



splunk>

# 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, Splunk>, Listen to Your Data, The Engine for Machine Data, Splunk Cloud, Splunk Light and SPL are trademarks and registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names, or trademarks belong to their respective owners. © 2018 Splunk Inc. All rights reserved.

# 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

# 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:

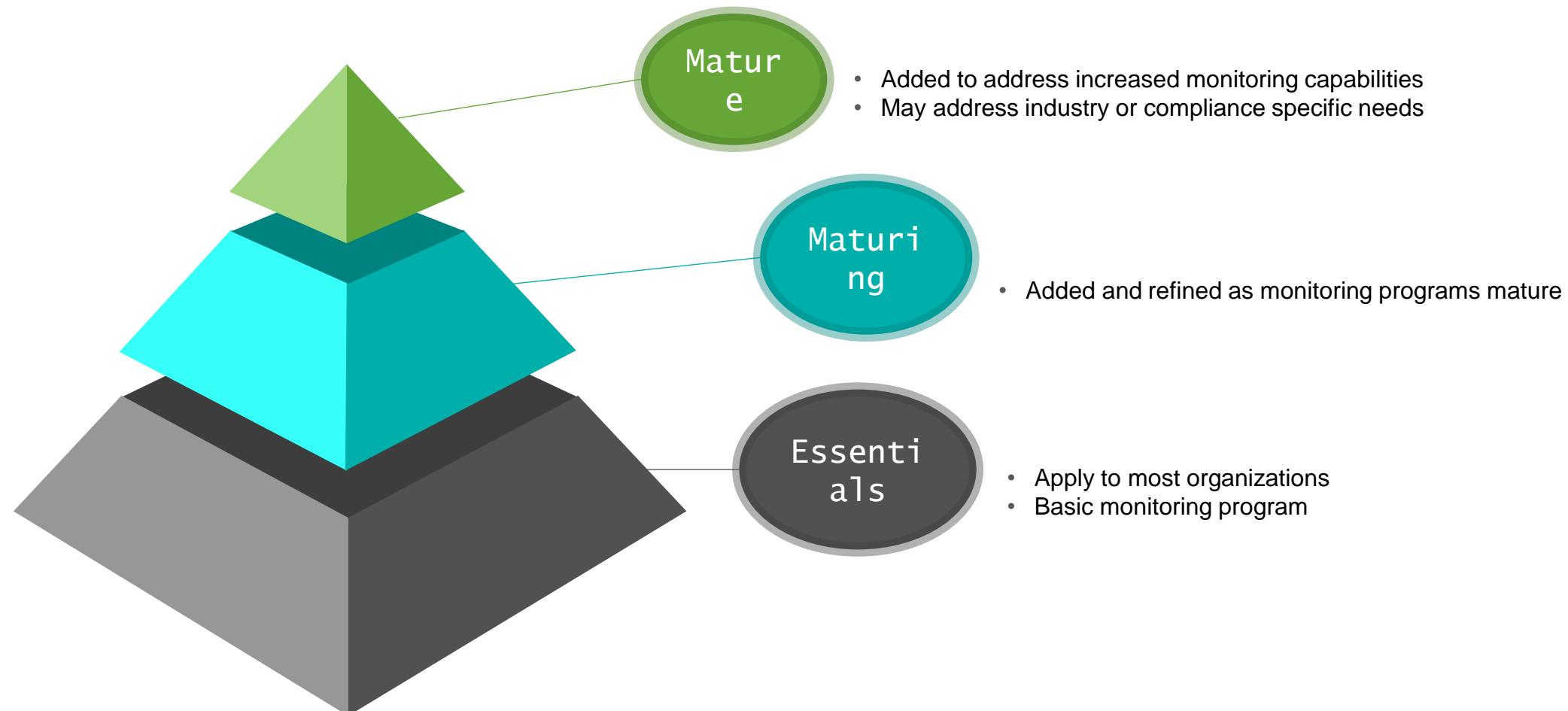
- *TOR exit node activity inbound*
  - *TOR exit node suspicious activity allowed*
  - *Internal host communication with Lojack C2 Domains*

