

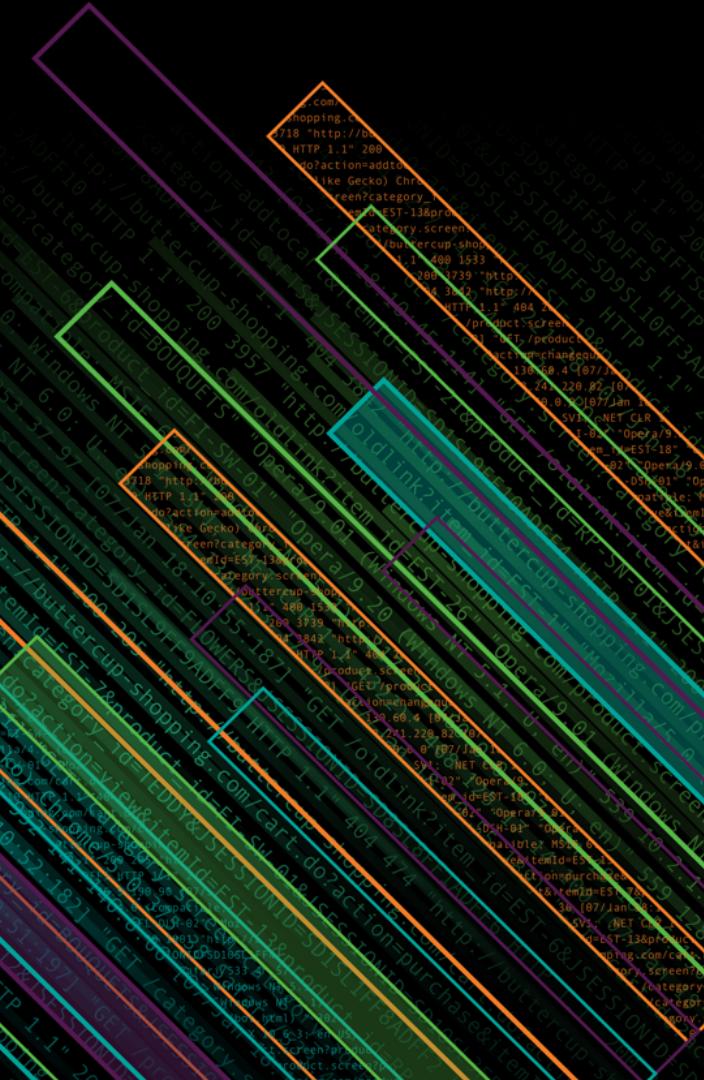


splunk>

# Splunk Security Essentials

## What's New, What's Awesome

David Veuve | Principal Security Strategist



# 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.

# Agenda

- ▶ Introductions – Who Are We, Who Are You?
  - ▶ What is SSE
  - ▶ What came in SSE 2.0 (Feb 2018)
  - ▶ What's come since SSE 2.0?
    - New Functionality
    - New Use Cases
  - ▶ Most Underused Functionality

# Introductions

# Personal Introduction

## ► David Veuve

Principal Security Strategist, Splunk

► [dveuve@splunk.com](mailto:dveuve@splunk.com)

► Former Splunk Customer

## ► Apps:

- **Splunk Security Essentials**
- SplunkJS For All
- Search Activity
- Newsletter
- Three more



If you want to know how  
to build an app like SSE

## ► 2018 Talks:

- Splunk Security Essentials: What's New and What's Awesome
- Go From Dashboards to Applications With Ease: SplunkJS for Non-Developers
- Security Ninjutsu Part Five: The Most Advanced Content Money Can Buy

## ► Past Conf Experience

- 8 Talks
- Delivered 11 Times
- To 2800+ people

# Who Are You?

# You're New To Splunk (or Security)

- ▶ You want to jump start with working content
  - ▶ You may not know where you want to start
  - ▶ You may want to see how the premium apps augment detection
  - ▶ You probably don't want to invest hundreds of hours reinventing the wheel

# You're Experienced with Splunk

- ▶ You want useful new SPL techniques
  - ▶ You want to see what's possible
  - ▶ You may like to come to my sessions to heckle me
  - ▶ You probably don't want to invest hundreds of hours reinventing the wheel

# Goal for Security Essentials and this Talk

- ▶ Collect a wide variety of great SPL in one place
- ▶ Provide ready-to-adapt Splunk content
- ▶ Cover the essential needs that someone getting started will have \*and\* the advanced needs of our biggest customers
- ▶ Make it easy to adopt this content
- ▶ Make the world a more secure place

# What Is SSE?

# Get The App

<https://splunkbase.splunk.com/app/3435/>

# 125+ Examples, with 180+ Searches

The screenshot shows the Splunk Security Content search interface. At the top, there's a navigation bar with links for "What's New in 2.2?", "Manage Bookmarks", "CSV", and more. Below the navigation is a search bar and filter controls for "Journey", "Security Use Case", "Category", "Data Sources", and "Recommended". The main area displays 21 search examples in a grid format:

