THE ESSENTIAL GUIDE TO SECURITY

How to Get Started Using the Splunk Platform to Solve Security Challenges

splunk>

WHAT'S YOUR PLAN FOR CYBERSECURITY?

Table of Contents

Introduction 4

Splunk's Analytics-Driven Security Journey 8

Splunk's Security Use Cases 9

Getting Specific 10

The Security Use Cases Defined 11

Splunk's Analytics-Driven Security Journey: How to Get Started 13

Stage 1: Collection 14

Stage 2: Normalization 18

Stage 3: Expansion 20

Stage 4: Enrichment 24

Stage 5: Automation and Orchestration 26

Stage 6: Advanced Detection 28

How to Solve Security Use Cases Using Splunk: Examples 30

- Security Monitoring 31
  - 1) Public S3 Bucket in AWS 31
  - 2) Multiple Infections on Host 33
- Advanced Threat Detection 36
  - 1) Connection to New Domains 36
  - 2) Emails With Lookalike Domains 39
- Compliance 42
  - 1) New Local Admin Account 42
  - 2) User Logged Into In-Scope System They Should Not Have 44
- Fraud Detection 48
  - 1) Detect Compromised User Accounts 48
  - 2) Find Anomalous Healthcare Providers 50
- Insider Threat 52
  - 1) Large Web Upload 52
  - 2) Successful Login of Account for Former Employee 55

ARE YOU SIMPLY "PLANNING FOR THE WORST, BUT HOPING FOR THE BEST?"

With digital technology touching every part of our lives and new threats popping up daily, it is imperative that your organization is precise, informed, and prepared when it comes to defending your assets and hunting your adversaries.

Recent high-profile breaches, global ransomware attacks and the scourge of cryptomining are good enough reasons why your organization needs to collect the right data. You also need to implement the right processes and procedures early on, often alongside new technologies, and with an ever-increasing velocity and variability of machine data.

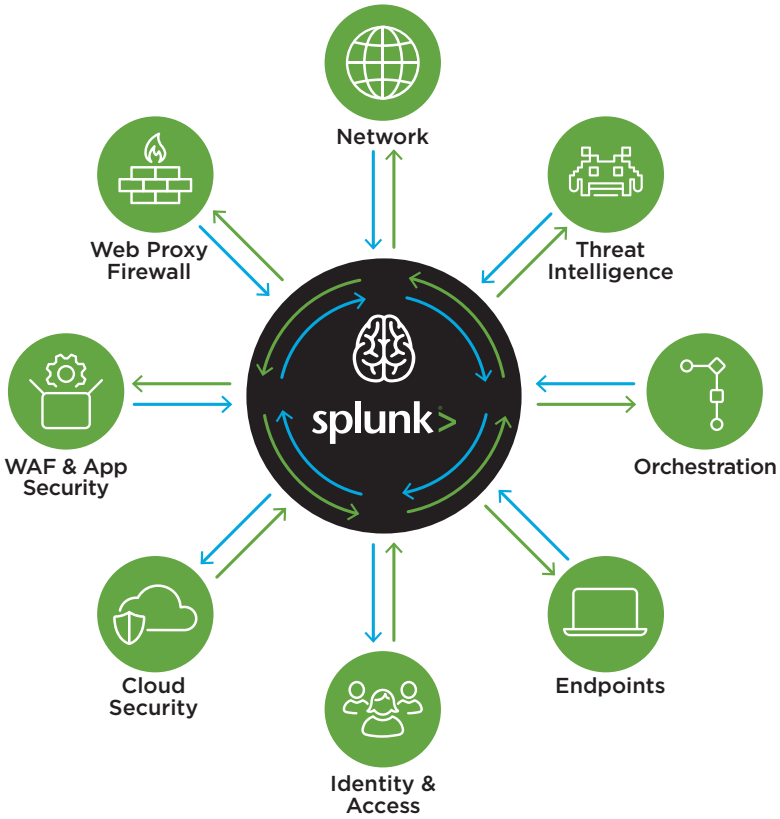
So how can you best defend your organization and hunt down new adversaries? Ultimately, by taking a holistic approach to your defense system across the enterprise. This is why Splunk believes every organization needs a security nerve center, implemented by following a six-stage **Security Journey** that we will describe for you.

Let's break down what that means.

Organizations optimize their people, process and technology around security with a nerve center. The Splunk platform acts as this nerve center by bringing multiple cybersecurity areas, and others outside of security, together to foster collaboration and implement best practices for interacting with your data. From there, the platform allows for modern workflow, all the way to invoking actions to address cyberthreats and challenges.

Splunk's Security Portfolio	
Splunk Enterprise	Monitors and analyzes machine data from any source to deliver Operational Intelligence to optimize IT, security and business performance.
Splunk Enterprise Security	A SIEM that provides insight into machine data generated from security technologies such as network, endpoint, access, malware, vulnerability and identity information.
Splunk UBA	A machine learning-powered solution that delivers answers organizations need to find unknown threats and anomalous behavior across users, endpoint devices and applications.
Apps	Developed by Splunk, our partners and our community to enhance and extend the power of the Splunk platform. The Splunk App for PCI Compliance is an example.
Essentials	Splunk developed apps that show users how to solve a use case. Splunk Security Essentials is one example.
Insights	Targeted Splunk developed apps featuring a use-case-specific licensing model that enables smaller organizations to ingest and analyze event logs from data sources to see all aspects of the environment as pertinent to a specific use case.

Security teams can use Splunk software to drive statistical, visual, behavioral and exploratory analytics that inform and execute insights, decisions and actions.



Splunk Enterprise Security includes a common framework for interacting with data and invoking actions. The Adaptive Response framework enables security teams to quickly and confidently apply changes to the environment. Splunk Enterprise Security can automate the response as well, enabling the security infrastructure to adapt to the attacker using a range of actions appropriate to each domain.

THE NERVE CENTER MODEL

includes using all the data from the security technology stack, which can help you investigate, detect, understand and take rapid, coordinated action against threats in a manual, semi-automated or automated fashion. Establishing a nerve center allows organizations to advance their security and focus on the real challenges within. When teams invest in their security infrastructure, their security ecosystem and skills become stronger, making it possible to expand into new areas, proactively deal with threats and stay ahead of the curve.

