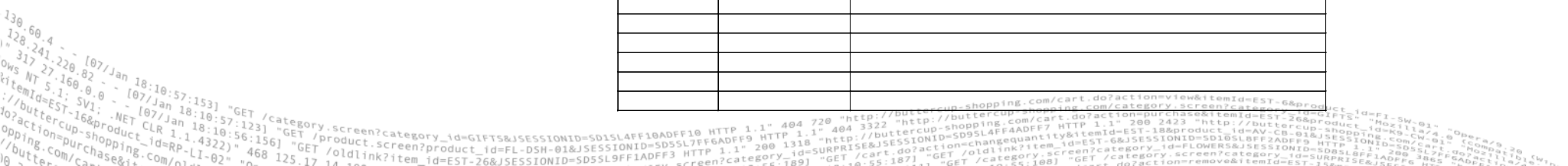
False Positives: <List of items which cause a Use Case to be less accurate>

Workflow: <What must happen once the event triggers>
<Extended information: Describe initial Triage, users involved, who to notify, escalation path, validation methods, resolution requirements, etc.>

References: <Any additional details regarding the validity or reason for this Use Case creation>

Revision History

Date	Author	Description of change



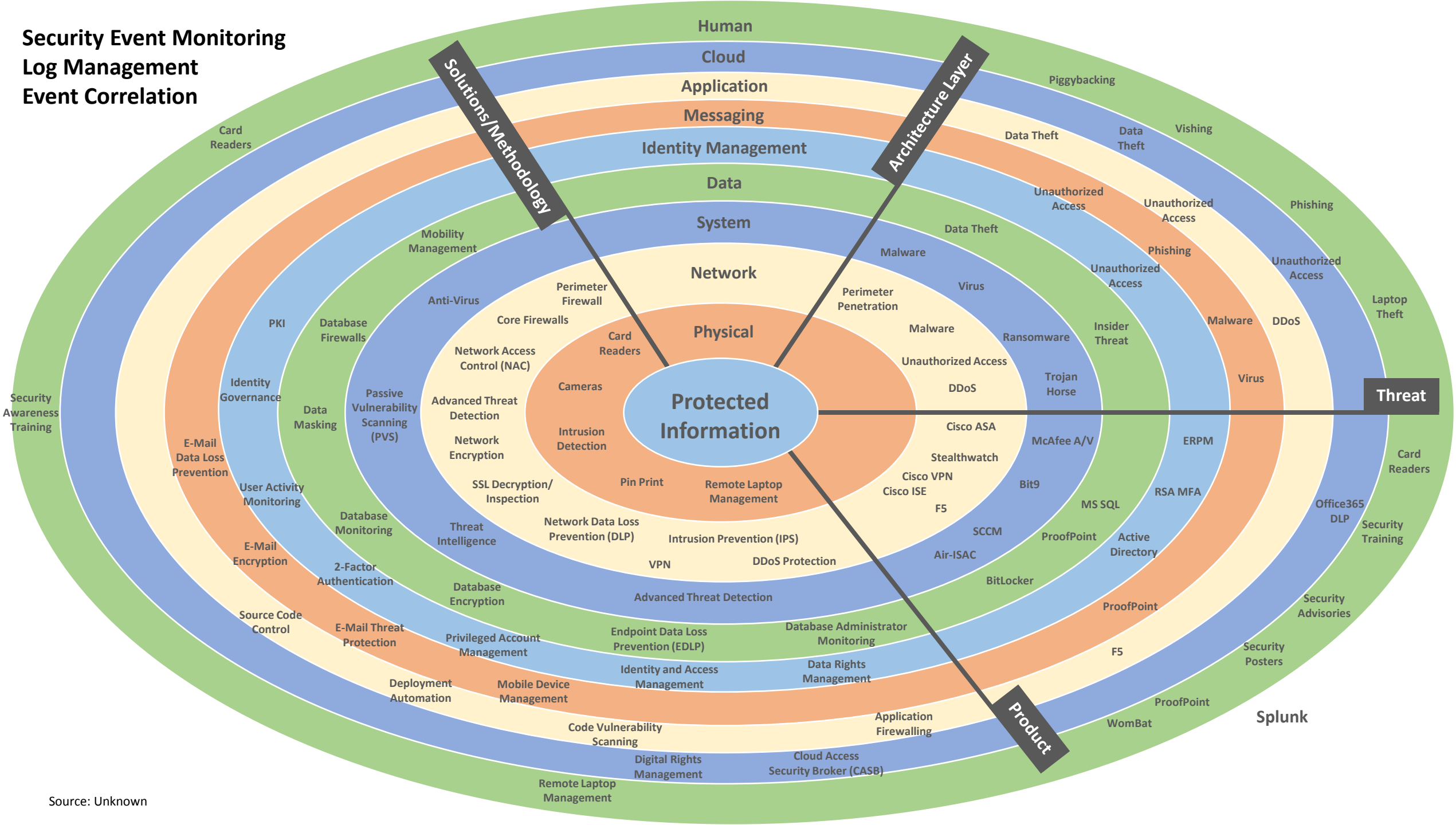
splunk> .conf18

Log Sources

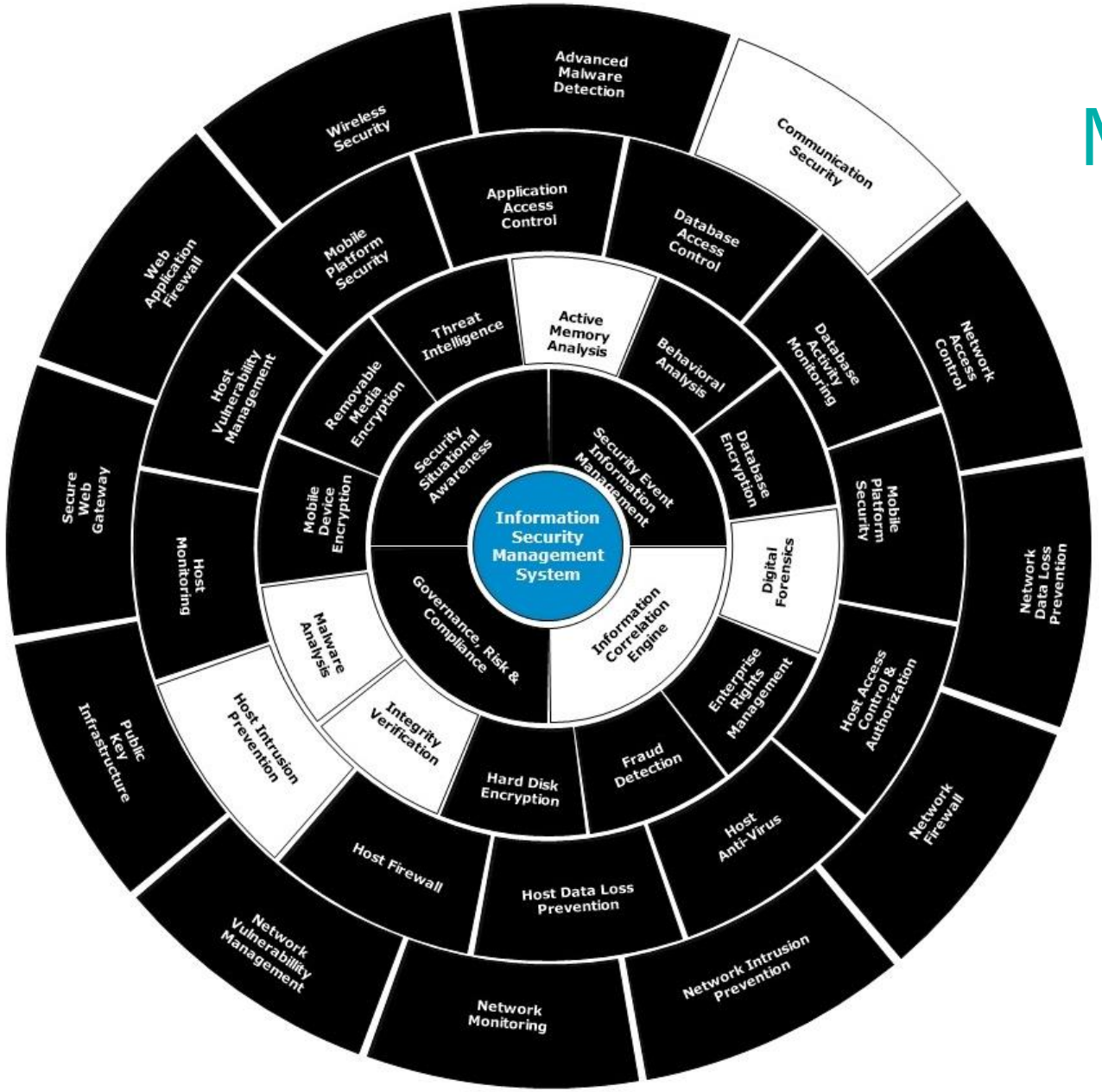
Relevant Data

splunk> .conf18

Security Event Monitoring
Log Management
Event Correlation



Source: Unknown



Information Security Management System

- Document Capability
- Target view of gaps

Vendor	Source	Description	Notes
Microsoft	Cloud App Security		
	Sysmon/Security		
	AD Authentication		
Cisco			