- 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)
- Basic Brute Force Detection**: Uses a simple threshold for Windows Security Logs to alert if there are a large number of failed logins, and at least one successful login from the same source. (Recommended, Searches Included, Windows Security)
- Basic Malware Outbreak**: Looks for the same malware occurring on multiple systems in a short period of time. (Recommended, Searches Included, Anti-Virus)
- Basic Scanning**: Looks for hosts that reach out to more than 500 hosts, or more than 500 ports in a short period of time, indicating scanning. (Recommended, Searches Included, Network Communication)
- Basic TOR Traffic Detection**: The anonymity of TOR makes it the perfect place to hide C&C, exfiltration, or ransomware payment via bitcoin. This example looks for ransomware activity based on FW logs. (Recommended, Searches Included, Network Communication)
- Detect Excessive User Account Lockouts**: This search detects accounts that have been locked out a relatively high number of times in a short period. (Recommended, Try ES Content Update, Authentication)
- Endpoint Uncleaned Malware Detection**: Detect a system with a malware detection that was not properly cleaned, as they carry a high risk of damage or disclosure of data. (Recommended, Searches Included, Anti-Virus)
- Flight Risk Web Browsing**: This search implements several heuristics to look for indications that a user is a flight risk from Web Logs. Detect a user who may be leaving before they do. (Recommended, Searches Included, Web Proxy)
- Increase in # of Hosts Logged into**
- Increase in Pages Printed**
- Large Web Upload**
- Multiple Infections on Host**
- New Interactive Logon from a Service Account**

Each includes:

- ▶ Description
- ▶ Relevance
- ▶ How to Implement
- ▶ How to Respond
- ▶ Known False Positives
- ▶ Line-by-Line SPL Documentation
- ▶ And More!

# Mapping of 300+ Detections from Premium Apps

**Security Content**

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

**Filter Examples**

Journey	Security Use Case	Category	Data Sources	Recommended	Originating App
All selected (6) ▾	All ▾	All ▾	All ▾	All ▾	4 selected ▾

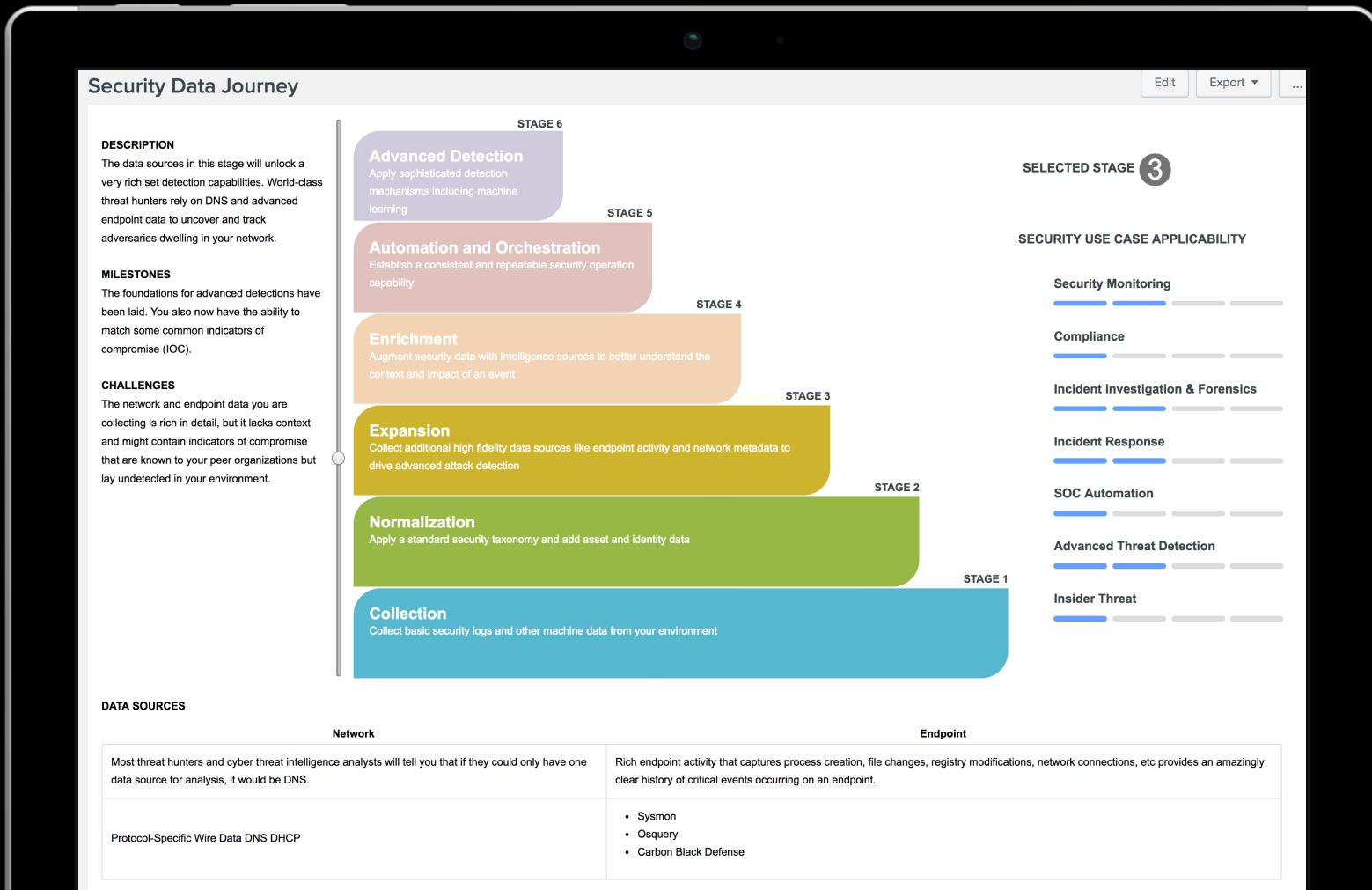
**Learn how to use this page**  431 Total | 431 Filtered