Sound good?

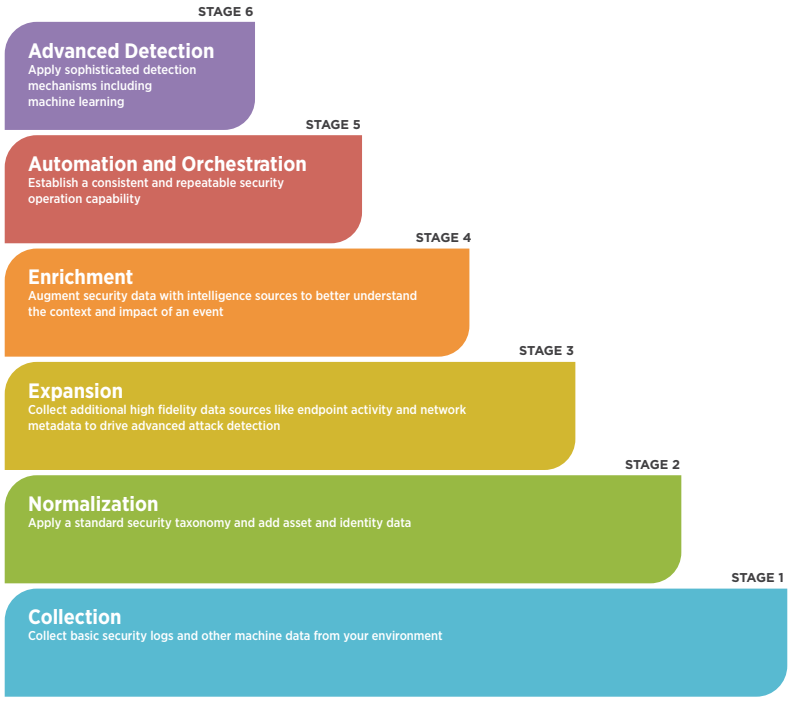
Great. So how do I make all of this happen in the real world, you ask?

First, you must understand your environment and find a place to begin. Ask yourself: what are you trying to protect? How will you protect it? What data do you need and how will you respond to the threats?

WANT US TO SHOW YOU HOW TO GET STARTED? SURE.

We've put together this short book to introduce you to the top security use cases organizations face. We've also outlined and mapped them into a six-stage security "data journey" that will help you create a kick-ass security practice. Take a look:

Splunk's Analytics-Driven Security Journey



Next, you will find the specific security use cases we've mapped to the journey. Go ahead. Choose your own adventure, or security challenge. The purpose of this book is to teach you how Splunk's analytics-driven platform can help solve your security challenges and advance your security journey, including:

Mapping Splunk With the Security Use Cases

Use Case	Splunk Solution
Security Monitoring	*Essentials,* SIEM, Enterprise
Advanced Threat Detection	*Essentials,* UBA, ES, Enterprise
Compliance	*Essentials,* PCI, Enterprise, ES
Fraud Detection	*Essentials,* Enterprise
Insider Threat	*Essentials,* UBA
Incident Investigation & Forensics	Enterprise, ES
SOC Automation	ES, Enterprise
Incident Response	ES, Enterprise

In this book, we will focus on solving common challenges around security monitoring, advanced threat detection, compliance, fraud and insider threat.

GETTING SPECIFIC

We will walk you through examples of how to solve common security challenges associated with some of these use cases. Each one detailing:

- Security Impact
- Security Data Journey Stage
- Data Sources Required
- SPL Difficulty
- Splunk Solution Required
- How to Implement
- Known False Positives
- How to Respond
- Searches
- Help

The Security Use Cases Defined

First, a quick primer on the use cases so we are all on the same page.

Security Monitoring

Security monitoring enables you to analyze a continuous stream of near real-time snapshots of the state of risk to your security data, the network, endpoints, as well as cloud devices, systems and applications. The Splunk platform enables security teams to detect and prioritize threats found in the stream of data from these sources.

Advanced Threat Detection

An advanced persistent threat (APT) is a set of stealthy and continuous computer-hacking processes, often orchestrated by a person or persons targeting a specific entity. APTs usually target either private organizations and states for business or political motives.

Splunk Enterprise enables organizations to search and correlate their data to track advanced threats. Splunk Enterprise Security (ES) and Splunk User Behavior Analytics (UBA) elevate existing capabilities to apply a kill chain methodology through statistical analysis, anomaly detection, and machine learning techniques to detect unknown and advanced threats.

Compliance

In nearly all environments, there are regulatory requirements in one form or another – especially when dealing with the likes of GDPR, HIPAA, PCI, SOC, and even common guidelines that aren't considered true compliance, like the 20 CIS Critical Security Controls. There are many ways of solving compliance challenges with Splunk. One example is the use of the Splunk platform to create correlation rules and reports that identify threats to sensitive data or key employees, as well as to automatically demonstrate compliance.

Fraud Detection

It's important to understand that machine data is at the heart of detecting fraudulent activities in the digital age. Splunk can onboard new data so that fraud teams are better able to detect and investigate anomalies. As a result, companies reduce financial loss, protect their reputation and maintain efficiency.

Insider Threat

Insider threats come from current or former employees, contractors or partners who have access to the corporate network and intentionally or accidentally exfiltrate, misuse or destroy sensitive data. They often have legitimate access to networks and permission to download sensitive material, easily evading traditional security products. The Splunk platform gives security teams the ability to detect and prioritize threats posed by insiders and compromised insiders that would have otherwise gone undiscovered.

Incident Investigation and Forensics

Security incidents can occur without warning and can often go undetected long enough to pose a serious threat to an organization. Investigations can be challenging and time-consuming. Usually by the time security teams are aware of an issue, there's a good chance the damage has been done. Splunk provides security teams with a "single source of truth" for all time stamped machine data in a computing environment. This helps them drive better, faster security investigations, reducing the chance of a threat going undetected for extended periods.

