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> .conf18

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

- Former Splunk Customer
- **Apps:**
  - **Splunk Security Essentials**
  - SplunkJS For All
  - Search Activity
  - Newsletter
  - Three more

- **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

splunk> .conf18

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

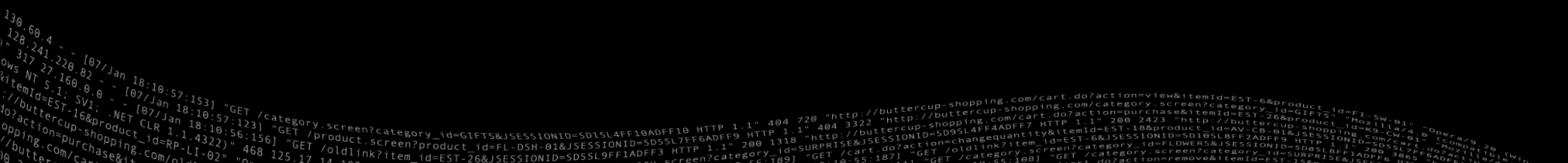
Goal for Security Essentials and this Talk

- 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?

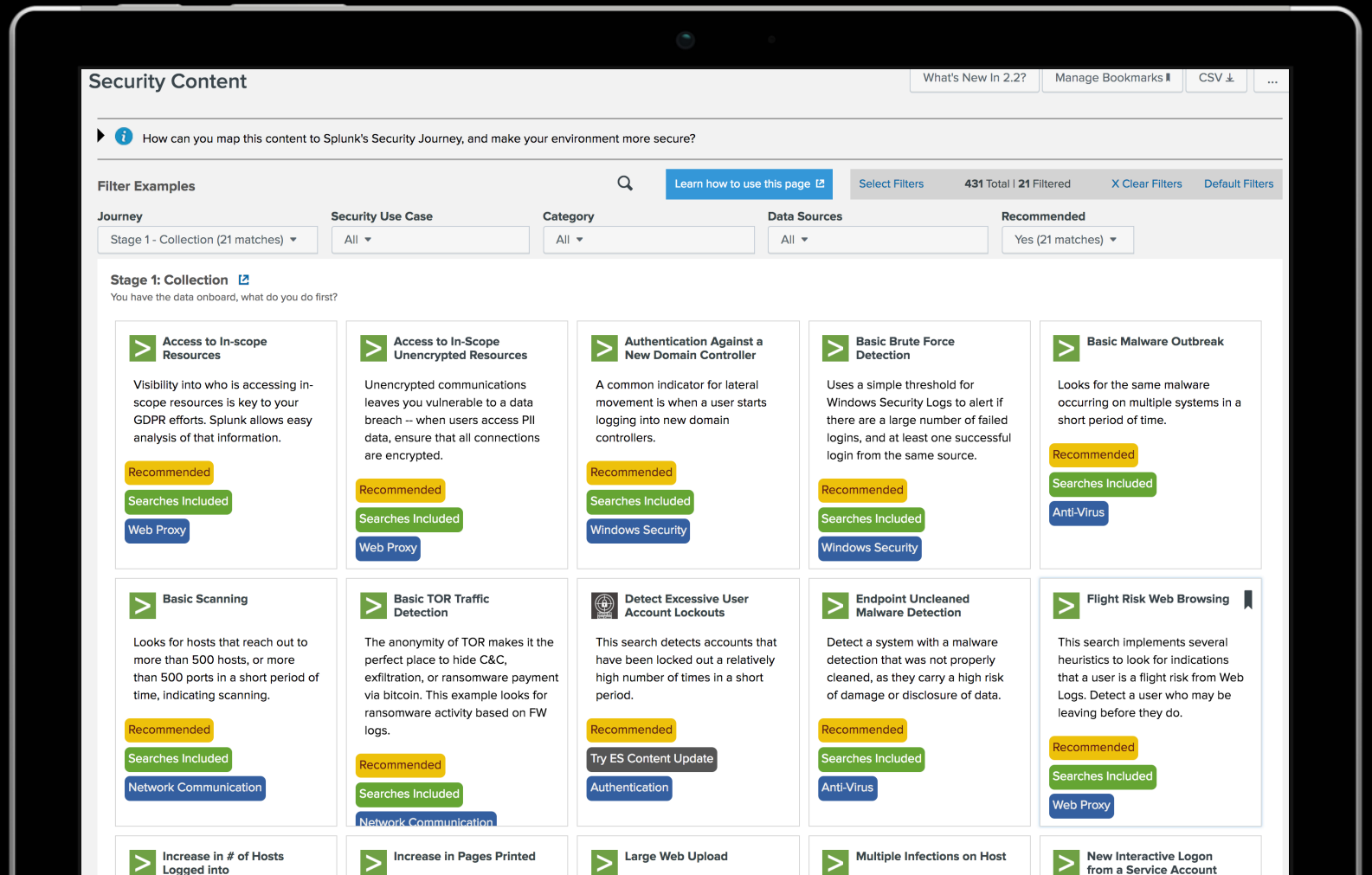
Get The App

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



splunk> .conf18

125+ Examples, with 180+ Searches

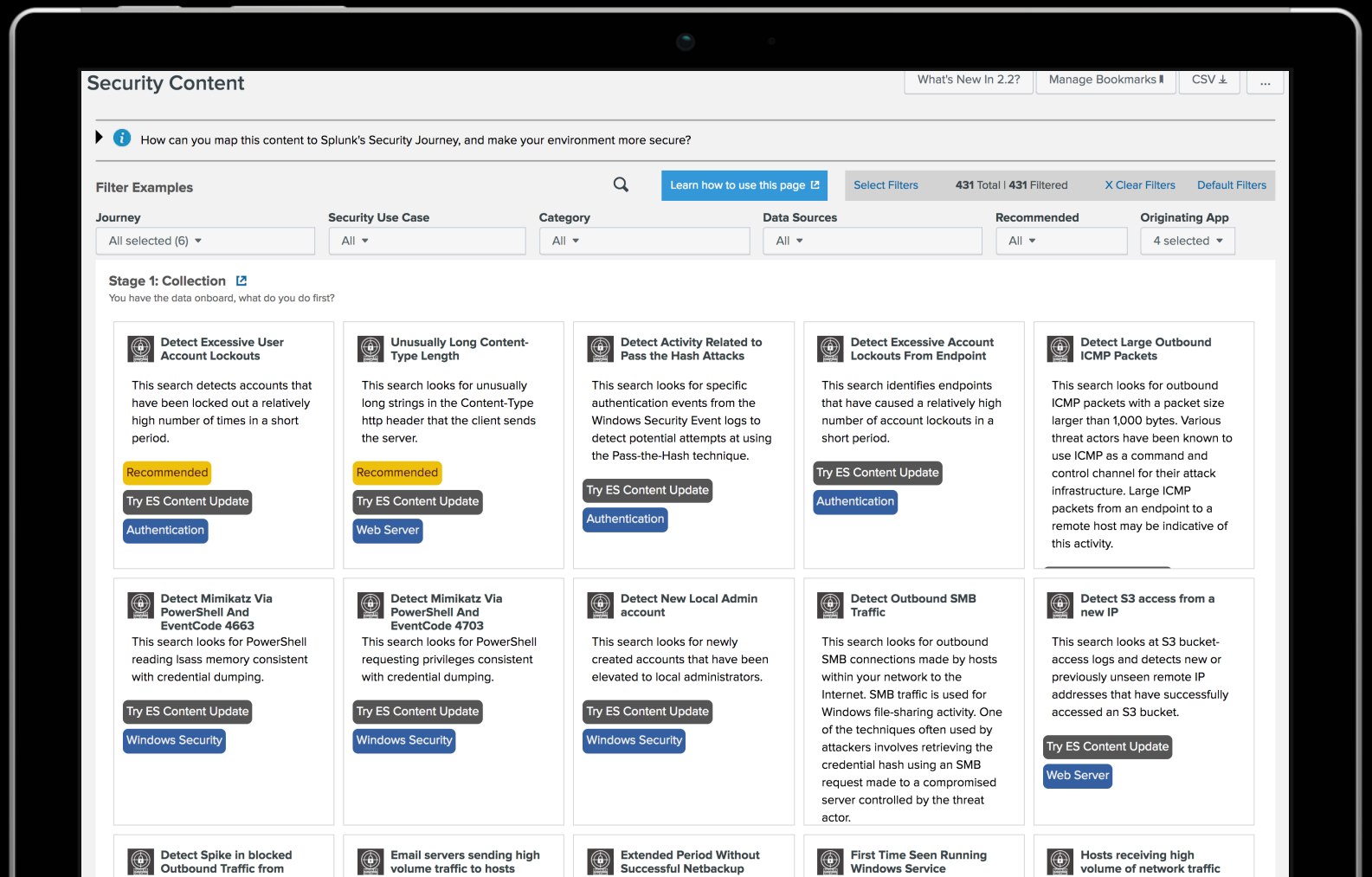


Each includes:

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

splunk> .conf18

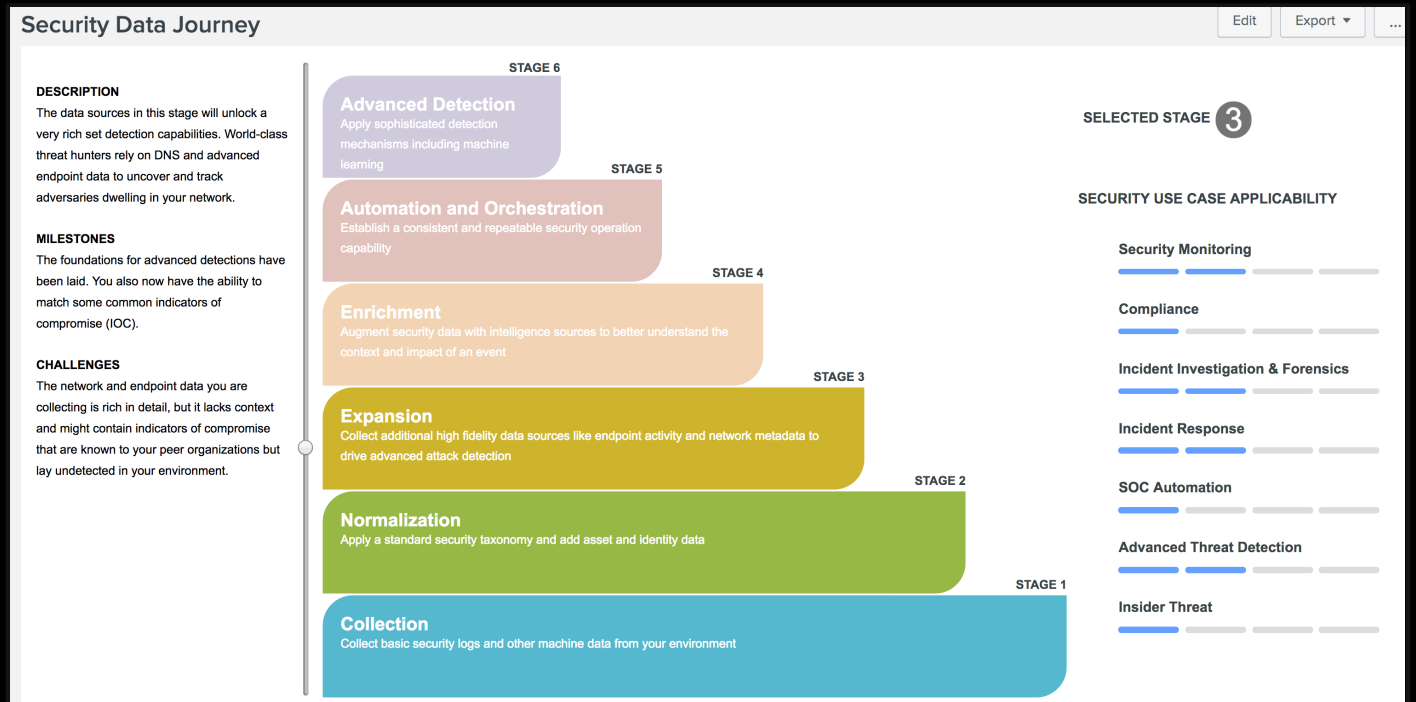
Mapping of 300+ Detections from Premium Apps