Source: Sphericube

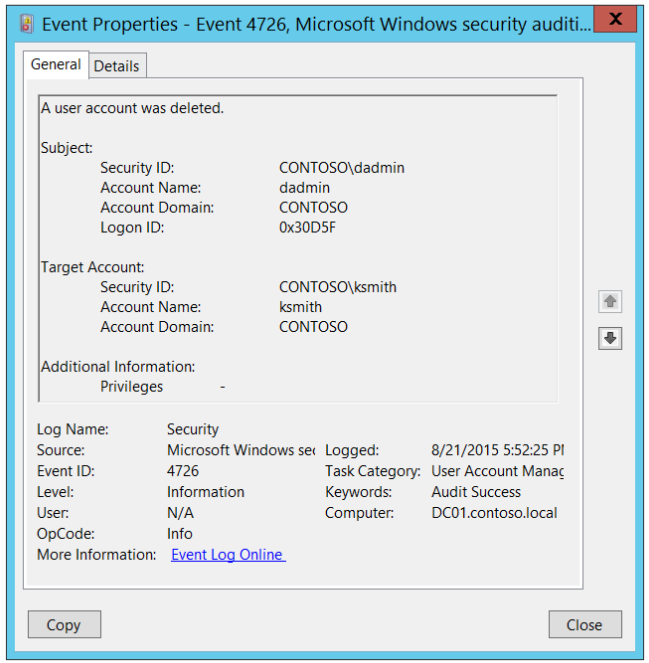
Degree of Effectiveness	
0	None
1	Deficient
2	Lacking
3	Inadequate
4	Adequate
5	Effective

Degree of Maturity	
0	None
1	Initial
2	Repeatable
3	Defined
4	Managed
5	Optimized

Degree of Coverage	
0	None
1	Minimal
2	Partial
3	Essential
4	Complete
5	Redundant

Data Source Review – Microsoft Windows

4726(S): A user account was deleted.



Event Description:

This event generates every time user object was deleted.

This event generates on domain controllers, member servers, and workstations.

Note For recommendations, see Security Monitoring Recommendations for this event.

Event XML:

```
- <Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event">
- <System>
  <Provider Name="Microsoft-Windows-Security-Auditing" Guid="{54849625-5478-4994-A5BA-3E3B0328C30D}" />
  <EventID>4726</EventID>
  <Version>0</Version>
  <Level>0</Level>
  <Task>13824</Task>
  <Opcode>0</Opcode>
  <Keywords>0x8020000000000000</Keywords>
  <TimeCreated SystemTime="2015-08-22T00:52:25.104613800Z" />
  <EventRecordID>175720</EventRecordID>
  <Correlation />
  <Execution ProcessID="520" ThreadID="1112" />
  <Channel>Security</Channel>
  <Computer>DC01.contoso.local</Computer>
  <Security />
  </System>
- <EventData>
  <Data Name="TargetUserName">ksmith</Data>
  <Data Name="TargetDomainName">CONTOSO</Data>
  <Data Name="TargetSid">S-1-5-21-3457937927-2839227994-823803824-6609</Data>
  <Data Name="SubjectUserSid">S-1-5-21-3457937927-2839227994-823803824-1104</Data>
  <Data Name="SubjectUserName">dadmin</Data>
  <Data Name="SubjectDomainName">CONTOSO</Data>
  <Data Name="SubjectLogonId">0x30d5f</Data>
```

Security Monitoring Recommendations:

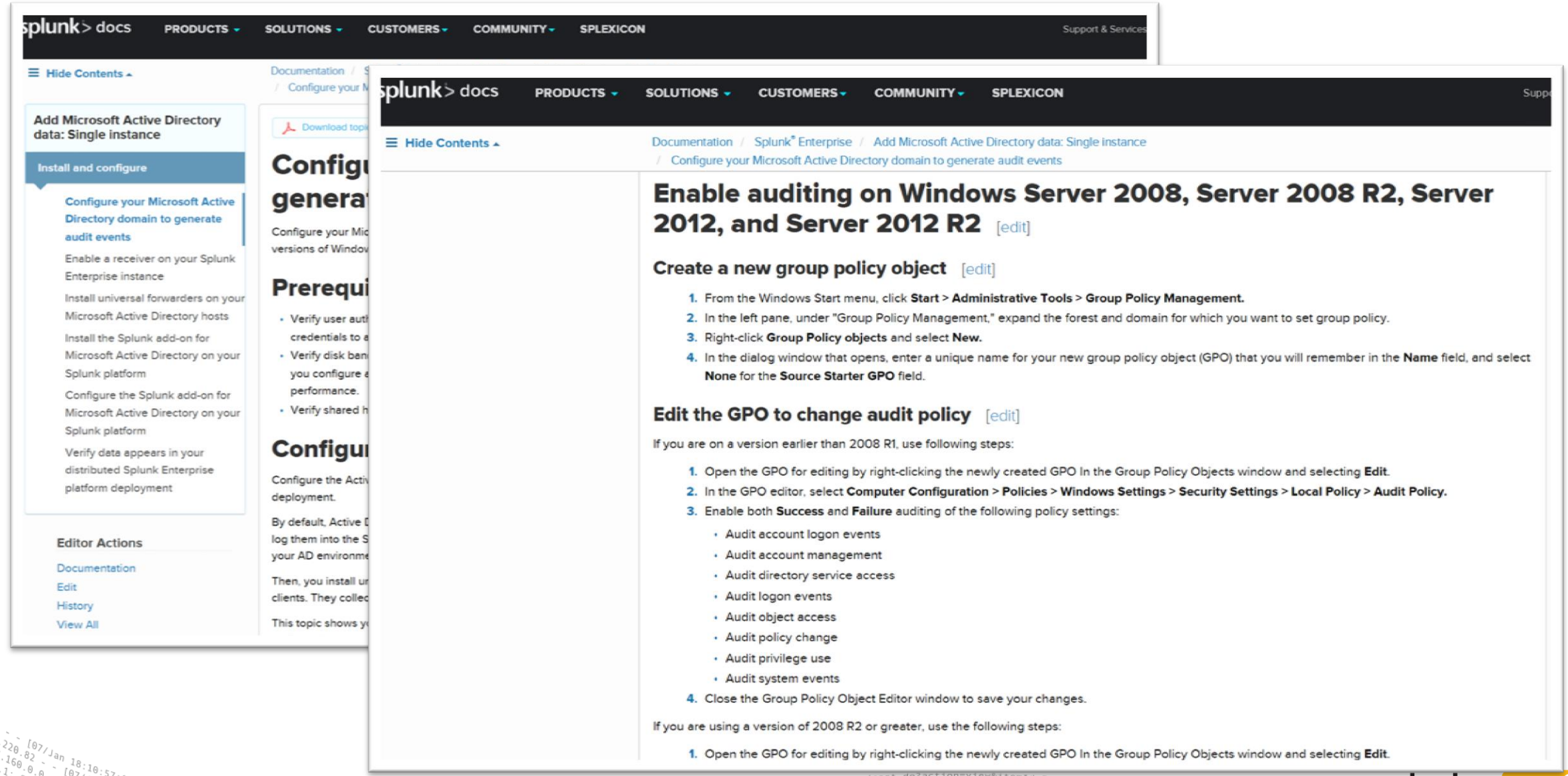
For 4726(S): A user account was deleted.

Important For this event, also see Appendix A: Security monitoring recommendations for many audit events.

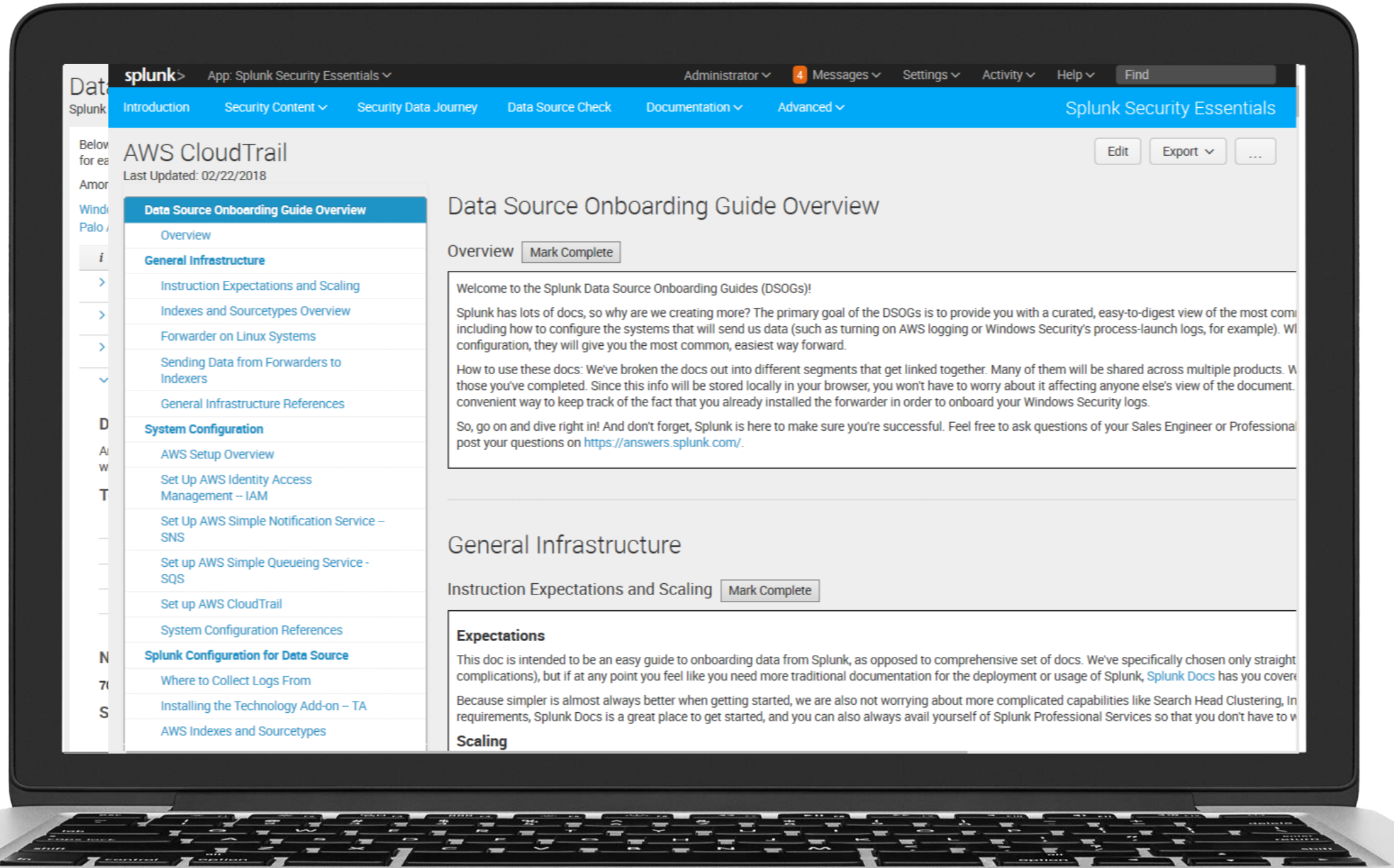
- If you have a high-value domain or local account for which you need to monitor every change (or deletion), monitor all 4726 events with the **"Target Account\Security ID"** that corresponds to the account.
- If you have a domain or local account that should never be deleted (for example, service accounts), monitor all 4726 events with the **"Target Account\Security ID"** that corresponds to the account.
- We recommend monitoring all 4726 events for local accounts, because these accounts typically are not deleted often. This is especially relevant for critical servers, administrative workstations, and other high value assets.