Incident Response

Organizations often work in silos in order to manage the response to malicious activities, incidents and breaches. And threats to the business can occur without detection, never becoming incidents. And of course, the threat landscape is dynamic and constantly evolving, making it difficult for security practitioners of all levels to keep up with the latest types of threats.

To help your incident responders handle the latest security threats, Splunk employs a security research team that provides customers of Splunk Enterprise Security with regular product content updates. This content allows customers to quickly assess their environments for threat indicators and behaviors so that overall response time is shortened.

SOC Automation

New threats are continuously emerging and evolving, making it a challenge for security teams to stay ahead of the game. Organizations can also lack the skills, experience and collaboration tools needed to quickly investigate and remediate threats. Security operations teams adopt Splunk software for detection, incident response solutions, threat intelligence, orchestration and automation to scale investigations, accelerate response and remediate advanced threats. The Splunk platform helps organizations operationalize analytics-driven security practices in their SOC to speed up investigations and automate responses.

Splunk's Analytics-Driven Security Journey: How to Get Started

Next we will explain the stages of the security journey and what you should be able to do, and how well, at each stage.

STAGE 1: **COLLECTION**

Collect basic security logs and other machine data from your environment.

SELECTED STAGE 1

SECURITY USE CASE APPLICABILITY

- **Security Monitoring**
- **Compliance**
- **Incident Investigation & Forensics**
- **Incident Response**
- **SOC Automation**
- **Advanced Threat Detection**
- **Insider Threat**

Description
This level focuses on the basics by collecting machine data generated by the foundational components of your security infrastructure.

Data Sources
At this stage, the best practice is to capture four primary categories of security data: network, endpoint (host-based), authentication and web activity.

Milestones
After successfully onboarding data from these four categories, you should have achieved the following:

- Moved critical activity logs to a separate system where they can't be easily tampered with by an attacker;
- Have the data necessary to perform basic investigations; and
- Have the raw materials to begin gaining a deeper understanding of the environment you must defend.

Challenges
This level focuses on the basics by collecting machine data generated by the foundational components of your security infrastructure.

1) Network
Visibility into network traffic is critical for any security team. At this early level, the priority is to see what types of traffic are entering and exiting your network. It's critical to see the traffic that's permitted as well as communication attempts that have been blocked.

Firewall traffic logs from devices from vendors like:

- Palo Alto Networks
- Cisco
- Checkpoint
- Fortinet

2) Endpoint
Endpoint logs complement network visibility to give insight into malicious activities such as malware execution, an insider performing unauthorized activity or an attacker dwelling in your network. It's important to capture this data from both servers and workstations as well as all operating systems (Windows, Linux, MacOS, etc.).

- Windows Event Logs
- Linux System Logs
- Linux Auditd
- MacOS System Logs

3) Authentication
Authentication logs can tell you when and from where users are accessing systems and applications. Since most successful attacks eventually include the use of valid credentials, this data is critical in helping to tell the difference between a valid login and an account takeover.

- Windows Active Directory
- Local Authentication
- Cloud Identity & Access Management (IAM)

4) Web Activity
Many attacks start with a user visiting a malicious website or end with valuable data being exfiltrated to a site that the attacker controls. Visibility into who's accessing what sites and when is critical for investigation.

Next generation firewall (NGFW) traffic filters or Proxy logs from vendors like:

- Palo Alto Networks
- Cisco
- Checkpoint
- Fortinet
- Bluecoat
- Websense

STAGE 2: **NORMALIZATION**

Apply a standard security taxonomy for asset and identity data.

SELECTED STAGE 2

SECURITY USE CASE APPLICABILITY

- **Security Monitoring**
- **Compliance**
- **Incident Investigation & Forensics**
- **Incident Response**
- **SOC Automation**
- **Advanced Threat Detection**
- **Insider Threat**

Description

This stage puts you in a position to begin implementing a security operations center to track systems and users on your network, and to consume a larger selection of detection mechanisms from vendors and the community. Even if you don't plan to stand up a formal SOC, normalized data will streamline investigations and improve the effectiveness of an analyst.

Data Sources

At this stage, you're ensuring your data is compliant with a standard security taxonomy. This means that fields representing common values such as the source IP address, port, username and so on, now have common names regardless of the device that created the event. This critical investment allows you to start consuming detection mechanisms from many sources, and to begin to scale the capabilities of your security team. It also allows for easier cross-source correlation.

Milestones

Data is mapped properly to the Common Information Model (CIM);

- Search performance is improved dramatically through the use of accelerated data models associated with CIM; and
- Asset and user details are correlated to events in your security log platform.

Challenges

Now that you have basic data that detections is searchable, you'll start to understand that some of the most effective security come from wire data and deeper endpoint visibility.

STAGE 3: **EXPANSION**

Collect additional high-fidelity data sources, like endpoint activity and network metadata to drive advanced attack detection.

SELECTED STAGE 3

SECURITY USE CASE APPLICABILITY

Security Monitoring

Compliance

Incident Investigation & Forensics

Incident Response

SOC Automation

Advanced Threat Detection

Insider Threat

Description

The data sources in this stage will unlock a very rich set of detection capabilities. World-class threat hunters rely on DNS and advanced endpoint data to uncover and track adversaries dwelling in the network.

Data Sources

Data sources at this stage include:

Network: Most threat hunters and cyberthreat intelligence analysts will tell you that if they could only have one data source for analysis, it would be DNS.

- Protocol-Specific Wire Data DNS DHCP

Endpoint: Rich endpoint activity that captures process creation, file changes, registry modifications, network connections provide an amazingly clear history of critical events occurring on an endpoint.

- Sysmon
- Osquery
- Carbon Black Defense

Milestones

- The foundation for advanced detections have been laid; and
- You also now have the ability to match some common indicators of compromise.

Challenges

The network and endpoint data you're collecting is rich in detail, however it lacks context and might contain indicators of compromise that are known to your peer organizations, but lay undetected in your environment.