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

<b>Detect Excessive User Account Lockouts</b> This search detects accounts that have been locked out a relatively high number of times in a short period.  <input type="button" value="Recommended"/> <input type="button" value="Try ES Content Update"/> <input type="button" value="Authentication"/>	<b>Unusually Long Content-Type Length</b> This search looks for unusually long strings in the Content-Type http header that the client sends the server.  <input type="button" value="Recommended"/> <input type="button" value="Try ES Content Update"/> <input type="button" value="Web Server"/>	<b>Detect Activity Related to Pass the Hash Attacks</b> This search looks for specific authentication events from the Windows Security Event logs to detect potential attempts at using the Pass-the-Hash technique.  <input type="button" value="Try ES Content Update"/> <input type="button" value="Authentication"/>	<b>Detect Excessive Account Lockouts From Endpoint</b> This search identifies endpoints that have caused a relatively high number of account lockouts in a short period.  <input type="button" value="Try ES Content Update"/> <input type="button" value="Authentication"/>	<b>Detect Large Outbound ICMP Packets</b> This search looks for outbound ICMP packets with a packet size larger than 1,000 bytes. Various threat actors have been known to use ICMP as a command and control channel for their attack infrastructure. Large ICMP packets from an endpoint to a remote host may be indicative of this activity.  <input type="button" value="Try ES Content Update"/>
<b>Detect Mimikatz Via PowerShell And EventCode 4663</b> This search looks for PowerShell reading lsass memory consistent with credential dumping.  <input type="button" value="Try ES Content Update"/> <input type="button" value="Windows Security"/>	<b>Detect Mimikatz Via PowerShell And EventCode 4703</b> This search looks for PowerShell requesting privileges consistent with credential dumping.  <input type="button" value="Try ES Content Update"/> <input type="button" value="Windows Security"/>	<b>Detect New Local Admin account</b> This search looks for newly created accounts that have been elevated to local administrators.  <input type="button" value="Try ES Content Update"/> <input type="button" value="Windows Security"/>	<b>Detect Outbound SMB Traffic</b> This search looks for outbound SMB connections made by hosts within your network to the Internet. SMB traffic is used for Windows file-sharing activity. One of the techniques often used by attackers involves retrieving the credential hash using an SMB request made to a compromised server controlled by the threat actor.  <input type="button" value="Try ES Content Update"/> <input type="button" value="Web Server"/>	<b>Detect S3 access from a new IP</b> This search looks at S3 bucket-access logs and detects new or previously unseen remote IP addresses that have successfully accessed an S3 bucket.  <input type="button" value="Try ES Content Update"/>
<b>Detect Spike in blocked Outbound Traffic from</b>	<b>Email servers sending high volume traffic to hosts</b>	<b>Extended Period Without Successful Netbackup</b>	<b>First Time Seen Running Windows Service</b>	<b>Hosts receiving high volume of network traffic</b>

- ▶ Covering: Enterprise Security, ESCU, UBA, and Pro Serv
- ▶ Mapped by Category, Maturity, Use Case, MITRE, Kill Chain, and Data Source

# Splunk Security Data Journey



## Each Stage Includes:

- ▶ Description
- ▶ Milestones
- ▶ Benefits
- ▶ Challenges
- ▶ Data Sources
- ▶ Use Case Mapping

# What's New – SSE 2.0?

February 2018 Was a Big Release...

## 2.0 Major Features

- ▶ The Journey
  - ▶ Expansion of Content (GDPR, AWS, and the Basics)
  - ▶ Data Onboarding Guides
  - ▶ New Mapping of Content
  - ▶ It's Pretty!

# But Why Tell You When I Can Show You?

- ## ▶ Insert Meme...



# Journey

## Security Data Journey

Edit Export ...

### DESCRIPTION

Find anomalous behavior and unknown threats by applying machine learning, data science and advanced statistics to analyze the users, endpoint devices, and applications in your environment.

### MILESTONES

At this stage, you have given yourself a fighting chance to detect adversaries and insiders even when they leave only subtle traces of their activity.

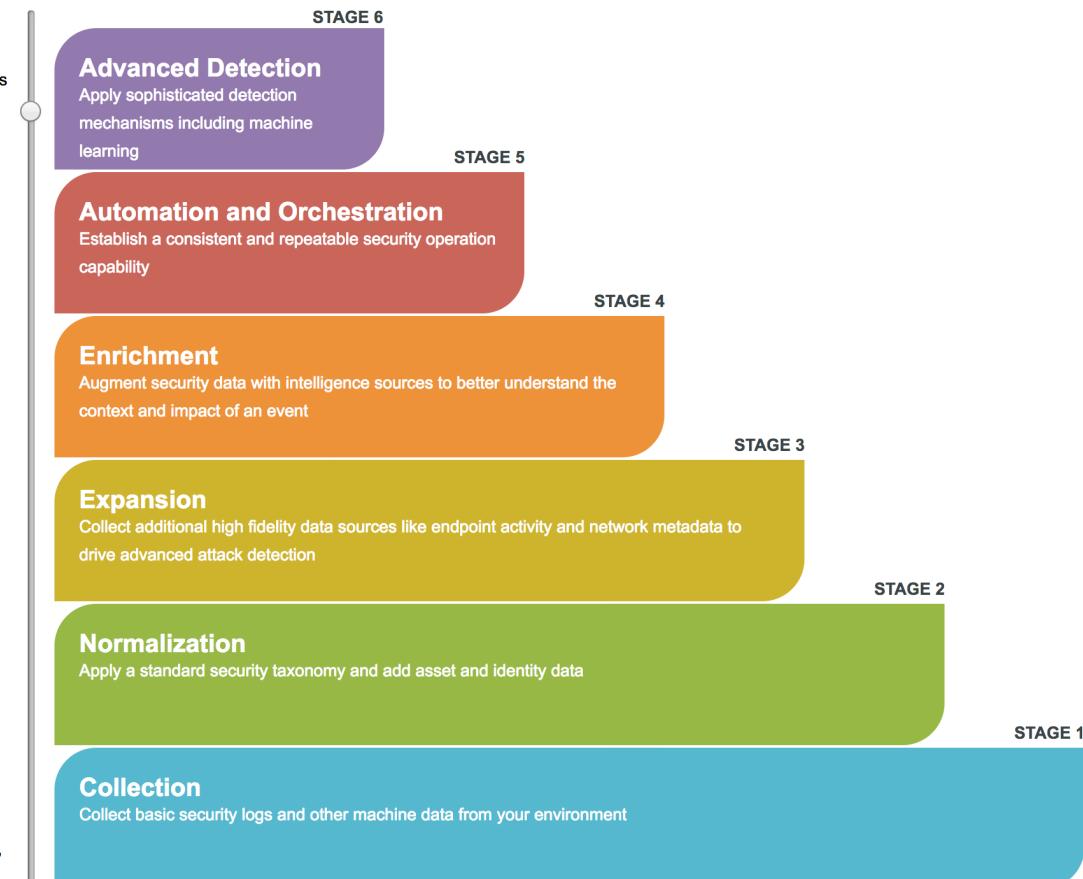
- You are employing the most advanced techniques available to identify unknown threats.
- You are employing new detection mechanisms as they become available, leveraging your team's expertise and leveraging outside research organizations.