- https://www.Microsoft.com/en-us/download/details.aspx?id=52630

New Documentation Assistance



splunk> .conf18



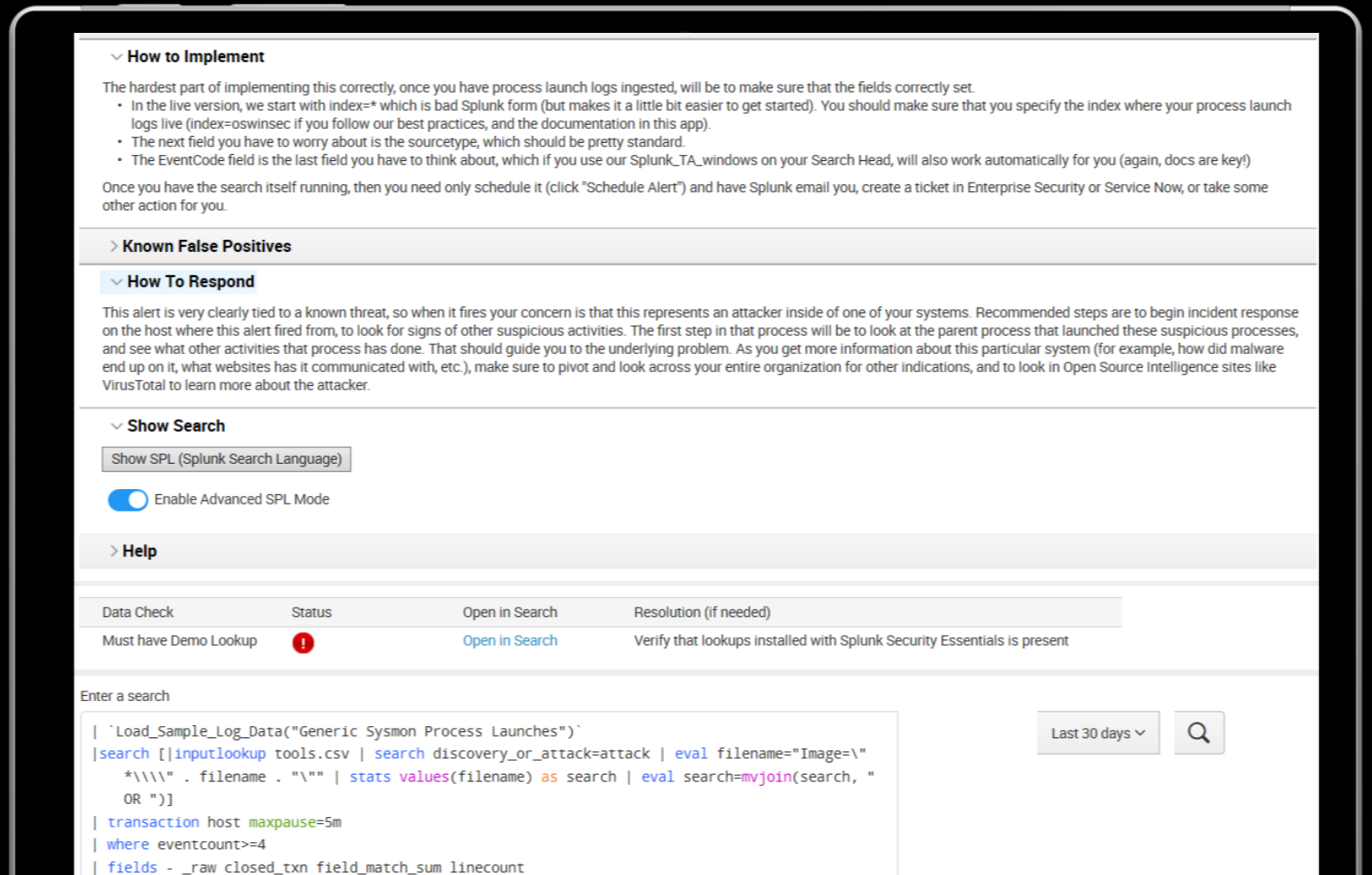
Operational Flow

Defining Processes

Source: memegen.com

Use Case Details

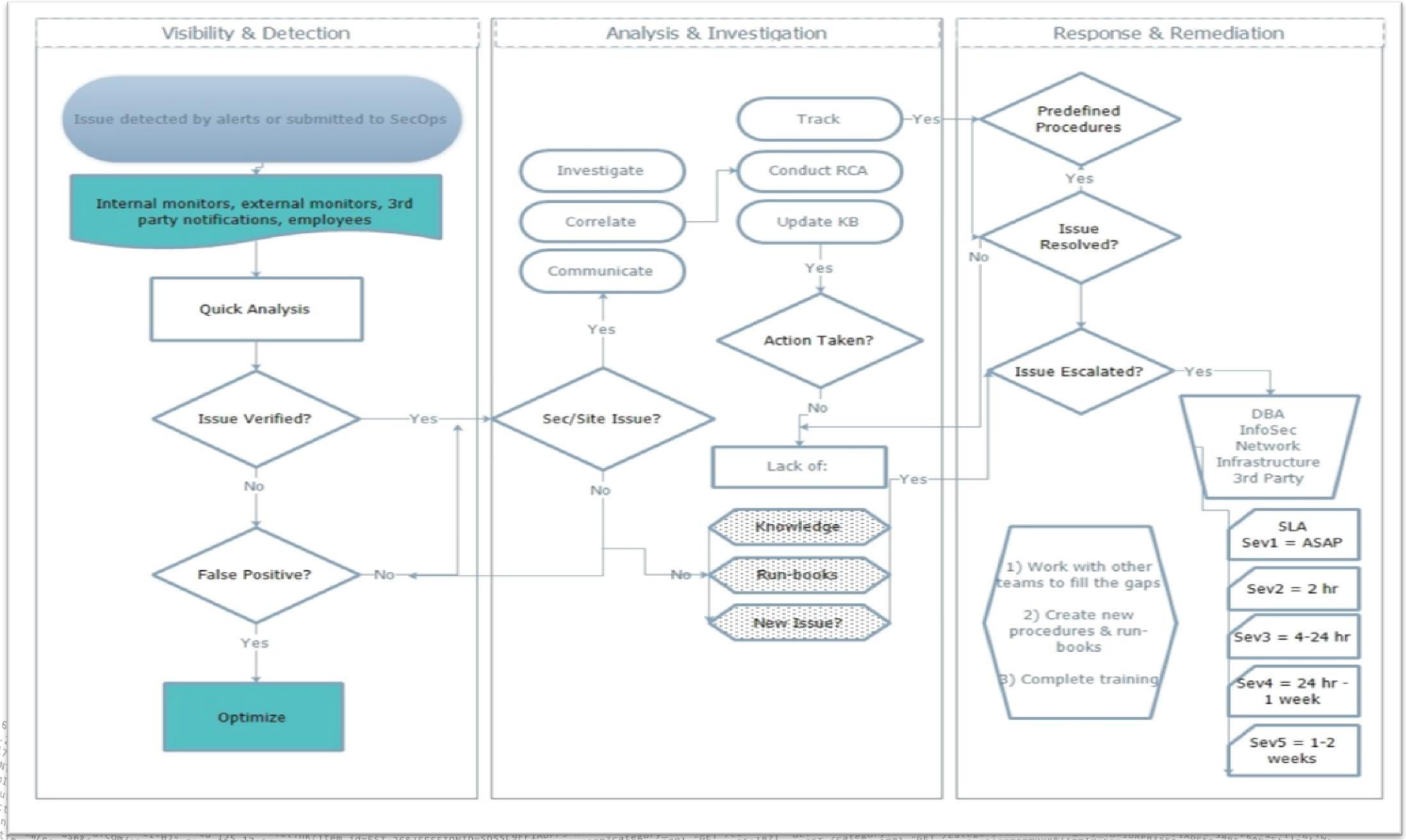
Concentration of Attacker Tools by Filename