Network

Most threat hunters and cyberthreat intelligence analysts will
tell you that if they could only have one data source for analysis, it would be DNS, but there are other network-related sources of data that are important:

- Protocol-Specific Wire Data from sources like Splunk Stream
  or Bro;
- DNS query-level data from debug-level logs or from wire
  data sources; and
- DHCP activity.

STAGE 4: **ENRICHMENT**

Augment security data with intelligence sources to better understand the context and impact of an event.

SELECTED STAGE 4

SECURITY USE CASE APPLICABILITY

- **Security Monitoring**
- **Compliance**
- **Incident Investigation & Forensics**
- **Incident Response**
- **SOC Automation**
- **Advanced Threat Detection**
- **Insider Threat**

Description

Machine data is important, but high-performing security teams enrich their data with other internal and external sources. A wealth of contextual and investigative knowledge including threat-intelligence feeds, open-source intelligence (OSINT) sources, and internally-sourced information allows your security personnel to extract more value from the data you are collecting to detect security events and incidents sooner.

Data Sources

- Local IP/URL block lists;
- Open-source threat intel feeds; and
- Commercial threat intel feeds.

Milestones

- You're able to understand the urgency of an alert based on the criticality of the asset; and
- Your team quickly augments alerts in your environment by matching them against threat-intelligence feeds, pivoting to other systems and initiating additional context gathering activities.

Challenges

You have significant detection capabilities, but your team is operating in an ad-hoc fashion or not considering the context of what they are seeing by correlating with information from outside of the business. Also, requests are not tracked, performance is not measured, collaboration is ad-hoc and lessons learned are not stored and leveraged for future use.

STAGE 5: **AUTOMATION AND ORCHESTRATION**

Establish a consistent and repeatable security operation capability.

SELECTED STAGE 5

SECURITY USE CASE APPLICABILITY

- **Security Monitoring**
- **Compliance**
- **Incident Investigation & Forensics**
- **Incident Response**
- **SOC Automation**
- **Advanced Threat Detection**
- **Insider Threat**

Description

Mature organizations are able to continuously monitor their environment for alerts and triage, as well as respond to threats in a consistent, repeatable and measurable way.

Data Sources

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

Milestones

- Ability to track incidents;
- Regular measurement of analyst effectiveness;
- Teams take action according to prescribed playbooks; and
- You can automate simple response actions and combine them together into more sophisticated orchestration.

Challenges

You have a functioning security organization and are ready to adopt the most advanced techniques to detect threats.

STAGE 6: **ADVANCED DETECTION**

Apply sophisticated detection mechanisms, including machine learning.

SELECTED STAGE 6

SECURITY USE CASE APPLICABILITY

- **Security Monitoring**
- **Compliance**
- **Incident Investigation & Forensics**
- **Incident Response**
- **SOC Automation**
- **Advanced Threat Detection**
- **Insider Threat**

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.

Data Sources

More granular data collection from your endpoints is critical for better adversary hunting.

Milestones

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

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

Challenges

At this stage, you'll be challenged to constantly improve your security organization and to gain new capabilities. Your team will also likely be required to perform new research. But by following the journey through to the end, you're at the top of your game. Although you will always be under attack, you have put yourself in the best position to detect and prevent many common and not-so-common threats to modern organizations.

Endpoint

Rich endpoint activity that captures process creation, file changes, registry modifications and network connections provide an amazingly clear history of critical events occurring on an endpoint. Some examples:

- Microsoft Sysmon
- Osquery
- Carbon Black Defense

HOW TO SOLVE SECURITY USE CASES USING SPLUNK: EXAMPLES

SECURITY MONITORING

1) Public S3 Bucket in AWS

Stage 1

Data Sources

Audit-Trail

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

Use Case
Security Monitoring, Advanced Threat Detection

Category
Data Exfiltration, SaaS, Compliance,
Privileged User Monitoring

Security Impact
Open S3 Buckets are an extremely common way for breaches to occur these days. People host files for quick transfer but forget to take them down, or use S3 Buckets for backups of sensitive data but inadvertently mess up permissions. Newly created S3 buckets are monitored and data is quickly pulled. If you have a corporate AWS environment, you should prioritize analyzing any open S3 buckets. You may even wish to automate the remediation of them through AWS functions.

Alert Volume
Very Low

SPL Difficulty
Medium

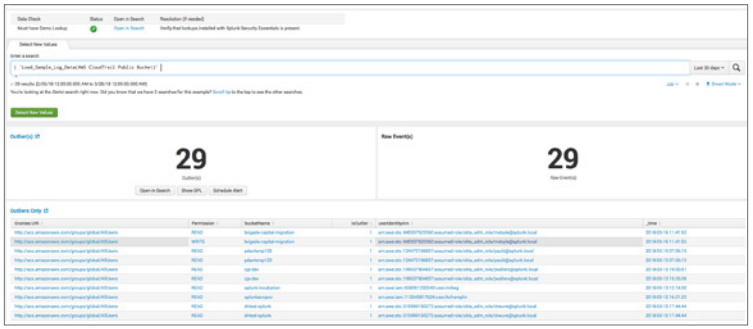
How to Implement
Assuming you use the ubiquitous AWS Add-on for Splunk to pull these logs in, this search should work automatically for you without issue. While implementing, make sure you follow the best practice of specifying the index for your data.

Known False Positives
There are two types of undesired alerts that can occur from this search. One is when someone intentionally creates a public bucket -- you may wish to whitelist marketing employees that do this on a regular basis, or create a policy for how to create a public bucket, so that you can exclude it. The other is when someone creates a bucket that is public momentarily, but then they switch it back to private.

How to Respond
When this alert fires, there are three questions that should be asked -- is it still public, are the files public, and what is in it. The first is easy to detect -- just search your logs for the bucket name and PutBucketACL, you will see any subsequent ACL changes. The second and third are trickier, and require that server access logging is turned on for the S3 bucket (not done by default, and pretty inconvenient, so don't bet on it).

How Does This Detection Work?
This search assistant runs standard Splunk searches -- read below for the particulars on this detection.