- 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

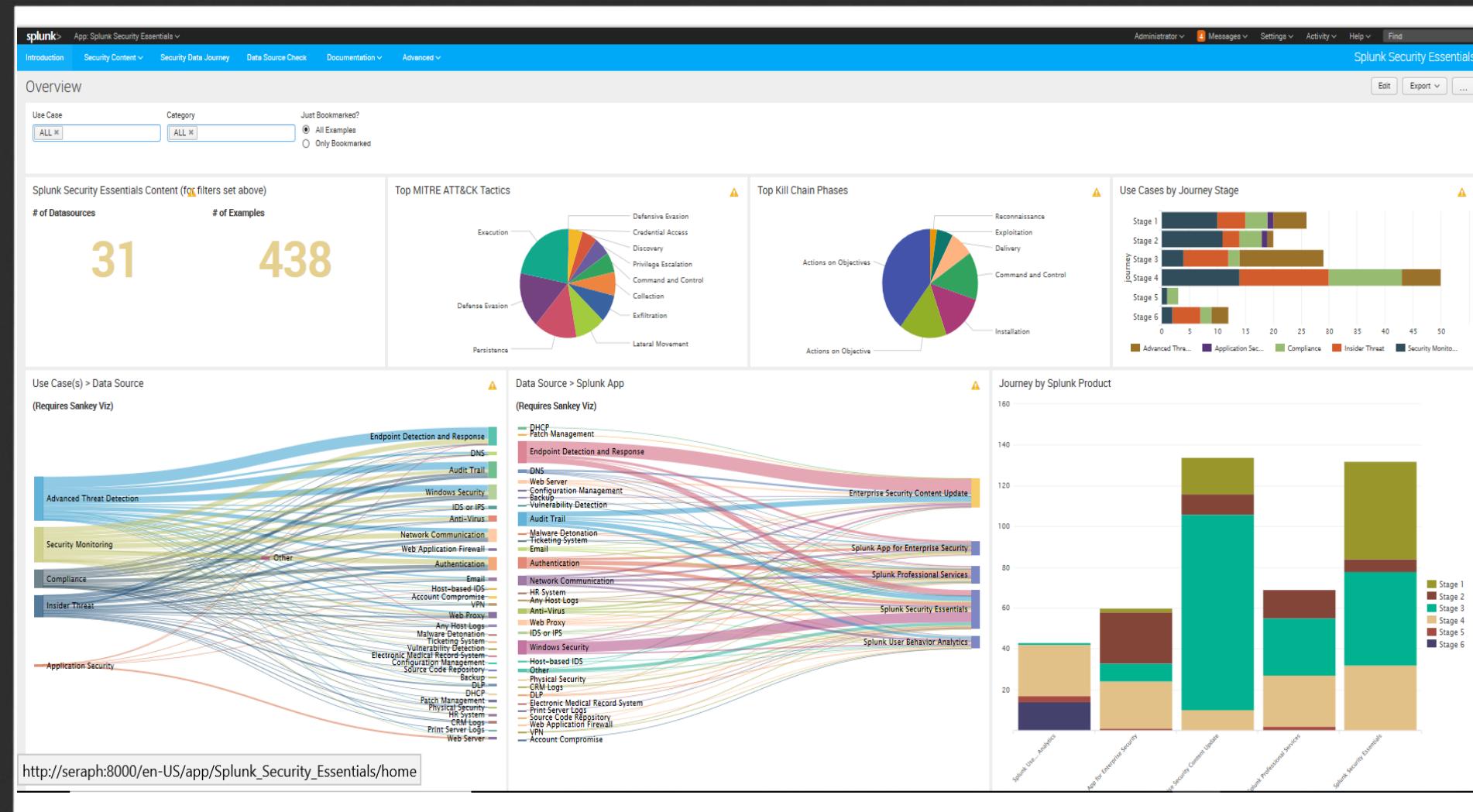


# VPN Monitoring Example Use Case

- ▶ 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

splunk > App: Splunk Secu... ▾ Administrator ▾ 4 Messages ▾ Settings ▾ Activity ▾ Help ▾ Find

Introduction Security Content ▾ Security Data Journey Data Source Check Documentation ▾ Advanced ▾ Splunk Security Essentials

Security Content

▶ ⓘ How can you map this content to Splunk's Security Journey, and make your environment more secure?

Filter Examples  Learn how to use this page ▾ Select Filters 431 Total | 89 Filtered X Clear Filters Default Filters

Journey All selected (6) ▾ Security Use Case All ▾ Category All ▾

Data Sources All ▾ Recommended Yes (89 matches) ▾

Stage 1: Collection ▾ You have the data onboard, what do you do first?

> Access to In-scope Resources  
Visibility into who is accessing in-scope resources is key to your GDPR efforts. Splunk allows easy analysis of that information.  
  
Recommended  
Searches Included  
Web Proxy

> Access to In-Scope Unencrypted Resources  
Unencrypted communications leaves you vulnerable to a data breach – when users access PII data, ensure that all connections are encrypted.  
  
Recommended  
Searches Included  
Web Proxy

> Authentication Against a New Domain Controller  
A common indicator for lateral movement is when a user starts logging into new domain controllers.  
  
Recommended  
Searches Included  
Windows Security

# Security Essentials Use Case Example

## Concentration of Attacker Tools by Filename

The screenshot shows the Splunk Security Essentials interface. At the top, there's a navigation bar with links for Introduction, Security Content, Security Data Journey, Data Source Check, Documentation, Advanced, and a search bar labeled "Splunk Security Essentials". Below the navigation is a main content area titled "Security Content / Concentration of Attacker Tools by Filename". It includes a "Description" section with a note about identifying multiple executions of attacker tools and a link to the MITRE CAR Reference. To the right of the description are buttons for "Learn how to use this page", "View Demo Data", and "Live Data". The main content area also contains sections for "Use Case", "Category", "Security Impact", "Alert Volume", "SPL Difficulty", "MITRE ATT&CK", "Kill Chain Phases", and "Data Sources".