- How to Implement
- Known False Positives
- How to Respond
- Show Search
- SPL

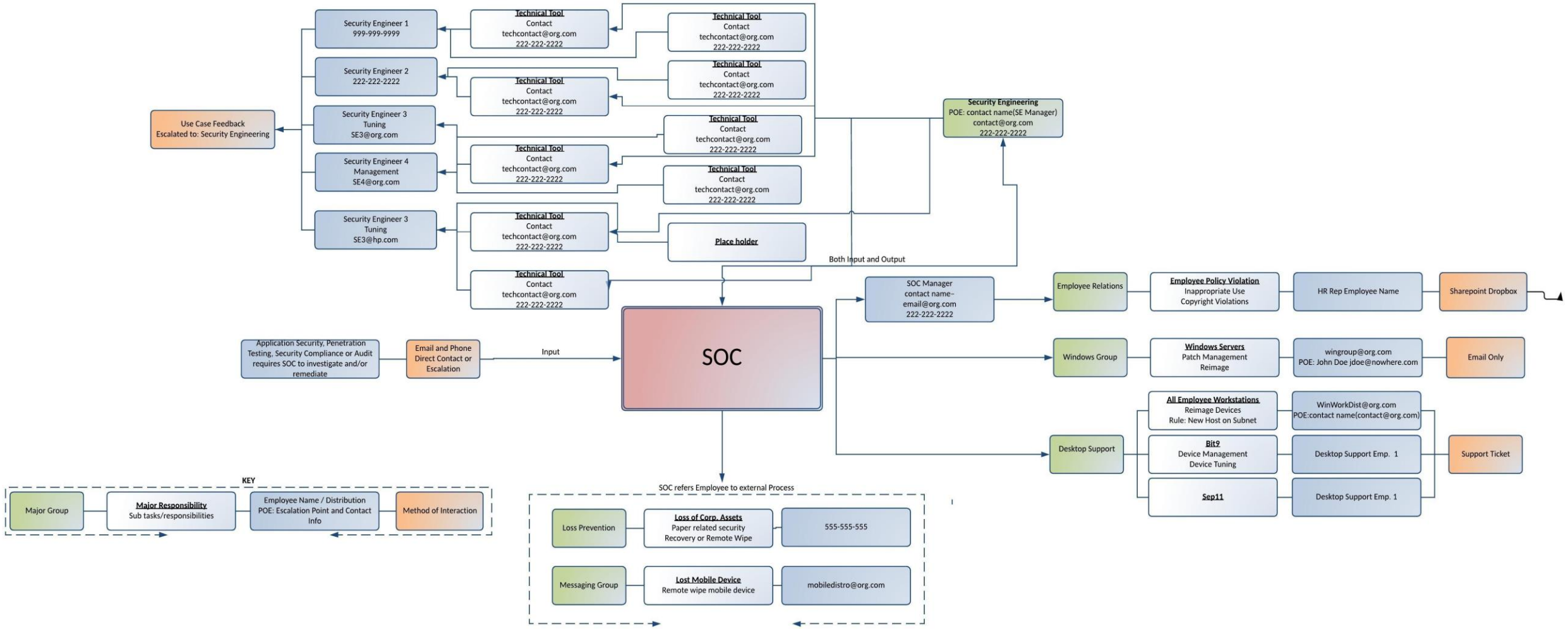
splunk> .conf18

Simple Event Management Operational Flow



splunk> .conf18

Operational Inputs/Outputs Example



splunk> .conf18

Example Use Case – VPN Monitoring

- Violations by VPN remote users
  - Use Case Type: Security Monitoring, Compliance
  - Data Sources: VPN, Authentication
- Use Cases with Actions
  - Notable created when X# of failed logins on VIP account detected. Action directs auto-ticketing through ServiceNow connectivity for User Support to contact VIP regarding activity. Start an investigation, review logs during the timeframe in question, if appears suspicious escalate.
  - Notable created after two successful logins from geographically infeasible locations.
    - Smaller organization: Action directs auto-ticketing to disable the user account pending Analyst triage of event circumstances.
    - Larger organization: Analyst triage and decides wither to open a ticket for contact or disable the user account.
  - Notable created when X# of disabled accounts in Y time period. Analyst triage to determine if it is a larger attack.