### CHALLENGES

- At this stage, you will be challenged to constantly improve your security organization.
- To gain new capabilities, your team will likely be required to perform new research.
- Although you are at the top of your game, there are no guarantees and the most advanced adversaries may still successfully attack your organization.

### DATA SOURCES

This stage focuses more on what you do with the data you have vs. onboarding new sources.



SELECTED STAGE **6**

### SECURITY USE CASE APPLICABILITY

#### Security Monitoring



#### Compliance



#### Incident Investigation & Forensics



#### Incident Response



#### SOC Automation



#### Advanced Threat Detection



#### Insider Threat



# GDPR Content

## Stage 4: Enrichment [🔗](#)

You are business aware, with Splunk aware of assets, identities, vulnerabilities, and threat intelligence.

<p><b>&gt; Brute Force Access Behavior Detected - Against Category</b></p> <p>Monitor your security controls and prove your GDPR compliance by detecting brute force (or password guessing) attacks on GDPR-tagged systems.</p> <p><b>Recommended</b></p> <p><b>Searches Included</b></p> <p><b>Authentication Windows Security</b></p>	<p><b>&gt; Excessive DNS Failures</b></p> <p>Alerts when a host receives many DNS failures in a short span</p> <p><b>Try Splunk ES</b></p> <p><b>DNS</b></p>	<p><b>&gt; Expected Host Not Reporting - in Category</b></p> <p>GDPR requires an audit trail for all activities, which means we should be receiving events constantly. Find GDPR-tagged systems that are no longer reporting events but should be.</p> <p><b>Recommended</b></p> <p><b>Searches Included</b></p> <p><b>Any Host Logs</b></p>	<p><b>&gt; Geographically Improbable Access Detected against Category</b></p> <p>To ensure you have a GDPR-mandated audit trail with individual accounts for each person, detect when the same account is logged into twice in a short period of time but from locations very far away, to a GDPR-tagged system.</p> <p><b>Recommended</b></p>	<p><b>&gt; In-Scope Device with Outdated Anti-Malware Found</b></p> <p>Alerts when a GDPR-tagged system has out of date malware definitions, which would conflict with GDPR's requirement to maintain a secure environment.</p> <p><b>Recommended</b></p> <p><b>Searches Included</b></p> <p><b>Anti-Virus</b></p>
<p><b>&gt; In-Scope System with Windows Update Disabled</b></p> <p>Any GDPR-tagged systems not receiving updates could jeopardize your GDPR status due to Article 32. Detect systems where the Windows Update service is disabled.</p> <p><b>Recommended</b></p> <p><b>Searches Included</b></p>	<p><b>&gt; New Connection to In-Scope Device</b></p> <p>Alert Data Protection Officers to new systems that become involved in processing GDPR-scoped data via network communication logs, so DPOs can ensure the systems are authorized and documented.</p> <p><b>Recommended</b></p> <p><b>Searches Included</b></p>	<p><b>&gt; User Has Access to In-Scope Splunk Indexes They Should Not Have</b></p> <p>Alerts the first time a user gains rights to search an index that they're not supposed to according to the output of a GDPR data source and GDPR user mapping exercise.</p> <p><b>Recommended</b></p> <p><b>Searches Included</b></p>	<p><b>&gt; User Logged into In-Scope System They Should Not Have</b></p> <p>Follow your GDPR requirement and action your data mapping exercise by tracking employee/vendor/supplier access to systems, to ensure that they are authorized to view the data present on any systems they log into.</p> <p><b>Recommended</b></p>	<p><b>&gt; Activity from Expired User Identity - on Category</b></p> <p>The GDPR requires that only authorized individuals access personal data. Alert when the account of a past employee is used to log into GDPR-tagged systems</p> <p><b>Searches Included</b></p> <p><b>Authentication Windows Security</b></p>
<p><b>&gt; Brute Force Access Behavior Detected Over One Day - Aga...</b></p> <p>Monitor your security controls and prove your GDPR compliance by detecting slow and low brute force (or password guessing) attacks on GDPR-tagged systems that occur gradually over the day.</p> <p><b>Searches Included</b></p> <p><b>Authentication Windows Security</b></p>				

## Stage 5: Automation and Orchestration [🔗](#)

# AWS Content

## Stage 3: Expansion ↗

You're ingesting advanced data sources and running better investigations.

### > AWS Cloud Provisioning Activity from Unusual Country

Looks for AWS Provisioning activities that occur from new IPs, using GeoIP to resolve the Country.