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

# Use Case Examples

**splunk>** App: Splunk Secu... ▾ Administrator ▾ 4 Messages ▾ Settings ▾ Activity ▾ Help ▾ Find

Introduction Security Content ▾ Security Data Journey Data Source Check

## Professional Services Use Case

### About Splunk Professional Services

You're exploring an example that is best accomplished by engaging [Splunk Professional Services](#). Splunk offers on-site or remote Professional Services (PS) consultants, who help you search examples identical or similar to the one you just clicked on.

 **Splunk PS:**

- Aligns the right people with your requirements and process to ensure success
- Provides project management where appropriate to keep efforts on track;
- Leverages a vast array of custom content from which to iterate on for your specific needs;
- Always delivers with Splunk best practices and proven architectures in mind.

To learn more about Splunk Professional Services, click [here](#) or contact your account manager.

### ESCU Use Case

#### About Splunk Enterprise Security Content Updates

You're exploring an example that is best handled in Splunk with the advanced [Enterprise Security \(ES\)](#) feature, [ES Content Updates \(ESCU\)](#).

 ES Content Updates provide Enterprise Security users with regularly-updated analytic stories to hunt for the most recent security threats, and optionally add new correlation searches and notable events to ES to detect these in near real-time. ESCU are iterative, and Splunk provides free updates for them on a regular basis via [Splunkbase](#). ESCU have the following features:

- Over 35 Analytic Stories covering a wide range of security domains;
- Stories broken down across a simplified Kill Chain, MITRE ATT&CK, and CSC20 for better applicability to your investigations;
- Leverage Splunk data models where possible for efficient searching;
- Contains narrative content to help you understand the nature of the threat and what Splunk is searching for; and
- Integrates with [Splunk ES](#) to create notable events from findings.

The Security Examples marked as [Try ES Content Update](#) within Security Essentials are "out-of-the-box" portions of analytic stories within ESCU, as shown in the screencaps that you can select below. Find out more about Splunk Enterprise Security Content Updates [here](#).

Select a Security Journey Stage for an Example Screenshot

Expansion Enrichment

#### Example Stage 3 ES Content Update Search Results:

*Monitor Web Traffic for Brand Abuse*

 **Malicious PowerShell Process With Obfuscation Techniques**

**Stage 3 ↗**

**Advanced Threat Detection**

**Endpoint Compromise**

This search looks for PowerShell processes launched with arguments that have characters indicative of obfuscation on the command-line.

**Recommended**

[Try ES Content Update](#)

[Endpoint Detection and Response](#)

[Execution](#)

[Command and Control](#)

[Actions on Objectives](#)

