What’s Your Plan for Cybersecurity?
Are you simply “planning for the worst, but hoping for the best?”
Introduction

What’s your plan for cybersecurity? 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’s imperative that your organization is precise, informed and prepared when it comes to defending your assets and hunting your adversaries.

High-profile breaches, global ransomware attacks and the scourge of cryptomining are good enough reasons why your organization needs to collect, leverage and understand the right data. You’ll also need to implement the right processes and procedures, often alongside new technologies, methods and requirements – all with an ever-increasing velocity and variety 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.
The Nerve Center Model
Establishing a nerve center allows organizations to advance their security by optimizing their people, processes and technology. It includes using all the data from the security technology stack, which can help you investigate, detect and take rapid, coordinated action against threats in a manual, semi-automated or fully-automated fashion. When security teams invest in their security infrastructure, their security ecosystem and skills become stronger, making it possible to expand security practices into new areas and proactively deal with threats.

The Splunk Data-to-Everything Platform acts as this nerve center by bringing together multiple cybersecurity areas, as well as others outside of security, to foster collaboration and implement best practices for interacting with your data. Security teams can use Splunk solutions to drive statistical, visual, behavioral and exploratory analytics that inform decisions and actions. From there, the platform allows for a modern workflow, from collecting data all the way to invoking actions to address cyberthreats and challenges.

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

To get you started, we put together this short guide to introduce you to the top security use cases organizations face and to show you how Splunk’s analytics-driven platform can help you solve your security challenges. This guide is divided into three sections:

1. Understanding the Fundamentals. Here you will find an introduction to the security journey and a quick primer on security use cases with each use case mapped to relevant Splunk solutions.

2. Embarking on Your Analytics-Driven Security Journey. Here we explain the six stages of the data-driven security journey — and what you should be able to do, and how well, at each stage.

3. Solving Common Security Challenges With Splunk. Here we walk through examples of how to solve common security challenges associated with:
   - Incident investigation and forensics
   - Security monitoring
   - Advanced threat detection
   - SOC automation
   - Incident response, compliance
   - Fraud and analytics detection
   - Insider threat

Ready to create a kick-ass security practice? We thought so.
Understanding the Fundamentals

Cyber criminals never rest, which means that you should constantly be looking for new security use cases and insights to maintain high levels of protection in your environment.

We’re here to help.

**Splunk’s Analytics-Driven Security Journey**

Anyone who has been asked the question, “Are we secure?” knows that cybersecurity is a journey, not a destination. While the expedition may not have an end point, and there will always be challenges, there are things you can do to make the trip successful.

First, you must understand your environment and find a place to begin. Ask yourself: What am I trying to protect? What is my critical data? How will I respond to the threats?

The six-stage analytics-driven security journey, shown in Figure 2, will help you answer these questions and create a kick-ass security practice that enables you to understand the gaps in your defenses, see the next challenge and take action to meet it head on.

**Figure 2: Splunk’s Analytics-Driven Security Journey**

**Stage 1: Collection**
Collect basic security logs and other machine data from your environment

**Stage 2: Normalization**
Apply a standard security taxonomy and add asset and identity data

**Stage 3: Expansion**
Collect additional data sources like endpoint activity and network metadata to drive advanced attack detection

**Stage 4: Enrichment**
Augment security data with intelligence sources to better understand the context and impact of an event

**Stage 5: Automation and Orchestration**
Establish a consistent and repeatable security operation capability

**Stage 6: Advanced Detection**
Apply sophisticated detection mechanisms including machine learning
Splunk’s Security Suite

Would you embark on a hiking expedition without a trail map and a backpack full of provisions and the right gear? Of course not. Just as no trip can be successful without the proper equipment, no security journey can be successful without the right technology.