Public S3 Bucket in AWS Help
This example leverages the Simple Search Assistant. Our example dataset is a collection of anonymized AWS CloudTrail logs, where someone creates a public bucket. Our live search looks for the same behavior using the very standardized index and sourcetype for AWS CloudTrail, as detailed in How to Implement.



2) Multiple Infections on Host

Stage 1

Data Sources

Anti-Virus

Description
Finds hosts that have logged multiple different infections in a short period of time.

Use Case
Security Monitoring

Category
Endpoint Compromise

Security Impact
Viruses happen, but multiple viruses at once are a greater concern, as it could indicate an exploit kit that tries several techniques where some might succeed, or just a host with multiple unrelated viruses. Those hosts should be prioritized and investigated immediately to see what else might not have been caught.

Alert Volume
Low

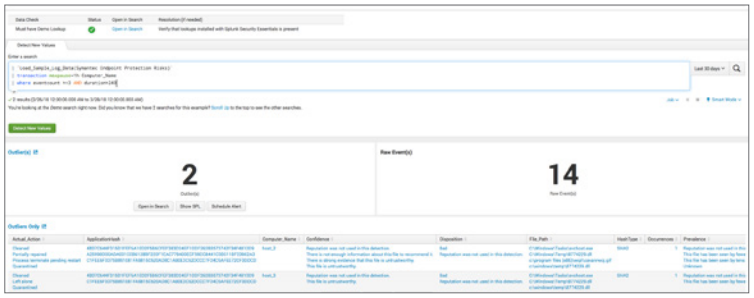
SPL Difficulty
Basic

How to Implement
With Symantec logs onboard, these searches should work easily. If you have a different Anti-Virus product, they should be very easy to adapt to the field names and sourcetypes for that product -- particularly if you use a Splunk Add-on that maps them to the Common Information Model (search on Splunkbase!).

Known False Positives
No known false positives.

How to Respond
When multiple infections occur to the same host, your response plan should be the same as any malware event, just with greater urgency.

Show Search



Help
How Does This Detection Work?
This search assistant runs standard Splunk searches -- read below for the particulars on this detection.

Multiple Infections on Host Help
This example leverages the Simple Search search assistant. Our example dataset is a collection of anonymized Symantec Endpoint Protection logs (onboarded in accordance with our Data Onboarding Guides), during which someone does something bad. Our live search looks for the same behavior using the standardized sourcetypes for Symantec Endpoint Protection or the Common Information Model.

ADVANCED THREAT DETECTION

1) Connection to New Domain

Stage 2

Data Sources

Web Proxy | DNS Resolver Logs

Description
Detects when users browse to domains never before seen in your organization.

Use Case
Advanced Threat Detection

Category
Command and Control, Data Exfiltration

Security Impact
Savvy Threat Hunters always know when users browse to new domains. This can be relevant in a variety of scenario, but the primary is that when your system connects to a command and control server, or to a staging server containing malware, those are usually on unusual domains. If you believe that a host is infected, checking to see whether it hit new domains is a great indicator to check. For more information on this detection in general, check out the great blog post specifically about this detection by Splunk's own Andrew Dauria.

Alert Volume
Very High

SPL Difficulty
Medium

How to Implement
Implementing this search is relatively straightforward, as it expects Common Information Model compliant data. Just ingest your proxy data (or other web browsing visibility, such as stream:http or bro), and make sure there is a uri field. The only other step is to make sure that you have the URL Toolbox app installed, which allows us to parse out the domains. When scaling this search to greater volumes of data (or more frequent runs), leverage acceleration capabilities.

Known False Positives
This search will inherently be very noisy. As a percentage of total domains, in most organizations new domains are very small. If you sent all of these events to the analysts though, it would be overwhelming. As a result, there are no known false positives per say, but value of any given alert is so small that you want to treat these alerts differently from most correlation searches. These are mostly appropriate just for contextual data, or to correlate with other indicators.

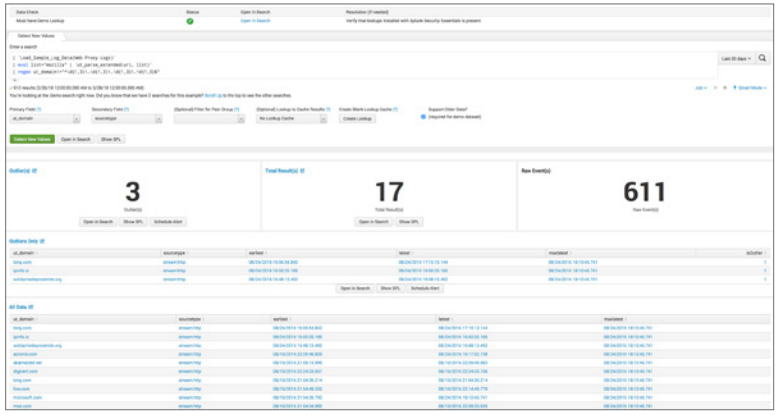
How to Respond
These events are generally best to look at as contextual data for another event, for example uncleaned malware, new services, or unusual logins. The easiest way to accomplish this is to just record the events in a summary index, and then include searching that index as a part of your investigative actions. Enterprise Security customers can do this easily with the Risk Framework, which is effectively that -- create a risk indicator adaptive response action when saving this search, and it will then adjust the risk score of the assets involved, and show up in investigator workbench when you analyze

an asset. Ultimately, to analyze the efficacy of any given alert here, we recommend looking up the domains in an Open Source Intelligence source like VirusTotal, ThreatCrowd, etc.

How Does This Detection Work

This method of anomaly detection tracks the earliest and latest time for any arbitrary set of values (such as the first logon per user + server combination, or first view per code repository + user combination, or first windows event ID indicating a USB Key usage per system). With normal usage, you'd check to see if the latest value is within the last 24 hours and alert if that's the case (with our demo data, rather than comparing to right now() we compare to the largest value of latest()). This is a major feature of many Security Data Science tools on the market (though not Splunk UBA) that you can get easily with Splunk Enterprise.

Connection to New Domain Help



This example leverages the First Seen Assistant. Our example dataset is a collection of anonymized Proxy logs, where browses to a new website. Our live search looks for the same behavior, as detailed in How to Implement.