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

splunk> .conf18

Splunk Security Data Journey



Each Stage Includes:

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

splunk> .conf18

What's New – SSE 2.0?

February 2018 Was a Big Release…

splunk> .conf18

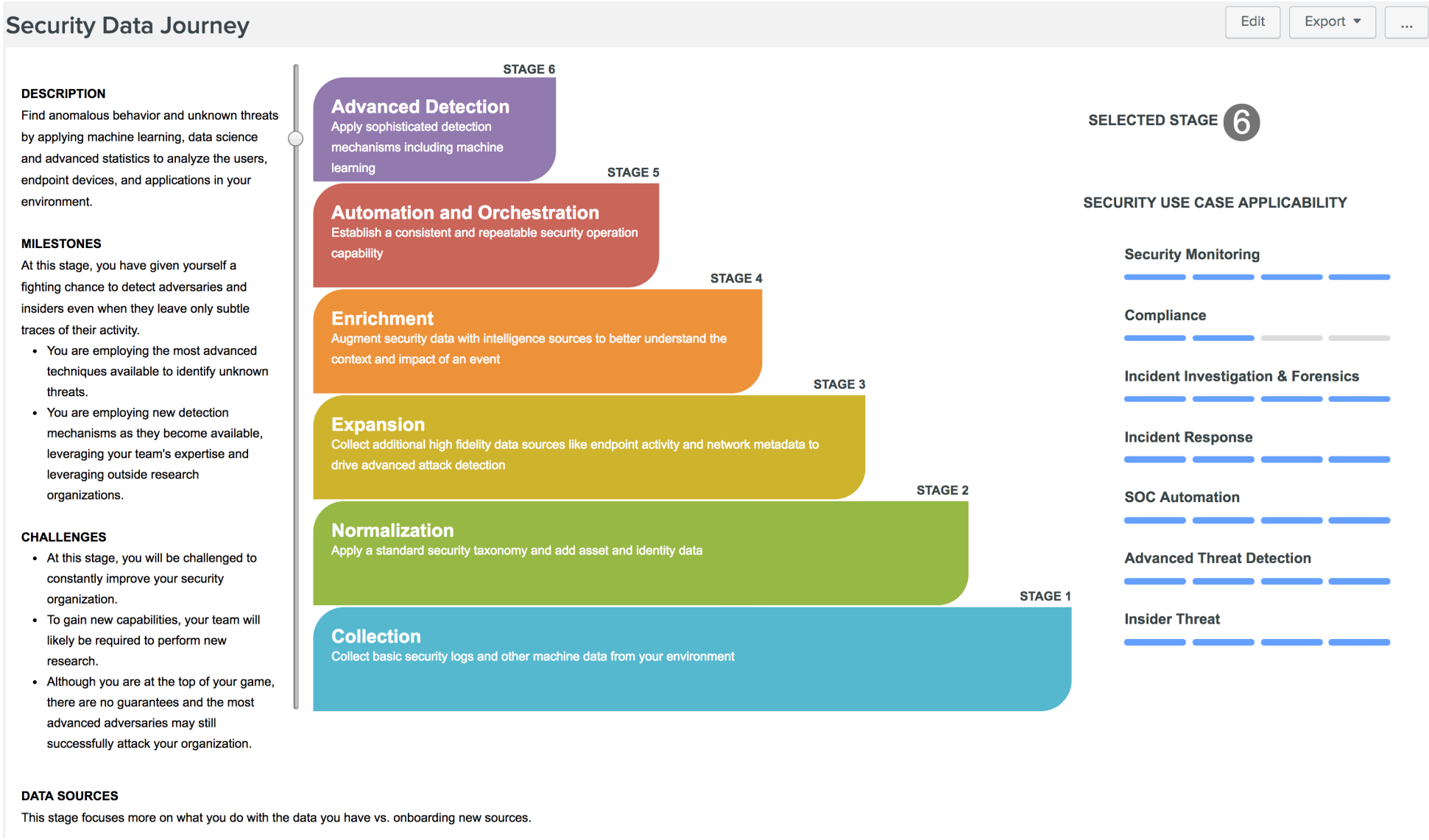
2.0 Major Features

- 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



splunk> .conf18

GDPR Content

Stage 4: Enrichment

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

Brute Force Access Behavior Detected - Against Category

Monitor your security controls and prove your GDPR compliance by detecting brute force (or password guessing) attacks on GDPR-tagged systems.

Recommended
Searches Included
Authentication
Windows Security

Excessive DNS Failures

Alerts when a host receives many DNS failures in a short span

Try Splunk ES
DNS

Expected Host Not Reporting - in Category

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.

Recommended
Searches Included
Any Host Logs

Geographically Improbable Access Detected against Category

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.