Recommended  
Searches Included  
Audit Trail

### > AWS Instance Created by Unusual User

Detects the first time a user creates a new instance.

Recommended  
Searches Included  
Audit Trail

### > AWS New API Call Per User

Looks for users that are using AWS APIs that they've never used before.

Recommended  
Searches Included  
Audit Trail

### > AWS Unusual Amount of Modifications to ACLs

Looks for a large number of Security Group ACL changes in a short period of time for a user.

Recommended  
Searches Included  
Audit Trail

### > Public S3 Bucket in AWS

Detects when new or existing S3 buckets are set to public.

Recommended  
Searches Included  
Audit Trail

### > AWS APIs Called More Often Than Usual Per User

Builds a per-user baseline for how many API calls is normal, and then alerts for deviations.

Searches Included  
Audit Trail

### > AWS Cloud Provisioning Activity from Unusual IP

Looks for AWS Provisioning activities that occur from new IPs (for organizations with strict IP controls).

Searches Included  
Audit Trail

### > AWS Instance Modified by Unusual User

Detects the first time a user modifies an existing instance.

Searches Included  
Audit Trail

### > Unusual AWS Regions

Looks for activity in AWS Regions that have not been used before across the organization.

Searches Included  
Audit Trail

## Stage 4: Enrichment ↗

You are business aware, with Splunk aware of assets, identities, vulnerabilities, and threat intelligence.

### > AWS New API Call Per Peer Group

Looks for users that are using AWS APIs that neither they, nor their team has ever used before.

Recommended

# Data Onboarding Guide

<b>Data Source Onboarding Guide</b>
<b>Overview</b>
Overview
<b>General Infrastructure</b>
Instruction Expectations and Scaling
Indexes and Sourcetypes Overview
Forwarder on Windows Systems
Sending Data from Forwarders to Indexers
General Infrastructure References
<b>Splunk Configuration for Data Source</b>
Sizing Estimate
Install the Technology Add-On -- TA
General Windows Indexes and Sourcetypes
Configuration Files
Splunk Configuration for Data Source References
<b>Windows Configuration</b>
Enabling Windows Security Log
Windows Configuration References

```
disabled = 0
sourcetype = WindowsUpdateLog
index = oswinsec

[WinHostMon://Service]
interval = 3600
disabled = 0
type = Service
index = oswinscript
```

## Splunk Configuration for Data Source References Mark Complete

Here are links from this section:

- [Splunkbase](#)
- [Splunkbase: Download Windows Add-on](#)

## Windows Configuration

### Enabling Windows Security Log Mark Complete

#### Overview

To maintain a good Security Posture, and to leverage the examples provided in Splunk Security Essentials, we recommend following Microsoft's official guidance for "Stronger" security visibility. The Audit Policy Recommendations page from Microsoft TechNet provides very detailed configuration settings per operating system from Windows 7 / Server 2008 and up here: <https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/audit-policy-recommendations>

#### Implementation

**Important Note:** Splunk is a monitoring product, and not an Active Directory system, so while we're working hard to centralize some of the recommendations you should follow in one place to make your life easy, we cannot offer support for the actual configuration of anything other than Splunk itself, and strongly recommend that you leverage trained Microsoft resources when making any changes. That's in large part why we're pointing you to Microsoft docs for the nitty gritty details!

If you are new to configuring auditing on Microsoft systems, there are two primary ways in which you can go about configuring auditing: a one-off (typically lab) system via the Local Security Policy, or a managed system via Group Policy. Virtually all Splunk customers will configure their Windows audit logging via Group Policy, but you absolutely can use Local Security Policy if you only have a small number of machines, or you are trialing on a few systems.

If you do want to configure via Local Security Policy, you can click Start (or highlight Cortana Search) and then type in "Local Security Policy" to open the policy editor. Finding the right configuration settings is straightforward, just expand "System Audit Policies – Local Group Policy" at the bottom of the list, and then the next item with the same name. If you compare these items to the link above (also included under "References"), you will find that they map directly and you can proceed to mirror what Microsoft recommends – use the Stronger column for adequate security visibility.

# Mapping of Content to Frameworks

**Security Content / New Local Admin Account**

Assistant: Simple Search

**Description**

Local admin accounts are used by legitimate technicians, but they're also used by attackers. This search looks for newly created accounts that are elevated to local admins.

**Use Case**  
Advanced Threat Detection, Security Monitoring, Compliance

**Category**  
Endpoint Compromise

**Alert Volume**  
Medium (?)

**SPL Difficulty**  
Medium

**Stage 1** **MITRE ATT&CK Tactics**  
**Defense Evasion** **Persistence**

**Kill Chain Phases**  
**Command and Control**

**Data Sources**  
**Audit Trail** **Windows Security**

> **Related Splunk Capabilities**  
 > **How to Implement**  
 > **Known False Positives**  
 > **How To Respond**  
 > **Show Search**  
 > **Help**

**DEMO DATA** You're looking at the *Demo* search right now. Did you know that we have 2 searches for this example? [Scroll Up](#) to the top to see the other searches.

Outlier(s)	Raw Event(s)
1	158

# New Functionality Since 2.0



# Content Access Enhancements

- ▶ Search Bar!
  - ▶ Notable Event Improvement
  - ▶ Link to ES and ESCU
  - ▶ Support for Windows TA 5.0 (\*eyeroll\*)

# Let's Go Look!

# Search Bar

**Security Content**

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

**Filter Examples** (25 hidden by filters) **aws** [Learn how to use this page](#) [Select Filters](#) 431 Total | 431 Filtered [X Clear Filters](#) [Default Filter](#)

Journey	Security Use Case	Category	Data Sources	Recommended
All selected (6) ▾	All ▾	All ▾	All ▾	All ▾

**Originating App**  
Splunk Security Essentials (125 matches) ▾

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

**Stage 2: Normalization**   
You've applied Common Information Model, opening you to detections shared from others, and premium apps.