2) Emails With Lookalike Domains

Stage 4

Kill Chain Phases

Delivery

Data Sources

Email Delivery

Description

Emailing from a domain name that is similar to your own is a common phishing technique, such as splunk.com receiving an email from spiunk.com. This search will detect those similar domains.

Use Case

Advanced Threat Detection

Category

Endpoint Compromise, SaaS

Alert Volume

Very Low

SPL Difficulty

Advanced

How to Implement

Implementing this search is generally fairly straightforward. If you have CIM compliant data onboarded, it should work out of the box, however you are always better off specifying the index and sourcetype of your email data (think particularly when you have multiple email log sources, such as a perimeter ESA and a core Exchange environment). If you have the right index,

sourcetype, you have the src_user field, and you've installed the URL Toolbox app, it should work like a charm.

Known False Positives

This search will through incoming emails for any domains similar to your domain names, much like running dnstwist on a domain name. If there are any incoming emails with source domain names that are very similar to but not the same, they would create alerts which could be false positives. One might imagine a scenario where a company who manufactures wooden planks for pirate ships, plank.com, emails their sales rep at splunk.com. That would create a difference of 2 (u->a, extra s) and would be flagged (Arrrr!). Known examples of this could be filtered out in the search, or you could pipe this into a First Time Seen detection to automatically remove past examples.

How to Respond

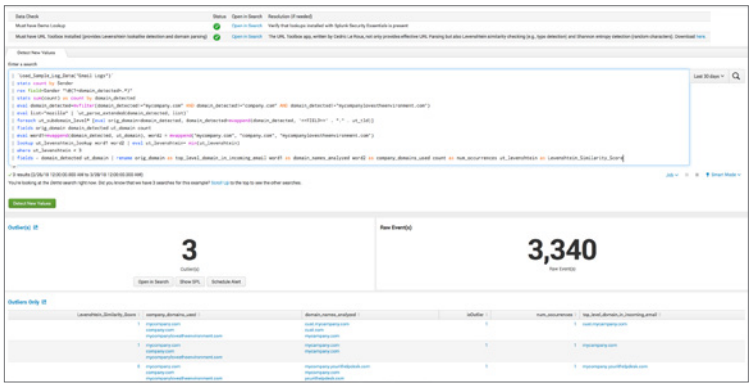
When this search returns values, initiate your incident response process and capture the time of the event, the sender, recipient, subject or the mail and attachments, if any. Contact the sender. If it is authorized behavior, document that this is authorized and by whom. If not, the user credentials may have been used by another party and additional investigation is warranted.

How Does This Detection Work?

This search assistant runs standard Splunk searches — read on for the particulars on this detection.

Emails With Lookalike Domains Help

This example leverages the Simple Search assistant. Our dataset is an anonymized collection of email logs centered around a particular user for a month.



COMPLIANCE

1) New Local Admin Account

Stage 1

MITRE ATT&CK Tactics

Defense Evasion | Persistence

Kill Chain Phases

Command and Control

Data Sources

Audit Trail | Windows Security

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

How to Implement
First, verify that you have Windows Security Logs coming in, and that you have implemented account change auditing (see the Windows Security data source documentation). Once your logs are coming in, you should be able to search for sourcetype="WinEventLog:Security" EventCode=4720 OR EventCode=4732 to see account creation or change events. Finally, make sure that your local admin group name is "administrators" so that we are looking for the right group membership changes.

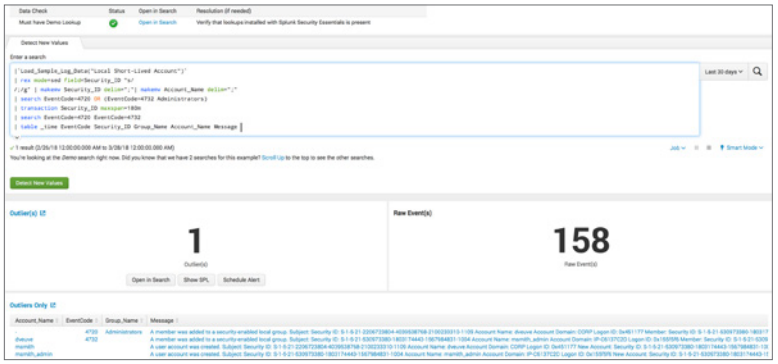
Known False Positives
The only real source of false positives for this search would be for help desk admins who create local admin accounts. If this is common practice in your environment, you should filter out their admin account creation messages by excluding their usernames from the base search. If your local admin group doesn't include the term "administrators" then it would potentially generate false negatives.

How to Respond
When this search returns values, initiate your incident response process and capture the time of the creation, as well as the user accounts that created the account and the account name itself, the system that initiated the request and other pertinent information. Contact the owner of the system. If it is authorized behavior, document that this is authorized and by whom. If not, the user credentials have been used by another party and additional investigation is warranted.

How Does This Detection Work?
This search assistant runs standard Splunk searches -- read below for the particulars on this detection.

New Local Admin Account Help
This example leverages the Simple Search assistant. Our dataset is a collection of Windows security logs for user creation and group modification. We then use the

transaction command to group an account create, and an addition to the local administrators group, in a short period of time. Anything that matches, we will surface.



2) User Logged Into In-Scope System They Should Not Have

Stage 4

Kill Chain Phases

Actions on Objective

Data Sources

Authentication | Windows Security

Description
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.

Use Case
Insider Threat, Compliance

Category
GDPR, IAM Analytics, Lateral Movement, Operations

Security Impact
GDPR gives the right to individuals that they can ask an organization where their data is stored (Article 15) - through data mapping reinforced by controls to detect violation, an organization can identify which vendors/ processors accessed the data and might store it and in which other services the data is processed regularly. If you're processing on behalf of a controller data - this search can prove that only authorized individuals have accessed it (Article 28).

Alert Volume
High

SPL Difficulty
Basic

How to Implement
First, use your data mapping results to build a lookup that associates systems to their GDPR category. Then do the same for users. At that point, as long as you have the data onboarded with common information model compliance, everything should go smoothly!