# 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 User Score to be less than 0.

**What is the relationship between the two sets?**

<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

# Log Sources

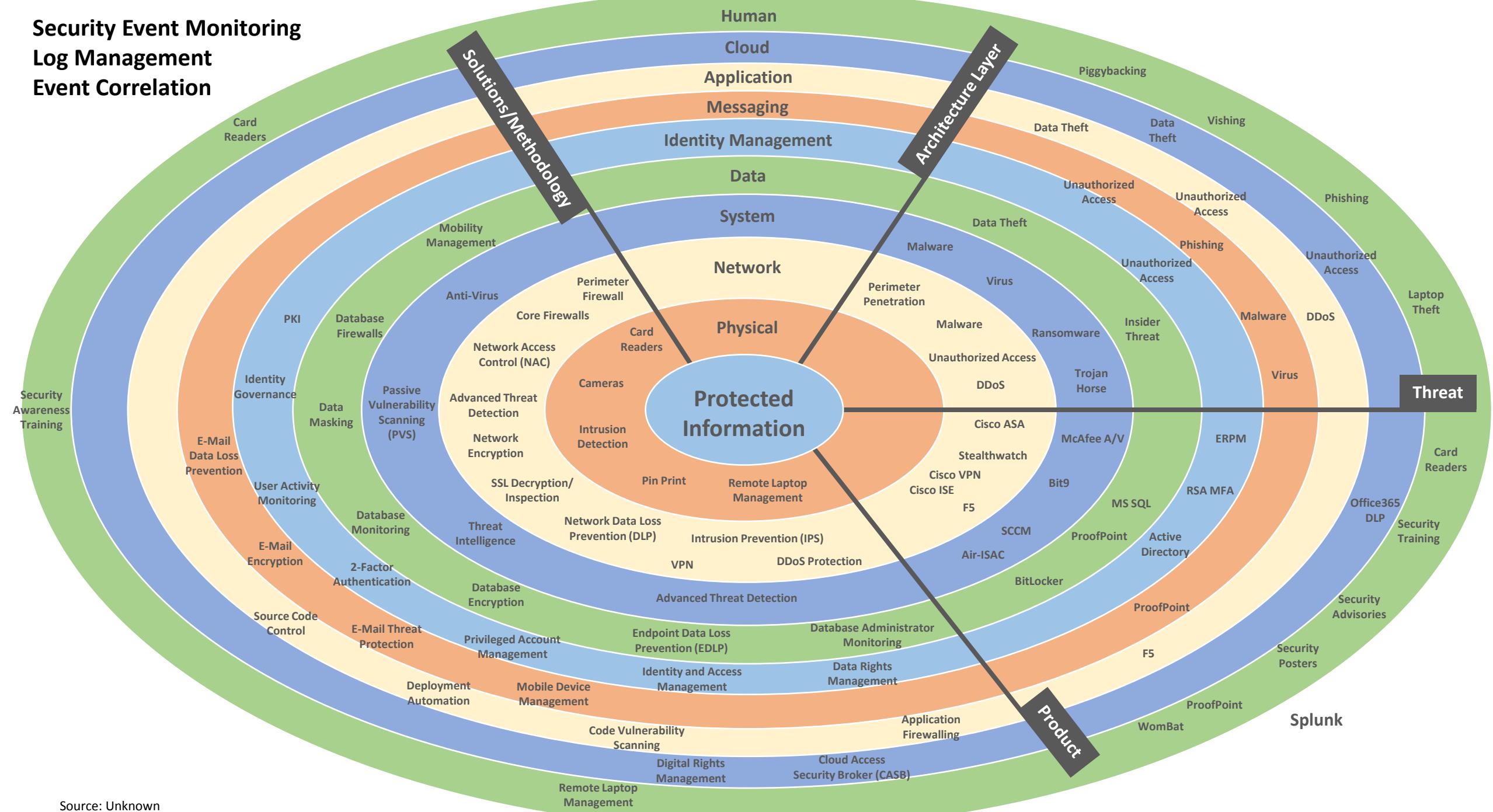
Relevant Data



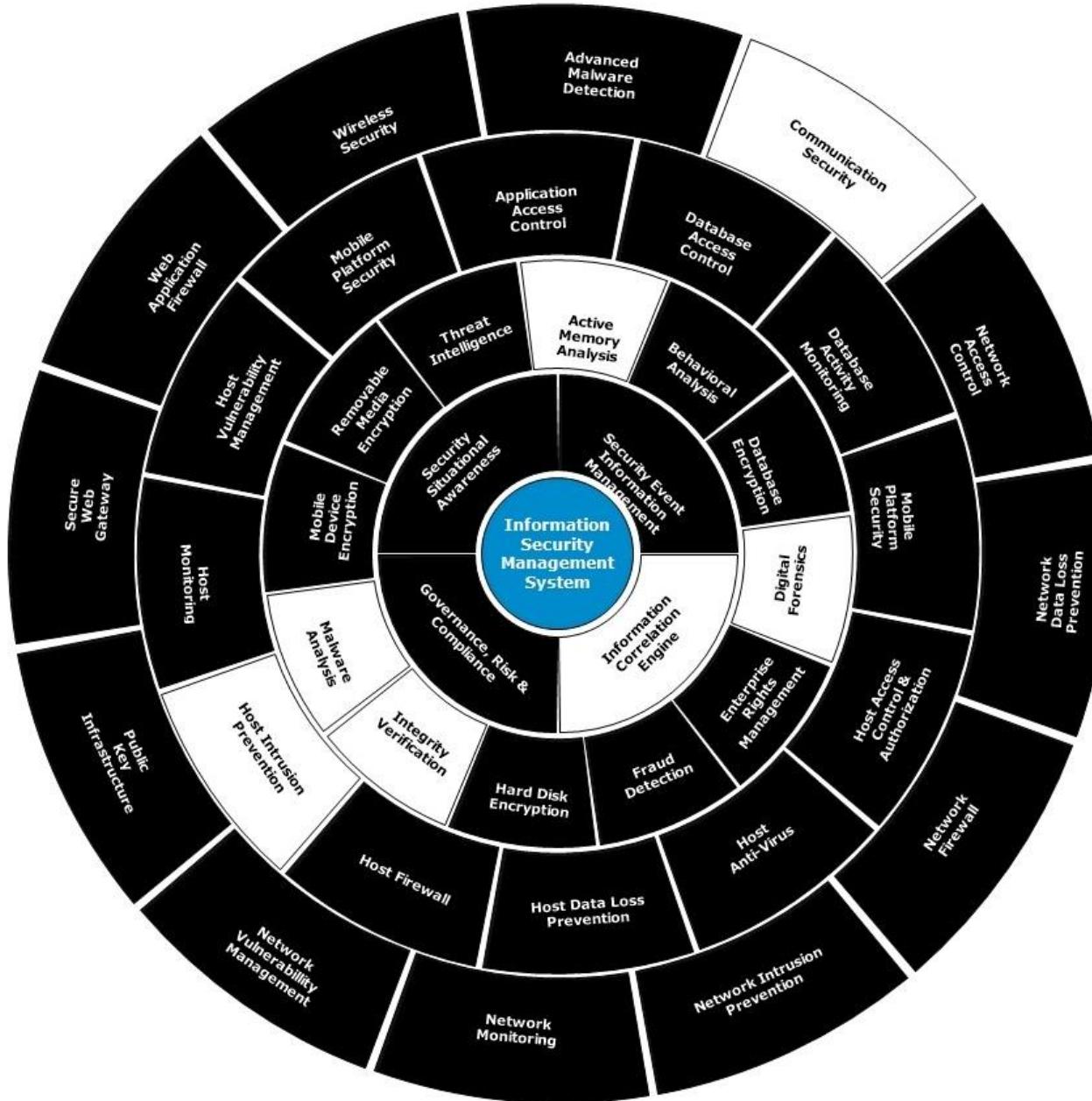