Splunk’s Security Suite helps security teams navigate uncharted waters and quickly identify, investigate, respond to and adapt to threats in dynamic, digital business environments. Splunk solutions can be used by a tier-1 analyst to do basic research on a time period, keyword, IP address or machine name. The same products enable advanced tier-2 and tier-3 analysts to perform advanced correlations, build analytical models or perform advanced forensics.
The Security Use Cases

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 Solutions to Security Use Cases

<table>
<thead>
<tr>
<th>Use Case</th>
<th>Splunk Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incident Investigation and Forensics</td>
<td>Splunk Enterprise, Splunk Enterprise Security, Splunk Phantom</td>
</tr>
<tr>
<td>SOC Automation</td>
<td>Splunk Enterprise, Splunk Enterprise Security, Splunk Phantom</td>
</tr>
<tr>
<td>Incident Response</td>
<td>Splunk Enterprise, Splunk Enterprise Security, Splunk Phantom</td>
</tr>
<tr>
<td>Compliance</td>
<td>Splunk Enterprise, Splunk Security Essentials App, PCI, Splunk Enterprise Security</td>
</tr>
<tr>
<td>Fraud Analytics and Detection</td>
<td>Splunk Enterprise, Splunk Security Essentials App, Splunk Enterprise Security</td>
</tr>
<tr>
<td>Insider Threat Detection</td>
<td>Splunk Enterprise, Splunk Security Essentials App, Splunk User Behavior Analytics</td>
</tr>
</tbody>
</table>

The Security Use Cases Defined

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

#### 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. 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.

#### Security Monitoring

Security monitoring enables you to analyze a continuous stream of near-real-time data for threats and other potential security issues. Data sources for monitoring include network and endpoint systems – as well as cloud devices, data center systems and applications. The Splunk Data-to-Everything 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 private organizations and/or states for business or political motives. Splunk Enterprise enables organizations to search and correlate data to track advanced threats. Splunk Enterprise Security and Splunk User Behavior Analytics elevate existing capabilities to apply a kill chain methodology through statistical analysis, anomaly detection and machine learning techniques to detect unknown and advanced threats.

#### SOC Automation

Security operations teams adopt Splunk software for orchestration and automation of enrichment and response actions, as well as for case management (i.e. incidents). They use Splunk’s SOC automation solutions to scale operations, accelerate response and remediate threats and other security issues. Splunk solutions also help organizations operationalize analytics-driven security practices and empower security teams to collaborate across the extended team.
Incident Response

Incident Response (IR) involves the monitoring and detection of security events on IT systems, and the execution of response plans to those events. IR Teams are sometimes called blue teams. Blue teams defend an organization’s infrastructure when threats are detected, whereas red teams attempt to discover weaknesses in the existing configuration of those same systems. Splunk offers a variety of IR capabilities in the security portfolio, depending on the offerings you choose. Each offers mechanisms to perform investigations for detected events. Splunk solutions may also include capabilities to guide an incident responder through standardized response procedures.

Compliance

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

Fraud Analytics and Detection

Machine data plays a pivotal role in and is at the heart of detecting fraudulent activities in the digital age. Splunk can onboard new data so that fraud teams are able to better detect and investigate anomalies. As a result, companies are positioned to reduce financial losses, protect reputation and maintain organizational efficiencies.

Insider Threat Detection

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. By using Splunk solutions, security teams have the ability to detect and prioritize threats posed by insiders and compromised insiders that would have otherwise gone undiscovered.

Embarking on Your Analytics-Driven Security Journey

To be effective, a cybersecurity program must continually evolve. The problem is that many organizations lack a clear sense of where they are and how to improve. Knowing where you are in your journey will help you manage your time and resources more effectively. And with a sense of what’s to come, you can better plan for success in the later stages.