Known False Positives
This will fire when someone is not in the documented list, so the most common scenario is that the documented list is just old.

How to Respond
The most likely scenario when this alert fires is that the documentation is simply out of date. Look for indications that someone should be added to the documentation, but validate with your data protection officer or their team before doing so.

How Does This Detection Work?
This search assistant runs standard Splunk searches -- read below for the particulars on this detection.

User Logged Into In-Scope System They Should Not Have Help
This example leverages the Simple Search assistant. Our example dataset is a collection of anonymized Windows Authentication logs, during which someone logs into a new system. Our live search looks for Windows Authentication activity across any index in the standard sourcetype.

FRAUD DETECTION

1) Detect Compromised User Accounts

Data Sources

Web Application Logs

Description
Any account could be taken over by fraudsters, including bank, credit card, email, medical accounts and other service providers from any industry. Online accounts are usually taken over as a result of phishing, spyware or malware scams.

Use Case
Fraud Detection

Category
Account Takeover

Impact
Detect when multiple different IP addresses were able to successfully login to single user account. Organizational losses stretch beyond monetary losses, to damaged reputation, organizational efficiencies and the ability to meet compliance mandates. Attackers gain access and credential information to execute fraudulent activities. Attackers can take over an account without you recognizing it, simply by posing as a legitimate user. This can allow access to even more sensitive data. All of this can create significant costs and high risk of loss.

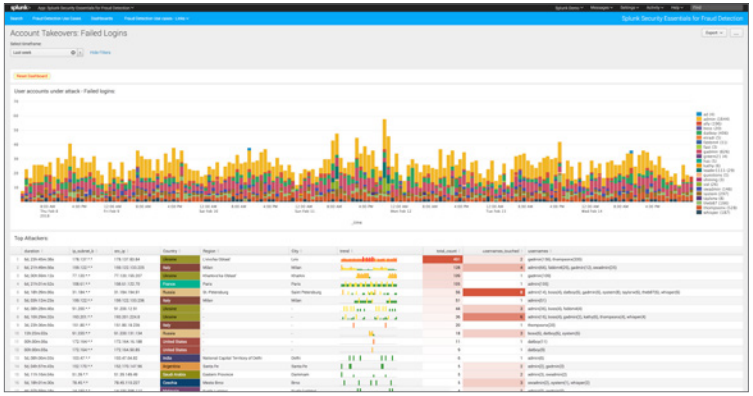
Alert Volume
Medium

SPL Difficulty
Medium-High

How to Implement
Choose use your critical user accounts data and that the fields are properly extracted.

Known False Positives
None.

How to Respond
These are mostly brute force attempts to take over user accounts. Investigate attacking IPs and subnet and adjust firewall rules accordingly to minimize potential of account takeover. Notice spikes on a timechart and investigate accounts that are experiencing high volume of attacks.



How it Works
Data must contain information about login attempts and flag whether the attempt was successful or failure. The SPL concept is:

```
index=web-logs action=login result=failure | stats count,
sparkline as trend  by src_ip | where count>5 | sort - count
| table _time src_ip trend count
```

2) Find Anomalous Healthcare Providers

Data Sources

Medicare Provider Utilization | Payment Data

Description
Find nationwide and statewide anomalies in prescription drug claims

Use Case
Fraud Detection

Category
Account Takeover

Impact
More than 400 people across the country have been charged with participating in healthcare care pharmaceutical fraud scams, this can impact regulations and requirements making it more difficult for providers to conduct daily business and harder on customers to get the prescriptions that are actually needed. You can also incur impactful financial penalties and criminal charges.

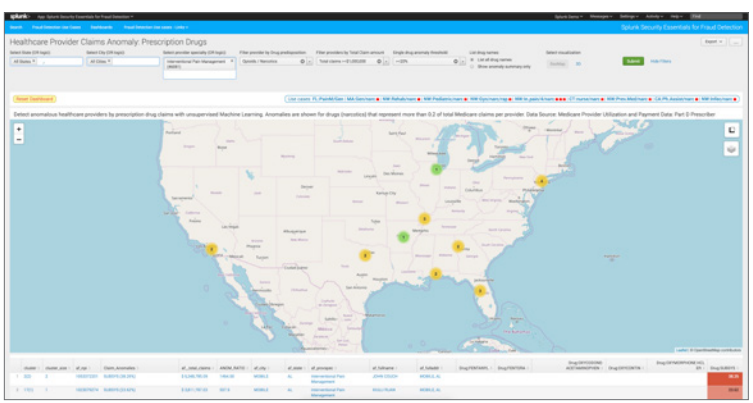
Alert Volume
Medium

SPL Difficulty
Medium-High

How to Implement
- Datasets could be downloaded from https://data.cms.gov/
- Data comes in CSV format making it easy to be ingested.
- See dashboard source for SPL. However app already comes with CMS dataset packaged.

Known false positives
Results are shown as anomalies and outliers. There are no definitive indication of whether the providers shows are fraudulent or not. However upon further research (using Google) we found that in many cases anomalous providers (especially prescribing opioids in large quantities) were involved in questionable business practices sometimes years after datasets we're published.

How to Respond
Clicking on a provider name to open detailed profile analysis dashboard. Investigate detailed prescription data and confirm that provider behavior is not matching to his peer group prescribing behavior within "nationwide provider profile vs this provider profile" charts. Clicking on a provider name on detailed profile analysis dashboard to open Google search page to scan public web for any results related to chosen provider.



How it Works
Anomalies are shown on a map. Clicking on the yellow circle will show summary data on specific anomaly. Clicking on a provider name will open detailed profile analysis dashboard with specific data related to given provider.

INSIDER THREAT

1) Large Web Upload

Stage 1

Data Sources

Web Proxy

Description
Uses a basic threshold to detect a large web upload, which could be exfiltration from malware or a malicious insider.