Recommended

In-Scope Device with Outdated Anti-Malware Found

Alerts when a GDPR-tagged system has out of date malware definitions, which would conflict with GDPR's requirement to maintain a secure environment.

Recommended
Searches Included
Anti-Virus

In-Scope System with Windows Update Disabled

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.

Recommended
Searches Included

New Connection to In-Scope Device

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.

Recommended
Searches Included

User Has Access to In-Scope Splunk Indexes They Should Not

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.

Recommended
Searches Included

User Logged into In-Scope System They Should Not Have

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.

Recommended

Activity from Expired User Identity - on Category

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

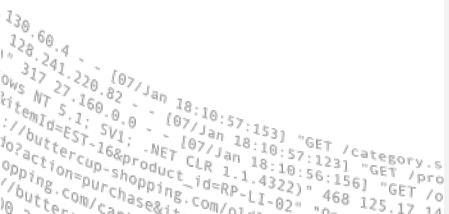
Searches Included
Authentication
Windows Security

Brute Force Access Behavior Detected Over One Day - Aga...

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.

Searches Included
Authentication
Windows Security

Stage 5: Automation and Orchestration



splunk> .conf18

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

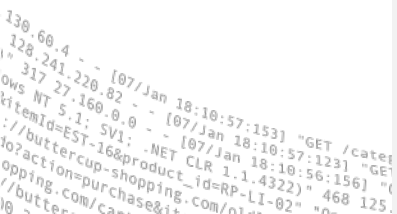
Stage 4: Enrichment

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



splunk> .conf18

Data Onboarding Guide


```
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

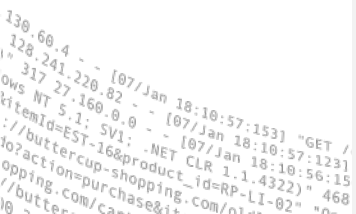