## Security Event Monitoring

# Log Management

## Event Correlation



# Information Security Management System



- ▶ Document Capability
- ▶ Target view of gaps

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



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



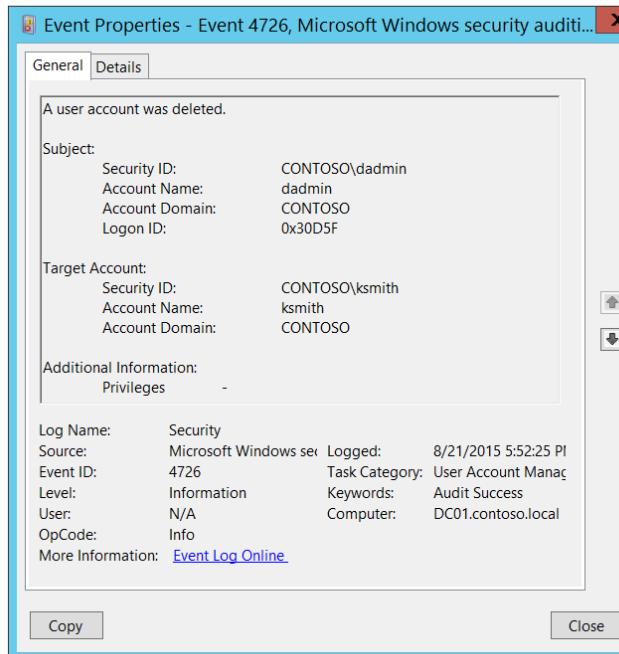
Degree of Maturity	
0	None
1	Initial
2	Repeatable
3	Defined
4	Managed
5	Optimized