Use Case
Security Monitoring, Insider Threat

Category
Data Exfiltration

Security Impact
Data Exfiltration usually occurs over standard channels these days, with insiders uploading data to Google, Dropbox, Box, smaller file sharing sites, or even unlisted drop sites. Because HTTPS is always allowed out, exfiltration becomes relatively easy in most organizations. Detect those big transfers!

Alert Volume
Medium

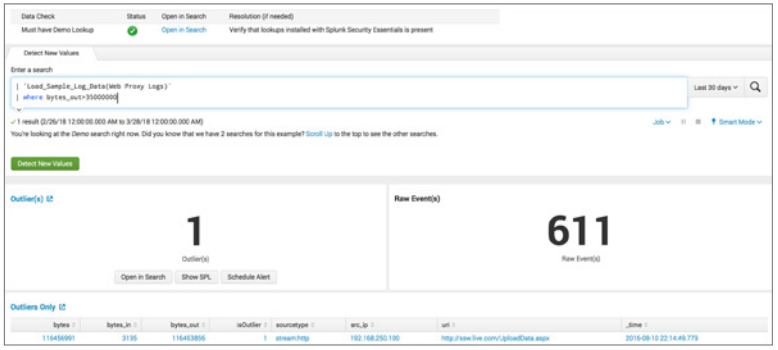
SPL Difficulty
Basic

How to Implement
This search should work immediately for any Palo Alto Networks environment, and can be easily adapted to apply to any other source of proxy visibility (dedicated proxies, along with network visibility tools such as Splunk Stream or bro). Just adjust the sourcetype and fields to match, and you will be good to go.

Known False Positives
By definition, this search is very simple and will fire for many innocent occurrences (uploading vacation photos, etc.). Many organizations will try to filter this down by focusing on users who are on a watchlist either because they have access to sensitive data (execs, scientists, etc.) or because of employment reasons (performance plan, notice given, contract ending, etc.). These watchlists can be implemented by using lookups.

How to Respond
When this fires, it will usually do so for perfectly legitimate reasons (uploading vacation photos, etc.). When this fires, many analysts will look where the data was sent to, whether the user has uploaded data to that site before. Often analysts will call the user to confirm the activity, preferably with the knowledge of that employee's status in the organization (e.g., are they on a performance plan or reaching the end of a contract, where they would be at greater risk of data exfiltration). If you have SSL Inspection turned on via your NGFW or DLP for that site, you can sometimes see the actual files that were transferred, which can help provide context.

Show Search



Help

How Does This Detection Work?

This search assistant runs standard Splunk searches -- read below for the particulars on this detection.

Large Web Upload Help

This example leverages the Simple Search search assistant. Our example dataset is a collection of anonymized Palo Alto Networks proxy logs (onboarded in accordance with our Data Onboarding Guides), during which someone does something bad. Our live search looks for the same behavior using the standardized sourcetypes for Palo Alto Networks or the Common Information Model.

2) Successful Login of Account for Former Employee

Stage 4

Data Sources

Authentication | Windows Security

Description

You shouldn't see any successful authentication activity on the accounts of former employees. Track this easily in Splunk.

Use Case

Security Monitoring, Insider Threat

Category

Account Compromise, Insider Threat

Security Impact

Users who have left your organization should generally not be logging in. It could mean that their credentials were compromised earlier, or it could mean that they are trying to log in to take some inappropriate actions. Either way, this is something you want to detect.

Alert Volume

Low

SPL Difficulty

Basic

How to Implement

If you have followed the data onboarding guides in this app, this search will work immediately for you. You should generally specify the index where you are storing Windows Security logs (e.g., index=oswinsec), and if you use a mechanism other than the Splunk Universal Forwarder to onboard that data, you should verify the sourcetype and fields that are used. The rest is simple!

Known False Positives

If your organization doesn't actually disable or remove accounts, then this search may not be actionable. If this is you, consider creating some boundaries around this behavior by specifying systems that "acceptable" post-termination activity can be expected on, such as the email environment. Also put a detective control in place to ensure that passwords are changed when an employee goes from active to not, and try to limit the usage of accounts after the employee leaves.

How to Respond

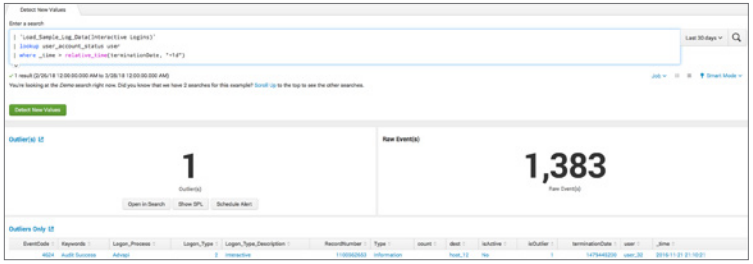
The first thing to understand after this alert fires is whether this was some continuation of normal system operations (e.g., the desktop under their desk was still logged in, or iPhone account still active) versus a deliberate action. Obviously success or failure also carries weight. Finally, particularly for sysadmin type employees in less structured organizations, it's important to make sure that there are no services or scheduled jobs running under that account where disabling the account outright might impact operations.

How Does This Detection Work?

This search assistant runs standard Splunk searches -- read below for the particulars on this detection.

Successful Login of Account for Former Employee Help

This example leverages the Simple Search search assistant. Our example dataset is a collection of anonymized Windows Authentication logs (onboarded in accordance with our Data Onboarding Guides), during which someone does something bad. Our live search looks for the same behavior using the standard sourcetypes.



READY TO LEARN MORE ABOUT HOW TO IMPROVE YOUR SECURITY POSTURE?

Learn to solve 335 different security challenges for free by downloading the Splunk Security Essentials app from Splunkbase.

Then work with Splunk's security professionals and partners to implement the use cases within your environment.

Contact us to get started today!

www.splunk.com/asksales

ABOUT SPLUNK.

Splunk Inc. makes machine data accessible, usable and valuable to everyone. Join millions of passionate users by trying Splunk for free: **www.splunk.com/free-trials.**

splunk>

© 2018 Splunk Inc. All rights reserved. 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.

BK-Splunk-Essential-Guide-to-Security-101