**Stage 3: Expansion**   
You're ingesting advanced data sources and running better investigations.

**> AWS Cloud Provisioning Activity from Unusual Country**  
Looks for AWS Provisioning activities that occur from new IPs, using GeoIP to resolve the Country.

[Recommended](#)  
[Searches Included](#)  
[Audit Trail](#)

**> AWS Instance Created by Unusual User**  
Detects the first time a user creates a new instance.

[Recommended](#)  
[Searches Included](#)  
[Audit Trail](#)

**> AWS New API Call Per User**  
Looks for users that are using AWS APIs that they've never used before.

[Recommended](#)  
[Searches Included](#)  
[Audit Trail](#)

**> AWS Unusual Amount of Modifications to ACLs**  
Looks for a large number of Security Group ACL changes in a short period of time for a user.

[Recommended](#)  
[Searches Included](#)  
[Audit Trail](#)

**> Public S3 Bucket in AWS**  
Detects when new or existing S3 buckets are set to public.

[Recommended](#)  
[Searches Included](#)  
[Audit Trail](#)

**> AWS APIs Called More Often Than Usual Per User**

**> AWS Cloud Provisioning Activity from Unusual IP**

**> AWS Instance Modified by Unusual User**

**> Unusual AWS Regions**



# Notable Event Improvement

- ▶ When you save a notable-creating search, it will automatically move that search into the ES workspace.
  - ▶ Then it will grab the search object and set the appropriate parameters that can't be passed through the normal search save dialog
  - ▶ Then it will prompt you and provide a link to go edit that search in ES

# Link to ES and ESCU

splunk>enterprise App: Splunk Security Essentials ▾

H David Veuve ▾ 17 Messages ▾ Settings ▾ Activity ▾ Help ▾ Find

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

**Splunk Security Essentials**

**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 screenshots that you can select below. Find out more about [Splunk Enterprise Security Content Updates](#) [here](#).

**Detect Excessive User Account Lockouts**

**Stage 1**

**Security Monitoring**

**Account Compromise**

This search detects accounts that have been locked out a relatively high number of times in a short period.

**Recommended**

**Try ES Content Update**

**Authentication**

**Analytic Story Details**

Story Name	# of Detection Searches	# of Investigative Searches	# of Contextual Searches	# of Supporting Searches	Description	Launch!
Account Monitoring and Controls	4	2	6	0	A common attack technique is to leverage user accounts to gain unauthorized access to the target's network. This Analytic Story minimizes opportunities for attack by helping you actively manage creation/use/dormancy/deletion—the lifecycle of system and application accounts.	<a href="#">Open in ESCU</a>

# Support for Windows TA

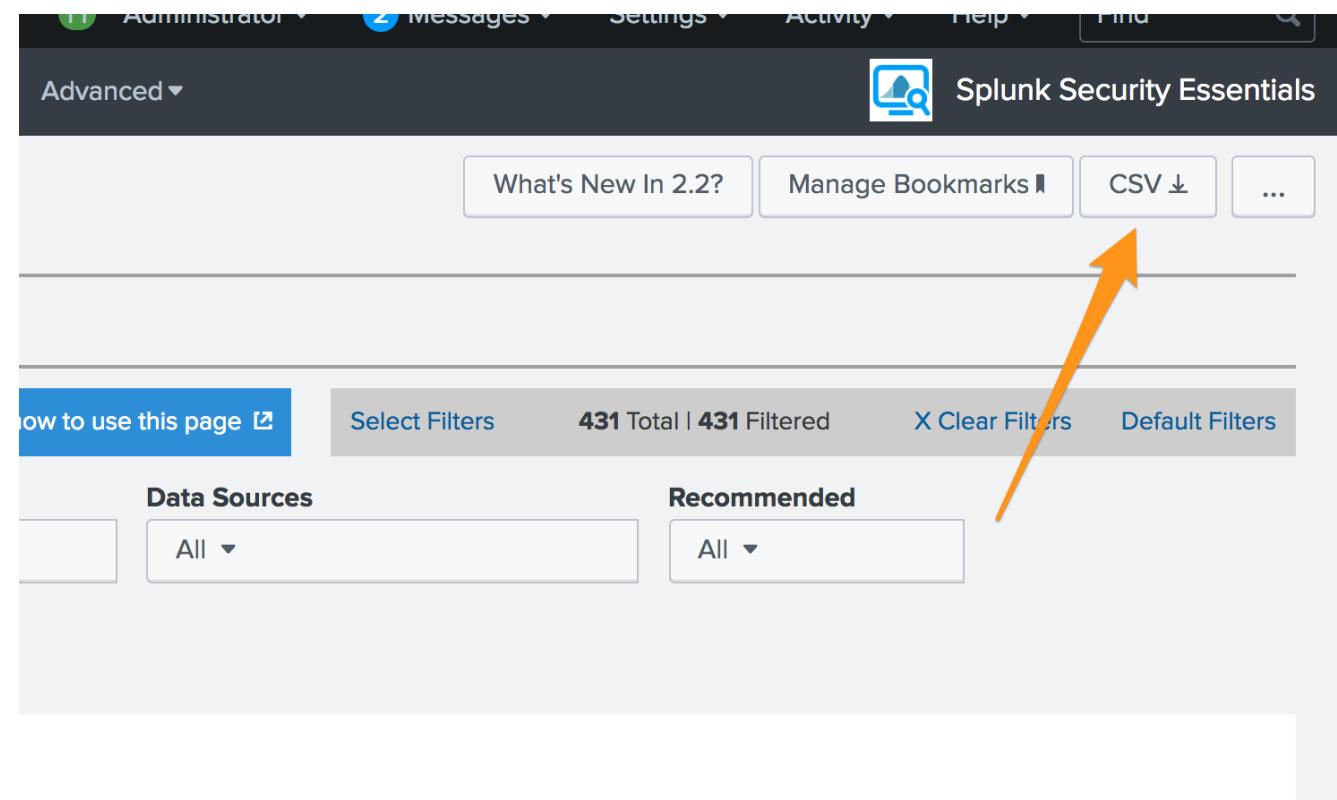
- ▶ Switched sourcetype=win\*security to source=win\*security