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>
<Data Name="Privileges" />
```

## 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

The screenshot shows two versions of a documentation page for "Add Microsoft Active Directory data: Single instance".

**Left Panel (Original Page):**

- Header:** splunk> docs, PRODUCTS, SOLUTIONS, CUSTOMERS, COMMUNITY, SPLEXICON, Support & Services
- Section:** Add Microsoft Active Directory data: Single instance
- Sub-section:** Install and configure
- Content:**
  - Configure your Microsoft Active Directory domain to generate audit events
  - Enable a receiver on your Splunk Enterprise instance
  - Install universal forwarders on your Microsoft Active Directory hosts
  - Install the Splunk add-on for Microsoft Active Directory on your Splunk platform
  - Configure the Splunk add-on for Microsoft Active Directory on your Splunk platform
  - Verify data appears in your distributed Splunk Enterprise platform deployment
- Editor Actions:** Documentation, Edit, History, View All

**Right Panel (Updated Page):**

- Header:** Documentation / Splunk® Enterprise / Add Microsoft Active Directory data: Single instance
- Section:** Configuration general
- Content:**
  - Configure your Microsoft Active Directory domain to generate audit events
  - Enable a receiver on your Splunk Enterprise instance
  - Install universal forwarders on your Microsoft Active Directory hosts
  - Install the Splunk add-on for Microsoft Active Directory on your Splunk platform
  - Configure the Splunk add-on for Microsoft Active Directory on your Splunk platform
  - Verify data appears in your distributed Splunk Enterprise platform deployment
- Section:** Prerequisites
  - Verify user authentication credentials to a domain controller
  - Verify disk bandwidth and processor usage when you configure a universal forwarder for performance
  - Verify shared host file system access
- Section:** Configuration
  - Configure the Active Directory receiver to log them into the Splunk platform
  - By default, Active Directory users are mapped to their accounts in your AD environment
  - Then, you install universal forwarders on your clients. They collect logs from Active Directory users
- Text:** This topic shows you how to add Microsoft Active Directory data to your Splunk Enterprise instance.
- Section:** Enable auditing on Windows Server 2008, Server 2008 R2, Server 2012, and Server 2012 R2 [edit]
- Section:** Create a new group policy object [edit]
  - From the Windows Start menu, click Start > Administrative Tools > Group Policy Management.
  - In the left pane, under "Group Policy Management," expand the forest and domain for which you want to set group policy.
  - Right-click **Group Policy objects** and select **New**.
  - In the dialog window that opens, enter a unique name for your new group policy object (GPO) that you will remember in the **Name** field, and select **None** for the **Source Starter GPO** field.
- Section:** Edit the GPO to change audit policy [edit]
 

If you are on a version earlier than 2008 R1, use following steps:

  - Open the GPO for editing by right-clicking the newly created GPO in the Group Policy Objects window and selecting **Edit**.
  - In the GPO editor, select **Computer Configuration > Policies > Windows Settings > Security Settings > Local Policy > Audit Policy**.
  - Enable both **Success** and **Failure** auditing of the following policy settings:
    - Audit account logon events
    - Audit account management
    - Audit directory service access
    - Audit logon events
    - Audit object access
    - Audit policy change
    - Audit privilege use
    - Audit system events
  - Close the Group Policy Object Editor window to save your changes.

If you are using a version of 2008 R2 or greater, use the following steps:

  - Open the GPO for editing by right-clicking the newly created GPO in the Group Policy Objects window and selecting **Edit**.

splunk > App: Splunk Security Essentials

Administrator 4 Messages Settings Activity Help Find

Introduction Security Content Security Data Journey Data Source Check Documentation Advanced Splunk Security Essentials

AWS CloudTrail Last Updated: 02/22/2018

**Data Source Onboarding Guide Overview**

Overview General Infrastructure System Configuration Splunk Configuration for Data Source

Instruction Expectations and Scaling Indexes and Sourcetypes Overview Forwarder on Linux Systems Sending Data from Forwarders to Indexers General Infrastructure References AWS Setup Overview Set Up AWS Identity Access Management – IAM Set Up AWS Simple Notification Service – SNS Set up AWS Simple Queueing Service – SQS Set up AWS CloudTrail System Configuration References Where to Collect Logs From Installing the Technology Add-on – TA AWS Indexes and Sourcetypes