Here’s a breakdown of the six stages of the analytics-driven security journey that uses data to stay ahead of attacks. For each stage we take a look at:

- Use case applicability
- Data sources
- Milestones
- Challenges
Stage 1: **Collection**

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

### Security Use Case Applicability

<table>
<thead>
<tr>
<th>Use Case</th>
<th>Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incident Investigation &amp; Forensics</td>
<td></td>
</tr>
<tr>
<td>Security Monitoring</td>
<td></td>
</tr>
<tr>
<td>Advanced Threat Detection</td>
<td></td>
</tr>
<tr>
<td>SOC Automation</td>
<td></td>
</tr>
<tr>
<td>Incident Response</td>
<td></td>
</tr>
<tr>
<td>Compliance</td>
<td></td>
</tr>
<tr>
<td>Fraud Analytics and Detection</td>
<td></td>
</tr>
<tr>
<td>Insider Threat</td>
<td></td>
</tr>
</tbody>
</table>

### Description

**Stage 1** focuses on obtaining the raw materials necessary to start gaining a deeper understanding of the environment you must defend.

### Data Sources

The best practice for **Stage 1** is to capture machine data generated by the four 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.

   Sources include:
   - Firewall traffic logs from vendors such as:
     - Palo Alto Networks
     - Cisco
     - Checkpoint
     - Fortinet
2. **Endpoint (host-based).** 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 servers, workstations and all operating systems.

**Sources include:**
- Windows event logs
- Linux system logs
- Linux Auditd logs
- 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.

**Sources include:**
- Windows Active Directory
- Local authentication
- Cloud identity and access management (IAM)
- Linux auditd logs
- MacOS system logs

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.

**Sources include:**
- Next-generation firewall (NGFW) traffic filters or proxy logs from vendors such as:
  - Palo Alto Networks
  - Cisco
  - Checkpoint
  - Fortinet
  - Bluecoat
  - Websense

**Milestones**
After successfully onboarding data from these four categories, you should have achieved the following milestones:
- Critical activity logs reside in a separate system where they can’t easily be tampered with by an attacker; and
- Data from the four categories is available to perform basic investigations.

**Challenges**
Collecting the different data sources can be a hassle and making sure the data is onboarded correctly can be tedious. It’s often done incorrectly and insufficient information is captured, causing lost time and incomplete investigations.
Stage 2: **Normalization**

Apply a standard security taxonomy and add asset and identity data.

**Security Use Case Applicability**

- Incident Investigation & Forensics
- Security Monitoring
- Advanced Threat Detection
- SOC Automation
- Incident Response
- Compliance
- Fraud Analytics and Detection
- Insider Threat

**Description**

In Stage 2, 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 which device created the event. This critical investment in normalizing data allows you to:

- Start implementing a security operations center to track systems and users on your network; and
- Begin to scale the capabilities of your security team.

Even if you don’t plan to stand up a formal SOC, normalized data will:

- Facilitate cross-source correlation;
- Streamline investigations; and
- Improve the effectiveness of an analyst.

**Data Sources**

In Stage 2 you should collect reference information about:

- IT assets (systems, networks, devices, applications); and
- User identities from Active Directory, LDAP and other IAM/SSO systems.

**Milestones**

Milestones for Stage 2 include:

- 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**

Although you have basic data that is searchable, you lack the insights or understanding you need for deeper security detections and endpoint visibility.
Stage 3: Expansion

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

**Security Use Case Applicability**

- Incident Investigation & Forensics
- Security Monitoring
- Advanced Threat Detection
- SOC Automation
- Incident Response
- Compliance
- Fraud Analytics and Detection
- Insider Threat

**Description**

Domain name system (DNS) and endpoint data will unlock a rich set of detection capabilities, empowering threat hunters to uncover and track adversaries dwelling in the network.

**Data Sources**

Data sources at this stage include:

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

2. **Endpoint.** Rich endpoint activity that captures process creation, file changes, registry modifications, network connections and so on provides an amazingly clear history of critical events occurring on an endpoint.
   