# Organizing Content

- ▶ Output content to CSV for your mapping exercises
  - ▶ Allows you to remember content that you find useful
  - ▶ Shared amongst team members
  - ▶ PDF Export!

# Let's Go Look!

# Output Content to CSV



# Bookmark

- ▶ Bookmark content to remember it
  - ▶ Share it amongst your team members
  - ▶ Set the status
  - ▶ Export a PDF or CSV with that content  
  - ▶ Check out this video of it: <https://youtu.be/W5KCn-zieDg>

# New Content Since 2.0



# Content Over Time

- ▶ 1.0: 42 Use Cases
- ▶ 1.1: 42 Use Cases
- ▶ 1.2: 47 Use Cases
- ▶ 1.3: 53 Use Cases
- ▶ 1.4: 53 Use Cases
- ▶ 2.0: 94 Use Cases (AWS Pack, Basics Pack) + 200+ Mapped Premium Content
- ▶ 2.1: 100 Use Cases (GDPR Pack) + 200+ Mapped Premium Content
- ▶ 2.2: 125 Use Cases (Insider Threat Pack) + 300+ Mapped Premium Content

# Let's Take a Tour



The screenshot shows the Splunk Security Essentials app interface. At the top, there are navigation links: Introduction, Security Content (selected), Security Data Journey, Data Source Check, Documentation, Advanced, and a Splunk logo. Below the navigation is a search bar and filter options: Journey (All selected), Security Use Case (All), Category (All), Data Sources (All), and a dropdown for Recommended. A message says "What's New In 2.27" and "Manage Bookmarks". The main area is titled "Security Content" and shows "Stage 1: Collection". It contains ten items, each with a green checkmark icon and a title: "Access to In-scope Resources", "Access to In-Scope Unencrypted Resources", "Authentication Against a New Domain Controller", "Basic Brute Force Detection", "Basic Malware Outbreak Detection", "Basic Scanning", "Basic TOR Traffic Detection", "Endpoint Undetected Malware Detection", "Flight Risk Web Browsing", and "Increase in # of Hosts Logged Into". Each item has a detailed description below it. At the bottom of the interface is a grid of 20 empty grey boxes, likely for additional content or filters.



... for the PDF copy of these slides ...

- ▶ You should go download the app!
  - ▶ It's pretty safe, I promise
  - ▶ You can also look at the content released in SSE 2.2, here:  
  - ▶ <https://splunk.box.com/s/s5clrzia7c3c3o25tfgxi1a2ib5btc4f>

# Most Underused Functionality



# Viewing the Full SPL

- ▶ At first glance, many may not notice that there's extensive documentation in the SPL
- ▶ Very few people actually click this (much to my chagrin)
  
- ▶ Spread the word!

**> How To Respond**

**>Show SPL (Splunk Search Language)** 

Enable Advanced SPL Mode

**> Help**

**DEMO DATA** You're looking at the Demo search right now. Did you know that we have 3 searches for this example? [Scroll Up](#) to the top to see the other searches.

**Outlier(s) ↗**  1 Outlier(s)

**Raw Event(s)**  612 Raw Event(s)

**Outliers Only**

bytes	bytes_in	bytes_out	inlist	uri	ut_domain	_time
1298	1122	176	true	<a href="http://sensitivedata.chickenkiller.com/updates?id=3020195">http://sensitivedata.chickenkiller.com/updates?id=3020195</a>	chickenkiller.com	2016-08-11



**View SPL ↗** 

```

`Load_Sample_Log_Data(Web Proxy Logs)`

eval list="mozilla" | `ut_parse_extended(uri,list)`

lookup dynamic_dns_lookup domain as ut_domain OUTPUT
inlist

search inlist=true

table _time ut_domain inlist bytes* uri

```

// First we bring in our basic demo dataset, proxy logs. We're using a macro called Load\_Sample\_Log\_Data to wrap around | inputlookup, just so it is cleaner for the demo data.

// Because we are looking for dynamic dns providers, we're going to need to separate out subdomains from the registered domain. URL Toolbox is just the tool for this job!

// Next we can use our lookup of ddns domains (see How to Implement). This will add a field called inlist with the value "true" for any matches.

// And finally we can look for those records that are matches.

// With our dataset complete, we just need to arrange the fields to be useful.

# Lookup Cache on First Time Seen

- ▶ First Time Seen detections are very easy to scale
- ▶ For most environments, for most detections, don't think twice
- ▶ "most"? Look at the size of the lookup.
  - If the lookup is < 10 MB, zero impact.
  - If the lookup is < 100 MB, basically no impact (but double check distsearch.conf blacklist to make sure it doesn't enter the search bundle)
  - If the lookup is < 500 MB, it will be slow but serviceable for daily queries (and double check distsearch.conf)
  - If the lookup is < 1000 MB, be cautious but expect success.. Maybe test in QA first
  - If the lookup is > 1000 MB, may be too big for SHC replication.. Definitely test in QA first

(all rough numbers)

- ▶ Okay, how do we take advantage of that?
- ▶ When running a query with the first time search builder, in advanced SPL mode, hit the dropdown for a lookup.