Welcome to the Splunk Data Source Onboarding Guides (DSOGs)! Splunk has lots of docs, so why are we creating more? The primary goal of the DSOGs is to provide you with a curated, easy-to-digest view of the most common ways to onboard data. By including how to configure the systems that will send us data (such as turning on AWS logging or Windows Security's process-launch logs, for example). With this configuration, they will give you the most common, easiest way forward. How to use these docs: We've broken the docs out into different segments that get linked together. Many of them will be shared across multiple products. When you're finished with one, click the "Mark Complete" button to indicate that you've completed it. Since this info will be stored locally in your browser, you won't have to worry about it affecting anyone else's view of the document. It's a convenient way to keep track of the fact that you already installed the forwarder in order to onboard your Windows Security logs. So, go on and dive right in! And don't forget, Splunk is here to make sure you're successful. Feel free to ask questions of your Sales Engineer or Professional Services team, or post your questions on <https://answers.splunk.com/>.

## General Infrastructure

Instruction Expectations and Scaling Mark Complete

### Expectations

This doc is intended to be an easy guide to onboarding data from Splunk, as opposed to a comprehensive set of docs. We've specifically chosen only straightforward configurations (no complex complications), but if at any point you feel like you need more traditional documentation for the deployment or usage of Splunk, [Splunk Docs](#) has you covered. Because simpler is almost always better when getting started, we are also not worrying about more complicated capabilities like Search Head Clustering, Ingestion requirements, and so on. Instead, we focus on the basics. If you need more information, Splunk Docs is a great place to get started, and you can also always avail yourself of Splunk Professional Services so that you don't have to worry about anything.

### Scaling

# Operational Flow

## Defining Processes



# **ONE DOES NOT SIMPLY ADD MONITORING**

# WITHOUT ALERTING

Source: memegen.com

splunk> .conf18

# Use Case Details

## Concentration of Attacker Tools by Filename

**How to Implement**

The hardest part of implementing this correctly, once you have process launch logs ingested, will be to make sure that the fields correctly set.

- In the live version, we start with index=\*, which is bad Splunk form (but makes it a little bit easier to get started). You should make sure that you specify the index where your process launch logs live (index=owinsec if you follow our best practices, and the documentation in this app).
- The next field you have to worry about is the sourcetype, which should be pretty standard.
- The EventCode field is the last field you have to think about, which if you use our Splunk\_TA\_windows on your Search Head, will also work automatically for you (again, docs are key!).

Once you have the search itself running, then you need only schedule it (click "Schedule Alert") and have Splunk email you, create a ticket in Enterprise Security or Service Now, or take some other action for you.

**Known False Positives**

**How To Respond**

This alert is very clearly tied to a known threat, so when it fires your concern is that this represents an attacker inside of one of your systems. Recommended steps are to begin incident response on the host where this alert fired from, to look for signs of other suspicious activities. The first step in that process will be to look at the parent process that launched these suspicious processes, and see what other activities that process has done. That should guide you to the underlying problem. As you get more information about this particular system (for example, how did malware end up on it, what websites has it communicated with, etc.), make sure to pivot and look across your entire organization for other indications, and to look in Open Source Intelligence sites like VirusTotal to learn more about the attacker.

**Show Search**

Show SPL (Splunk Search Language)

Enable Advanced SPL Mode

**Help**

Data Check	Status	Open in Search	Resolution (if needed)
Must have Demo Lookup	<span style="color: red;">!</span>	<a href="#">Open in Search</a>	Verify that lookups installed with Splunk Security Essentials is present

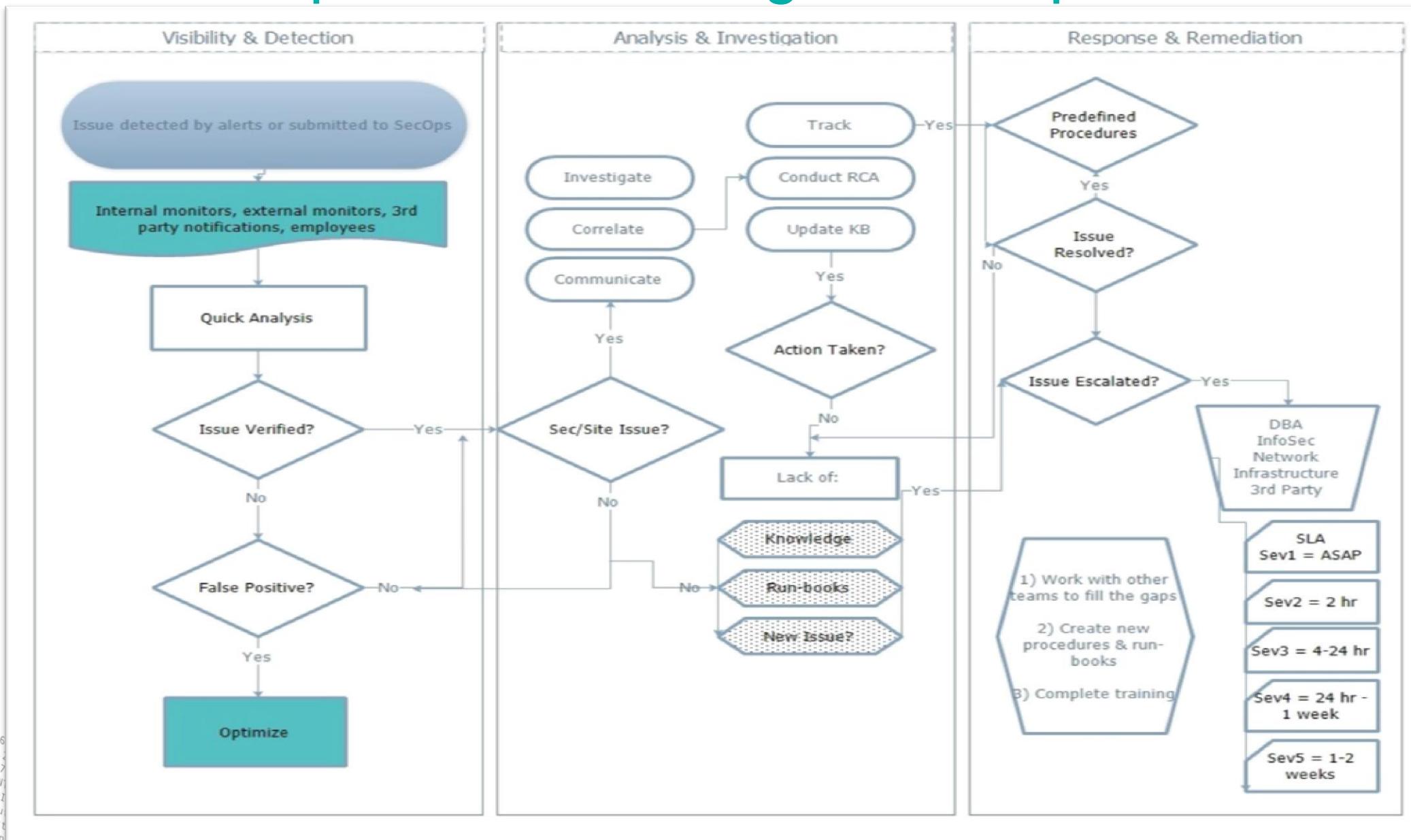
Enter a search