   Sources include:
   - sysmon
   - Osquery
   - Carbon Black Defense

**Milestones**

By collecting high-fidelity data sources, you will have:

- Laid the foundation for advanced detections; and
- Obtained 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 remain undetected in your environment.
Stage 4: **Enrichment**

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

### Security Use Case Applicability

| Use Case                                | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |
|-----------------------------------------|---|---|---|---|---|---|---|---|---|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| Incident Investigation & Forensics      |   |   |   |   |   |   |   |   |   |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
| Security Monitoring                     |   |   |   |   |   |   |   |   |   |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
| Advanced Threat Detection               |   |   |   |   |   |   |   |   |   |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
| SOC Automation                          |   |   |   |   |   |   |   |   |   |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
| Incident Response                       |   |   |   |   |   |   |   |   |   |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
| Compliance                              |   |   |   |   |   |   |   |   |   |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
| Fraud Analytics and Detection           |   |   |   |   |   |   |   |   |   |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
| Insider Threat                          |   |   |   |   |   |   |   |   |   |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |

### Data Sources

Data sources include:

- Local IP/URL block lists
- Open-source threat intelligence feeds
- Commercial threat intelligence feeds

### Milestones

By enriching data with intelligence that provides context, security personnel are able to:

- Understand the urgency of an alert based on the criticality of the asset; and
- Augment alerts 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 failing to consider 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 neither stored nor leveraged for future use.

### Description

In addition to collecting vital machine data, high-performing security teams enrich their data with intelligence from internal and external sources. Contextual and investigative knowledge, including threat-intelligence feeds, open-source intelligence (OSINT) sources and internally sourced information, allows security personnel to extract more value from the collected data to detect security events and incidents sooner.
Establish a consistent and repeatable security operation capability.

Security Use Case Applicability

- Incident Investigation & Forensics
- Security Monitoring
- Advanced Threat Detection
- SOC Automation
- Incident Response
- Compliance
- Fraud Analytics and Detection
- Insider Threat

Description

Leveraging a security orchestration, automation and response (SOAR) solution allows organizations to reduce risk in a number of powerful ways. Some of the key benefits of implementing automation and orchestration is the ability to strengthen your defenses by integrating existing security tools and threat intelligence sources, speed response to security events, simplify the investigation process and minimize damage from attacks. Mature organizations are able to continuously triage and prioritize inbound alerts automatically, freeing their human resources to focus on the most critical issues that require their attention. Mature organizations also gain better consistency and repeatability through the execution of standardized automation playbooks vs. execution of a response plan manually.

Data Sources

Data sources in this stage include the high-fidelity events that are generated by data platforms like Splunk Enterprise. Correlation searches, notable events, and other high-fidelity events are ingested by an automation and orchestration system for further actioning.

Milestones

Milestones in Stage 5 include the ability to:

- Track incidents;
- Regularly measure analyst effectiveness;
- Take action according to prescribed playbooks; and
- Automate simple response actions and combine them together into more sophisticated orchestration.

Challenges

Security teams are usually hard at work on the front lines, identifying, analyzing and mitigating threats when and where possible. Yet despite their best efforts, security incident backlogs continue to grow with time spent on consuming investigations and already-known threats. (The reality is that there simply aren’t enough skilled professionals to analyze the volume of incidents that most organizations face.)
Apply sophisticated detection mechanisms, including machine learning.

**Security Use Case Applicability**

- Incident Investigation & Forensics
- Security Monitoring
- Advanced Threat Detection
- SOC Automation
- Incident Response
- Compliance
- Fraud Analytics and Detection
- Insider Threat

**Data Sources**

Hunting adversaries requires more granular data collection from your endpoints. 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.

Sample sources include:

- Microsoft sysmon
- Osquery
- Carbon Black Defense

**Milestones**

In Stage 6 you’re employing:

- The most advanced techniques available to identify unknown threats; and
- New detection mechanisms as they become available, leveraging both your team’s expertise and outside research organizations.

**Challenges**

At this point, you’ll be challenged to constantly improve your security organization and gain new capabilities. Your team will also likely be required to perform new research. But by following the journey and maturing your capabilities, 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.