To maintain a good Security Posture, and to leverage the examples provided in Splunk Security Essentials, we recommend following Microsoft's official guidance for "Stronger" security visibility. The Audit Policy Recommendations page from Microsoft TechNet provides very detailed configuration settings 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

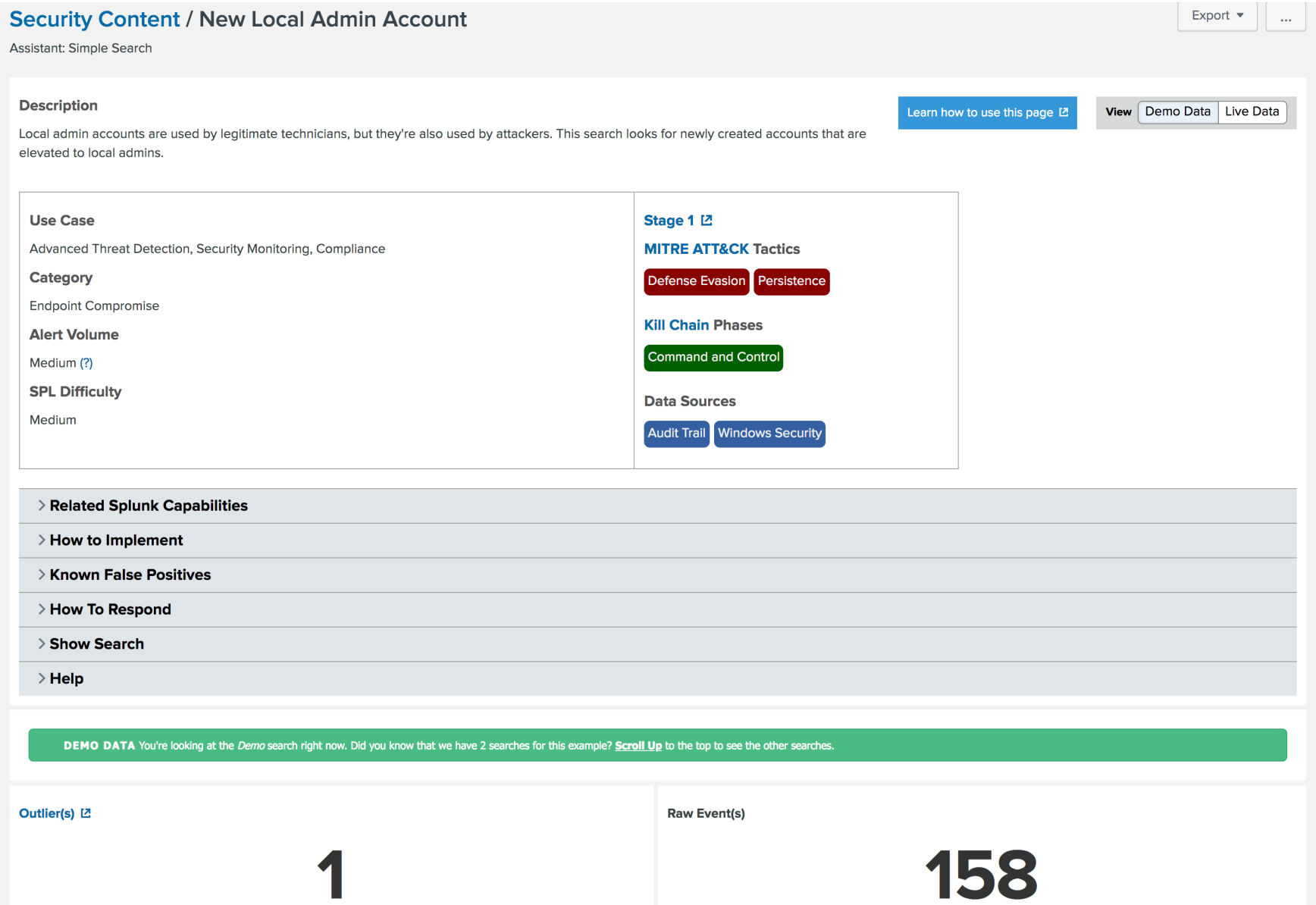
Important Note: Splunk is a monitoring product, and not an Active Directory system, so while we're working hard to centralize some of the recommendations you should follow in one place to make your life easy, we cannot offer support for the actual configuration of anything other than Splunk itself, and 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



splunk> .conf18