The screenshot shows the 'How To Respond' interface in Splunk. It includes sections for 'Show Search' (with 'Show SPL (Splunk Search Language)' and 'Enable Advanced SPL Mode' options), 'Help', and a main area for creating a lookup cache.

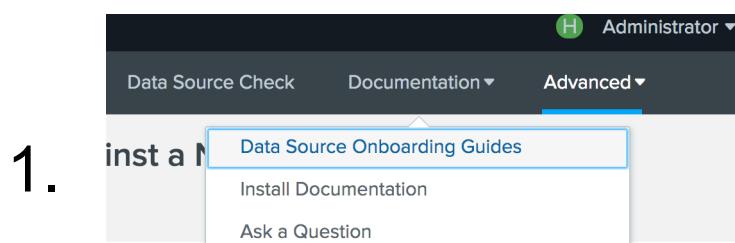
**1.** Shows the 'Create Blank Lookup Cache' button and an optional dropdown for 'Create Lookup'.

**1.5.** Shows the dropdown menu for selecting a group, with 'SampleCacheGroup' selected and checked.

**2.** Shows the dropdown expanded to show available groups: 'No Lookup Cache', 'account\_status\_tracker', 'previously\_seen\_S3\_access\_from\_remote\_ip', and 'SampleCacheGroup', which is highlighted with a blue border.

# Data Onboarding Guides

- ▶ Even if the data is onboarded, read through to learn the best practices
- ▶ You may discover something missing in your configuration!



1.

The screenshot shows a table titled 'Data Source Onboarding Guides' with the following data:

Data Source Onboarding Guides			
Splunk can ingest data from any type of product. Here are a few that are highlighted in Splunk Security Essentials.			
Below, you will find a detailed list of the Data Sources that commonly make Splunk for Security (and certainly Splunk Security Essentials) tick, along with some of the common products for each.			
Among the full list, we have several products where we've built out full data onboarding guides, to help walk you through the process:			
<a href="#">Windows Process Launch Logs</a>	<a href="#">Windows Security Logs</a>	<a href="#">Microsoft Sysmon</a>	<a href="#">Linux Auth Logs</a>
<a href="#">Cisco ASA</a>	<a href="#">Office 365</a>	<a href="#">Palo Alto Networks</a>	<a href="#">AWS CloudTrail</a>
<a href="#">Splunk Stream DNS</a>	<a href="#">Symantec EP</a>	<a href="#">AWS VPC Flow</a>	
Data Source	# of Common Products	# of Data Source Guides	
> Authentication	5	2	

2.

# Key Takeaways

# Download the app!

<https://splunkbase.com/app/3435>

Also, check out the booklet:

# The Essential Guide to Security

[https://www.splunk.com/en\\_us/form/the-essential-guide-to-security.html](https://www.splunk.com/en_us/form/the-essential-guide-to-security.html)

Splunk Security  
Essentials provides  
tons of ready-made  
content, and mappings  
to Splunk's premium  
content

If you find sessions and apps like this useful, please rate us in the app so that Splunk provides have more people build things like this.

# Other Recommended Talks

SEC1583 - Turning Security Use Cases into SPL	Hunting / IR
SEC1039 - Detection Technique Deep Dive	Hunting / IR
SEC1297 - Down in the Weeds, Up in the Cloud: Splunking your Azure and Office 365	Hunting / IR
SEC1355 - Hunting the Known Unknown: Microsoft Cloud	Hunting / IR
SEC1244 - Cops and Robbers: Simulating the Adversary to Test Your Splunk Security Analytics	Hunting / IR
SEC1547 - Splunk Security Essentials: What's New and What's Awesome	Hunting / IR
SEC1538 - Security Ninjutsu Part Five: The Most Advanced Content Money Can Buy	Hunting / IR
FN1209 - Visualize This, Mother Trucker	Visualizations
FN1398 - Splunk and the Machine Learning Toolkit in Action: Customer Use Cases	Data Science
SEC1979 - Splunk Phantom at Starbucks	Orchestration
SEC1898 - Pour Oil Not Sand Into Your Security Operations Center	Orchestration
SEC1233 - Hacking Your SOEL: SOC Automation and Orchestration	Orchestration
FN1913 - Old Meets New: Syslog and Splunk Connect for Kafka	Kafka
FN1211 - Don't Miss the Bus -- Splunking Kafka at Scale	Kafka
FN1184 - Unleashing Data Ingestion from Apache Kafka	Kafka
SEC1905 - 159 Security Use Cases in Record Time with Splunk and Kafka	Kafka
FN1629 - Exciting, To-Be-Announced Platform Session	Roadmap
FN1508 - Exciting, To-Be-Announced Platform Session	Roadmap
SEC1987 - What's New in Splunk for Security	General Security
SEC1983 - Splunk User Behavior Analytics (UBA): Methods and Best Practices to Get Started Now	UBA
SEC1275 - Monitoring and Mitigating Insider Threat with Splunk Enterprise and Splunk UBA	UBA
SEC1982 - Splunk UBA Tunes Down the Volume at Shentel	UBA
SEC1796 - Addressing Alert Fatigue and Threat Hunting with Analytic Stories	ES
SEC1310 - Enterprise Security Biology Revisited: Dissecting the Asset and Identity Frameworks	ES
SEC1570 - Enterprise Security Health Check	ES
SEC1479 - Say Goodbye to Your Big Alert Pipeline, and Say Hello To Your New Risk-Based Approach	ES and Risk

# Thank You

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