```
| `Load_Sample_Log_Data("Generic Sysmon Process Launches")`  
| search [|inputlookup tools.csv | search discovery_or_attack=attack | eval filename="Image=\\"*\\\\\\\" . filename . \"\" | stats values(filename) as search | eval search=mvjoin(search, "OR ")]  
| transaction host maxpause=5m  
| where eventcount>=4  
| fields - _raw closed_txn field_match_sum linecount
```

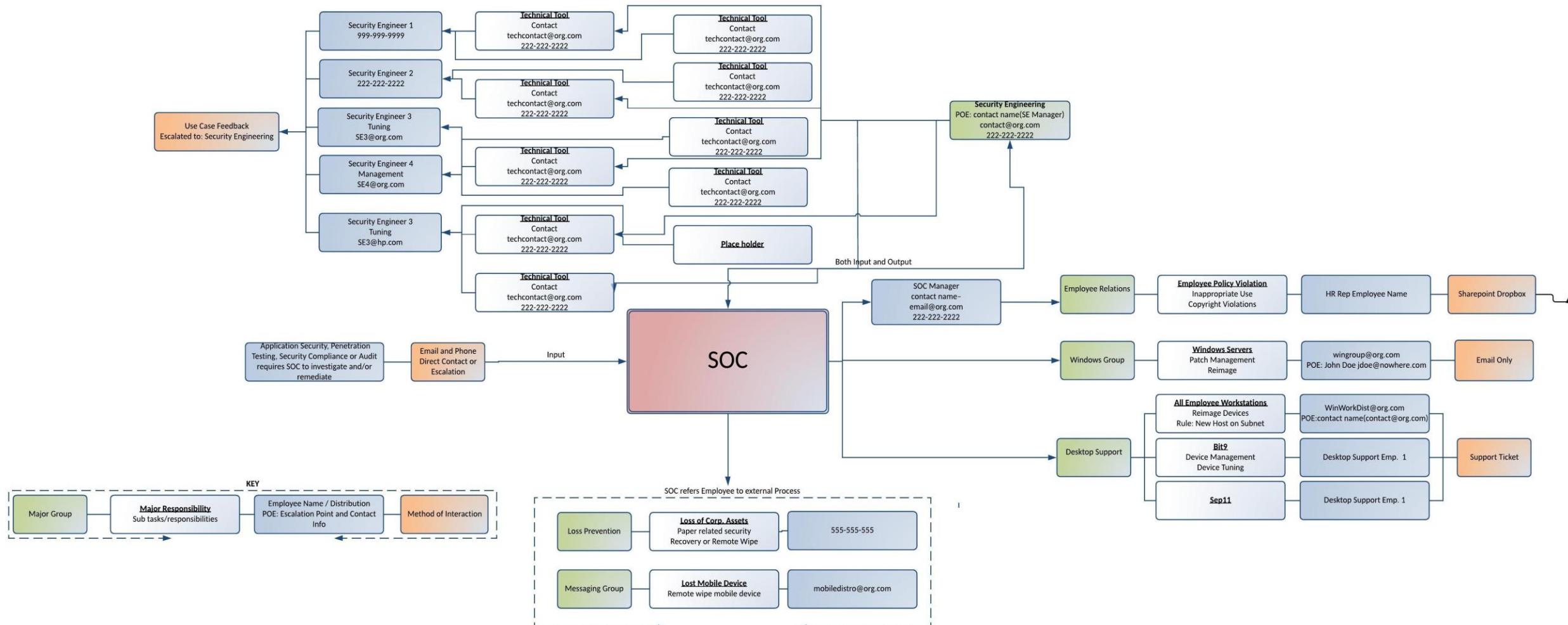
Last 30 days

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

# Simple Event Management Operational Flow



# Operational Inputs/Outputs Example



# 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 whether 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



# Thank You

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



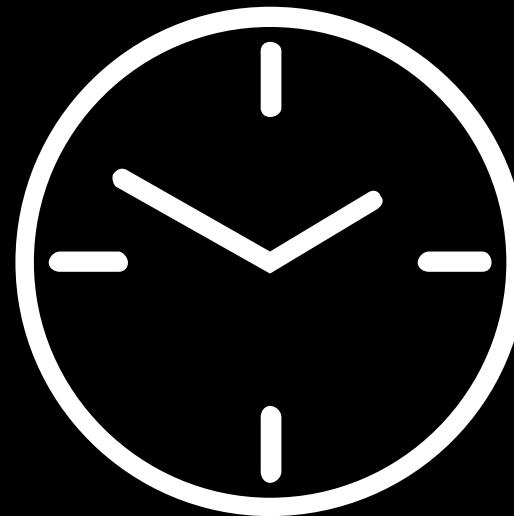
# Join the Pony Poll



[ponypoll.com/\\*\\*\\*](http://ponypoll.com/)

# Tracks and Sessions

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



# BREAK 15 MINUTES