**Description**

By applying machine learning, data science and advanced statistics to analyze the users, endpoint devices and applications in your environment, you’re giving yourself a fighting chance to detect adversaries, unknown threats and insider threats, even when they leave only subtle traces of their activity.
Solve Common Security Challenges With the Splunk Security Operations Suite

The security journey can be a bumpy road. Wouldn't it be great if you had a handbook of the challenges you may encounter so that, when they happen, you have the tools to handle the situation and stay on course?

No worries. We have you covered.

Here we provide some examples to help you solve 16 common security challenges (you can find more in the Splunk Security Essentials app or Splunk Security Online Demo). Each example explains the challenge and provides information about data sources, use cases, Splunk solutions, programming difficulty, how to implement, alert volume, known false positives and how best to respond.

The examples include:

- **Incident investigation and forensics**
  - Detect lateral movement with WMI
  - Identify multiple unauthorized access attempts

- **Security monitoring**
  - Detect public S3 buckets in AWS
  - Find multiple infections on host

- **Advanced threat detection**
  - Detect connections to new domains
  - Find emails with lookalike domains

- **SOC automation**
  - Automate malware investigations
  - Automate phishing investigations

- **Incident response**
  - Detect web data exfil DLP alerts for user
  - Identify basic dynamic DNS detection

- **Compliance**
  - Detect new local admin account
  - Find user logged into in-scope systems they should not have

- **Fraud analytics and detection**
  - Detect compromised user accounts
  - Find anomalous healthcare providers

- **Insider threat detection**
  - Detect large web upload
  - Detect successful login of account for former employee
Incident Investigation and Forensics

Detect Lateral Movement With WMI

STAGE 3

MITRE ATT&CK Tactics
- Lateral Movement
- Execution

MITRE ATT&CK Techniques
- Remote Services
- Windows Management Instrumentation

Data Sources
- Windows Security
- Endpoint Detection and Response

Security Challenge
Windows management instrumentation (WMI) has been gaining popularity amongst attackers for its ability to perform system reconnaissance, antivirus and virtual machine detection, code execution, lateral movement, persistence and data theft.

Use Case
Advanced threat detection

Category
Lateral movement

Splunk Solutions Required
Simple search assistant

SPL Difficulty
Basic

How to Implement
This use case requires sysmon to be installed on the endpoints you wish to monitor and the sysmon add-on installed on your forwarders and search heads.

Alert Volume
Low

Known False Positives
No known false positives

How to Respond
When this search fires, you will want to start your incident response process and investigate the actions taken by this process.
Identify Multiple Unauthorized Access Attempts

STAGE 1

**MITRE ATT&CK Tactics**
- Credential Access

**MITRE ATT&CK Techniques**
- Brute Force

**Data Sources**
- Authentication
- Windows Security

**Security Challenge**
Most login failures are due to failed passwords. However, multiple login failures to sensitive systems where the users simply aren’t authorized can indicate malicious intent. In most organizations, it’s rare for a user to get an unauthorized message, beyond low-risk scenarios such as proxy logs. When this occurs for higher-risk activities, such as system logins, file share access and so on, and when it occurs persistently for a user, there’s usually a reason to investigate.

**Use Case**
Insider threat

**Category**
Insider threat

Detect Lateral Movement with WMI Help
To detect lateral movement with WMI we first load our sysmon EDR data. Any other process launch logs with the full command line will also suffice. We look for any instances of Windows management instrumentation command-line (WMIC) being launched (EventCode 1 indicates a process launch), and filter to make sure our suspicious fields are in the CommandLine string.

```
index=* sourcetype=XmlWinEventLog:Microsoft-Windows-sysmon/Operational EventCode=1 Image=*wmic* CommandLine=*node* CommandLine="*process call create*"
| table _time host Image CommandLine
```
Splunk Solutions Required
Simple search assistant

SPL Difficulty
Medium

How to Implement
Ensure that you have data being ingested from the Universal Forwarder and the Splunk Technology Add-on present, and all will work automatically.