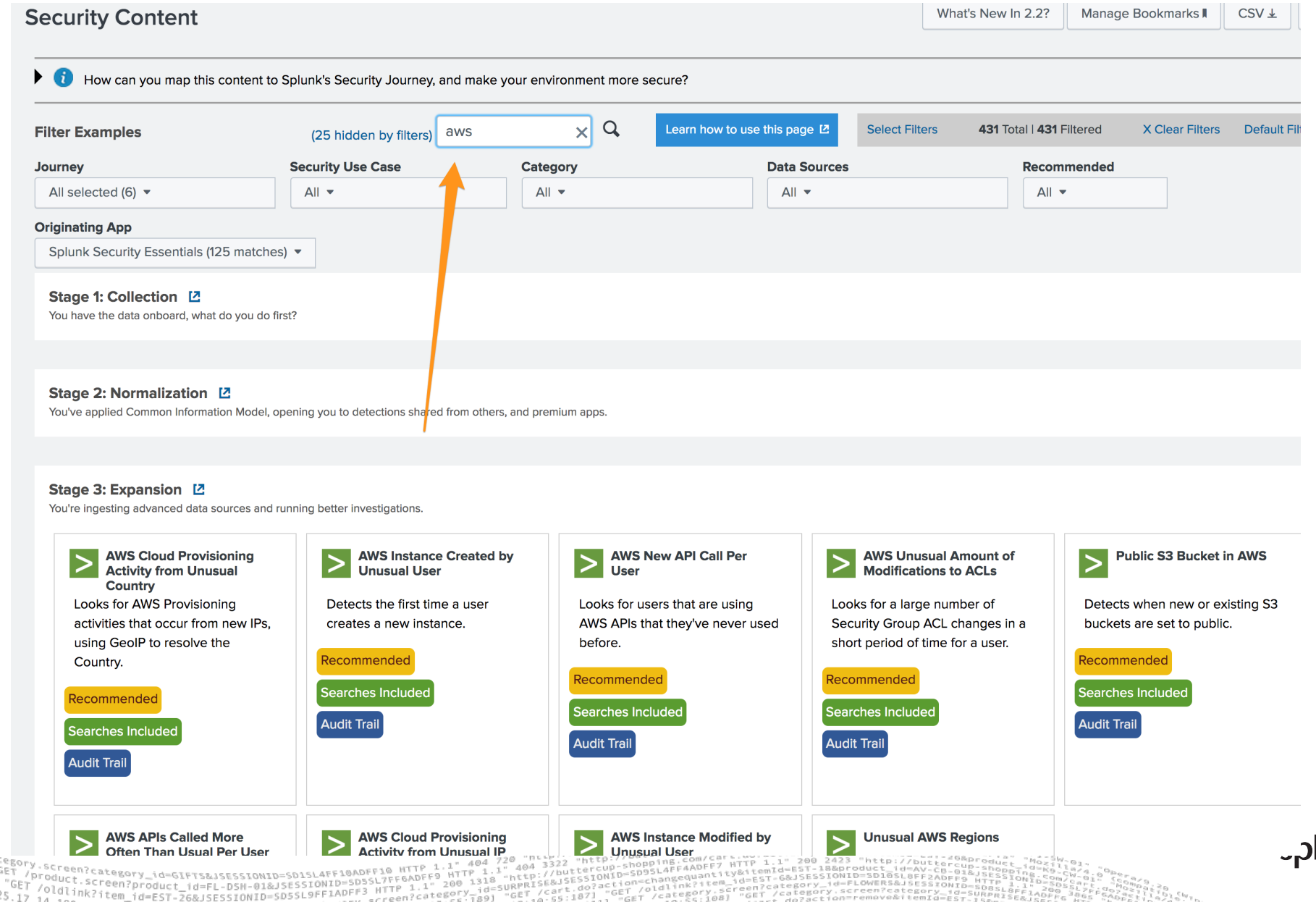
New Functionality Since 2.0

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

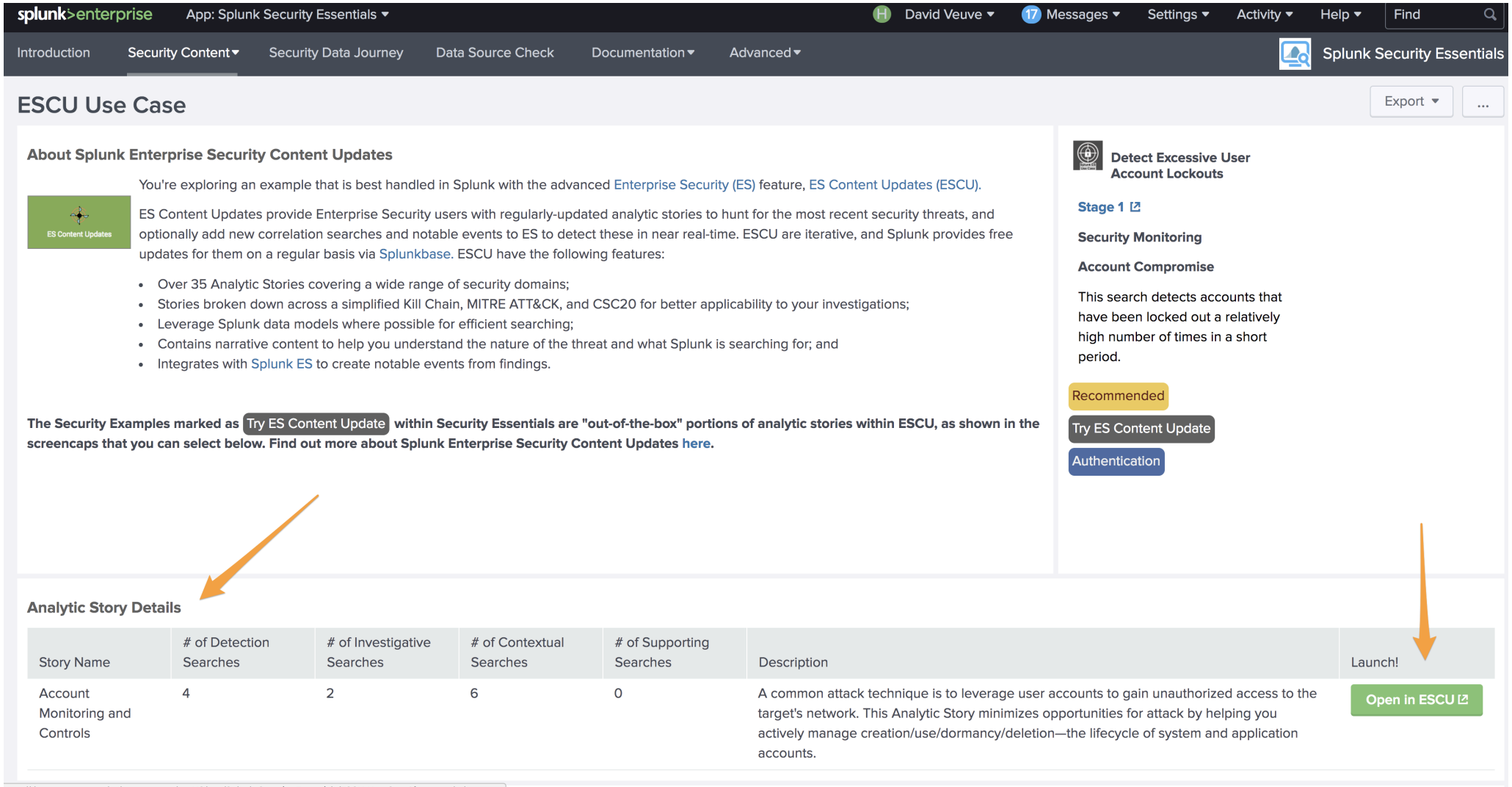


splunk> .conf18

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



Support for Windows TA

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

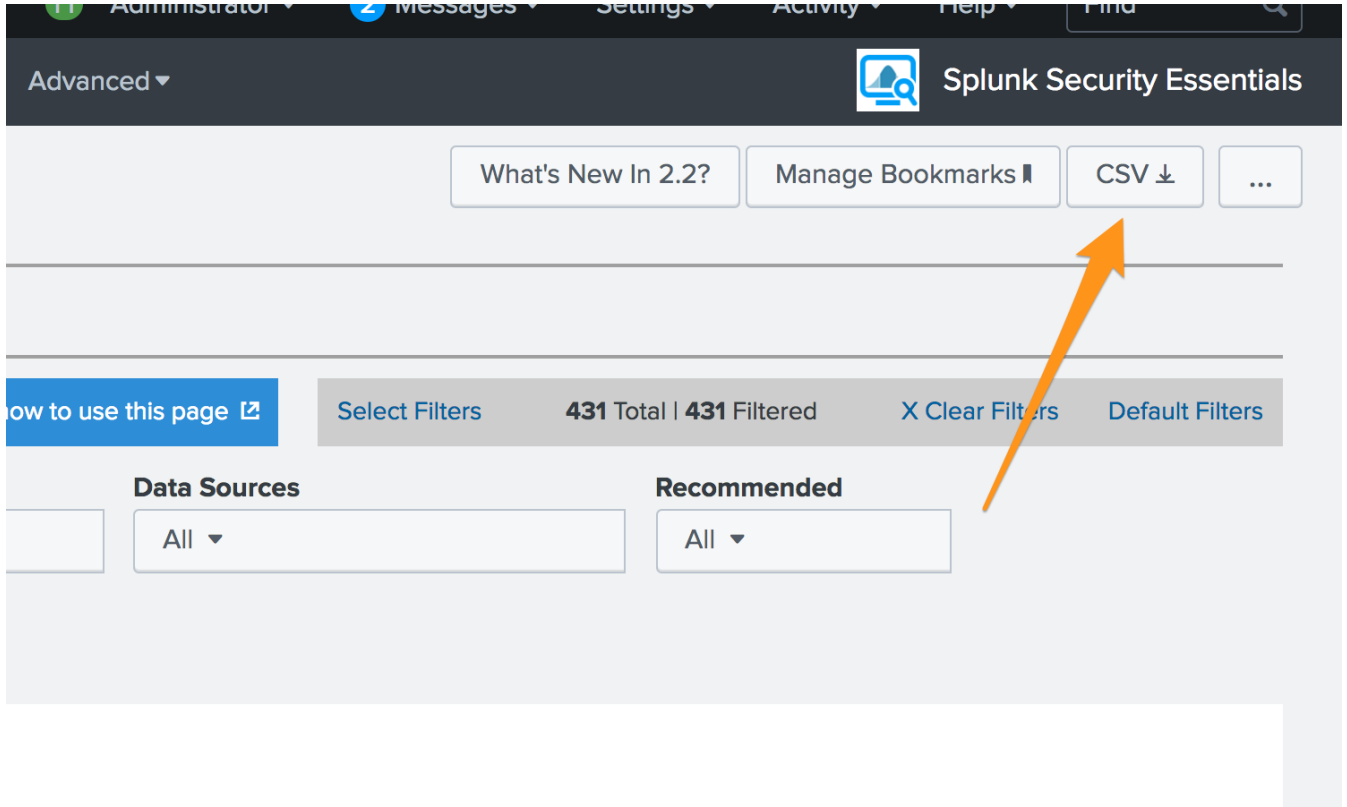
splunk> .conf18

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

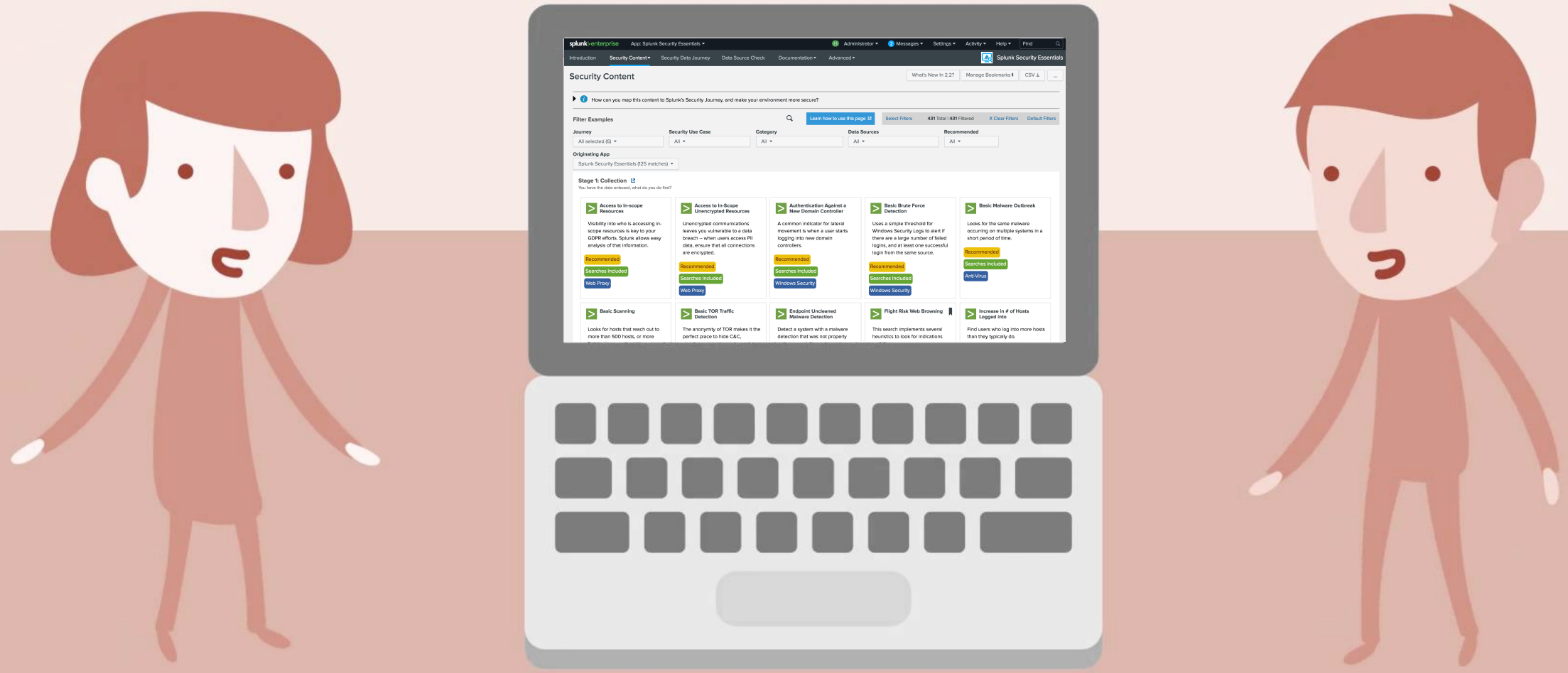
- Check out this video of it: https://youtu.be/W5KCn-zieDg

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



… 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

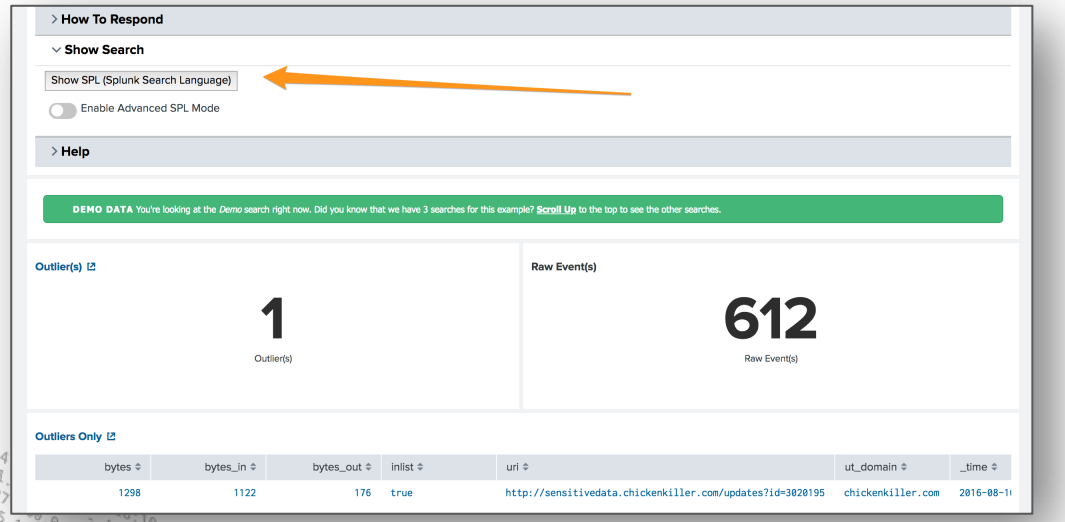
splunk> .conf18

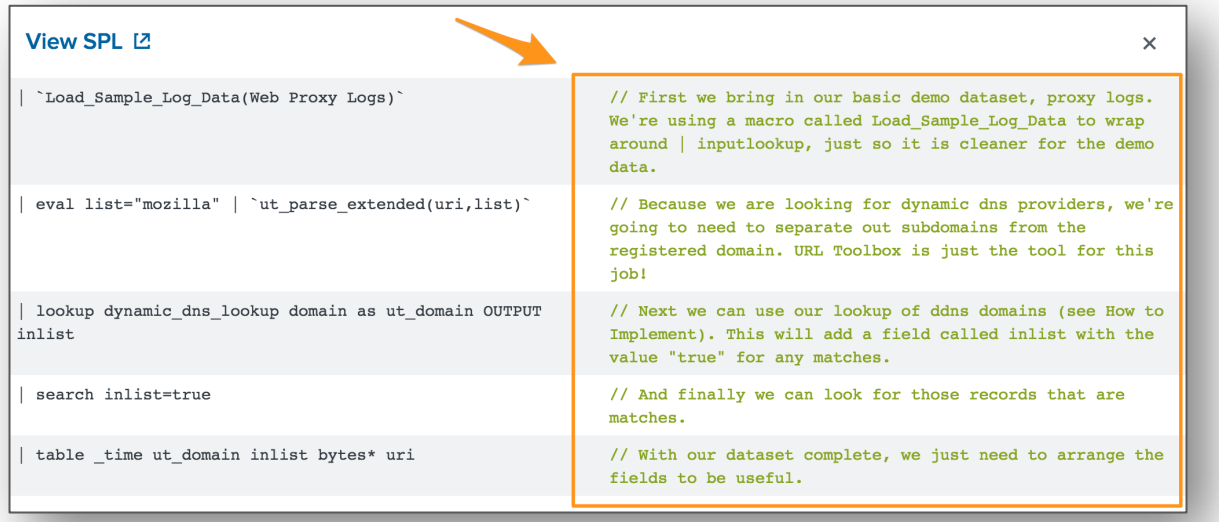
Most Underused Functionality