Example Use Case – User Behavior Monitoring

- Detection of malicious or compromised user activity
  - Use Case Type: Security Monitoring, Insider Threat
  - Data Sources: ALL
- Use Cases with Actions
  - Notable created from manual login to a NHA.
    - Smaller organization: Analyst triage to determine if this was legitimate use.
    - Larger organization: Action auto-creates a ticket to the admin team of the asset.
  - Account groups or roles changed
  - Actions performed by a user of group Y are anomalous to typical group Y users

Key Takeaways

1. Use Cases should solve *your* business issues
2. Take inventory of your data, document what you have, understand what the data means
3. A complete Use Case identifies the operational actions required once an alert is created

splunk>

Thank You

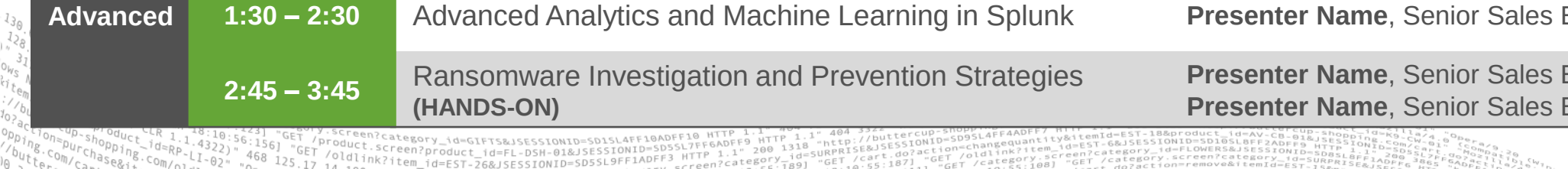
Don't forget to rate this session in the .conf18 mobile app

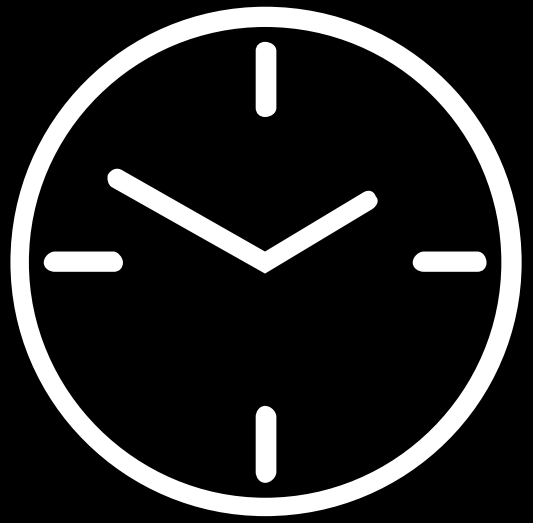
Join the Pony Poll

ponypoll.com/***

Tracks and Sessions

New to Splunk	**11:15 – 12:15**	Splunk Overview	**Presenter Name**, Senior Sales Engineer, Splunk **Presenter Name**, Senior Sales Engineer, Splunk
	1:30 – 2:30	Getting Started with Splunk Enterprise **(HANDS-ON)**	**Presenter Name**, Senior Sales Engineer, Splunk **Presenter Name**, Senior Sales Engineer, Splunk
	2:45 – 3:45	Data Onboarding	**Presenter Name**, Senior Sales Engineer, Splunk
IT Ops	**11:15 – 12:15**	Happy Apps, Happy Users: Using Splunk APM	**Presenter Name**, Senior Sales Engineer, Splunk **Presenter Name**, Senior Sales Engineer, Splunk
	1:30 – 2:30	Splunk Enterprise for IT Troubleshooting **(HANDS-ON)**	**Presenter Name**, Senior Sales Engineer, Splunk
	2:45 – 3:45	How to Design, Build and Map IT and Business Services in Splunk	**Presenter Name**, Senior Sales Engineer, Splunk **Presenter Name**, Senior Sales Engineer, Splunk
Security	**11:15 – 12:15**	Build a Security Portfolio That Strengthens Your Security Posture	**Presenter Name**, Senior Sales Engineer, Splunk **Presenter Name**, Senior Sales Engineer, Splunk
	1:30 – 2:30	Building an Analytics Driven Security Operation Center using Splunk Enterprise Security	**Presenter Name**, Senior Sales Engineer, Splunk **Presenter Name**, Senior Sales Engineer, Splunk
	2:45 – 3:45	An End-To-End Approach: Detect via Behavior and Orchestrate via SIEM	**Presenter Name**, Senior Sales Engineer, Splunk **Presenter Name**, Senior Sales Engineer, Splunk
Advanced	**11:15 – 12:15**	The Power of SPL	**Presenter Name**, Senior Sales Engineer, Splunk
	1:30 – 2:30	Advanced Analytics and Machine Learning in Splunk	**Presenter Name**, Senior Sales Engineer, Splunk
	2:45 – 3:45	Ransomware Investigation and Prevention Strategies **(HANDS-ON)**	**Presenter Name**, Senior Sales Engineer, Splunk **Presenter Name**, Senior Sales Engineer, Splunk





BREAK

15 MINUTES