splunk> .conf18

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!





splunk> .conf18

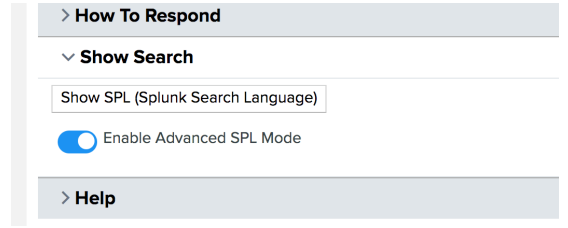
Lookup Cache on First Time Seen

- 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

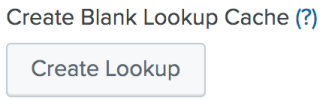
(all rough numbers)

- 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.

1.

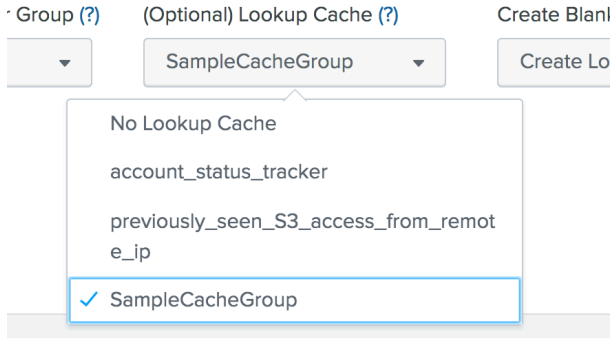


1.5.



(optional)

2.

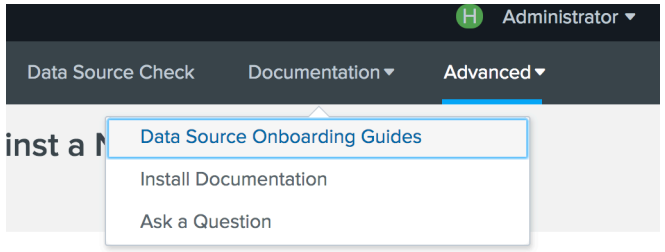


splunk> .conf18

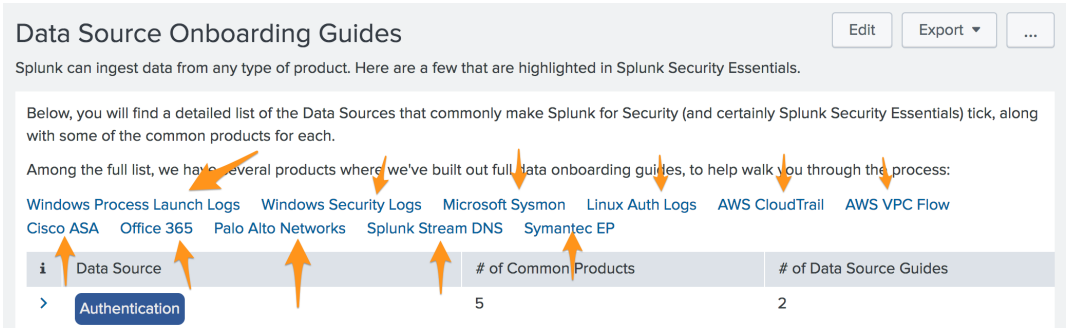
Data Onboarding Guides

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

1.



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

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 Miigating 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