Alert Volume
Low

Known False Positives
The most likely scenario where this detection indicates a false positive is where the user’s access has simply been messed up. For example, there was an AD group change last night, and the user was accidentally removed from the “dev_system_access” security group. Beyond that, there’s no standard pattern that would be expected for false positives.

How to Respond
When this alert fires:
1. Evaluate whether the user has previously had access to the desired resources.
2. Look for recent job role changes.
3. Look for recent changes around AD groups.

In most organizations, the next escalation step would be to consult the resources’ owner, and/or the user’s manager, to determine whether this behavior is intended. Keep an eye out for indications of malicious intent alongside potential account compromise.

Identify Multiple Unauthorized Access Attempts Help
To find multiple unauthorized access attempts using live data, we use the simple search and the below search processing language. Here we are bringing in Windows Security logs and specifically looking for the status code 0xC000015B, which indicates that the user hasn’t been granted the requested logon type. We’re looking for any user with many of these per day, which can indicate attempted access to sensitive resources. The screenshot below shows the results of a search on demo data.

```
index=* source=win*security user=* EventCode=* action=failure Logon_Type=* Failure Reason Logon Type Status=0xC000015B
```
Security Monitoring
Detect Public S3 Buckets in AWS

STAGE 3

Data Sources
Audit Trail  AWS

Security Challenge
It’s an all-too-common story. People host files in an AWS S3 bucket for quick transfer but forget to take them down, or use S3 buckets to backup sensitive data, but inadvertently mess up the permissions. Because misconfigured and public S3 buckets needlessly expose sensitive data to the risk of exploitation and are a common way for breaches to occur, it’s important to detect when new or existing S3 buckets are set to public.

Use Cases
Security monitoring
Advanced threat detection

Category
Data exfiltration, SaaS

Splunk Solutions Required
Splunk security essentials
Splunk Add-On for Amazon Web Services
Splunk Simple Search Assistant

SPL Difficulty
Medium

How to Implement
The search for public S3 buckets is facilitated by normalized data, which is mapped to the Common Information Model. The Splunk Add-On for Amazon Web Services provides visibility of various AWS service components, including events from the CloudTrail Service and S3 buckets. Assuming you use the 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.

Alert Volume
Very low

Known False Positives
There are two types of undesired alerts that can occur from this search. They occur when someone:
1. Intentionally creates a public bucket. You may wish to whitelist marketing employees who do this on a regular basis, or create a policy for how to create a public bucket so that you can exclude intentional public buckets from searches.
2. Creates a bucket that is public momentarily, but then switches it to private mode.

How to Respond
When this search fires, you will want to start your incident response process and investigate the actions taken by this process.
Detect Lateral Movement with WMI Help
To detect lateral movement with WMI we first load our sysmon EDR data. Any other process launch logs with the full command line will also suffice. We look for any instances of Windows management instrumentation command-line (WMIC) being launched (EventCode 1 indicates a process launch), and filter to make sure our suspicious fields are in the CommandLine string.

How to Respond
When an alert for a public S3 bucket fires, there are three questions that should be asked:

1. Is the S3 bucket still public?
2. Are the files public?
3. What is in the bucket?

The first question is easy to answer – just search your logs for the bucket name and “PutBucketACL.” You will see any subsequent ACL changes. The second and third questions are trickier, and requires that server access logging is turned on for the S3 bucket (not done by default, and it is pretty inconvenient, so don’t bet on it).

If you have a corporate AWS environment, prioritize analyzing any open S3 buckets. You may even wish to automate the remediation of them through AWS functions.

Detect Public S3 Bucket in AWS Help
To search for public S3 buckets using live data, we use the simple searchand the below search processing language. The live search operates on AWS Cloudtrail logs, filtering for the PutBucketAcl events that occur when bucket permissions are changed, and filtering for any that include AllUsers. The screenshot shows the results of a search on demo data.

```bash
index=* sourcetype=aws:cloudtrail AllUsers
| spath output=userIdentityArn
| spath output=bucketName
| spath output="requestParameters.bucketName"
| spath output=aclControlList
| spath input=aclControlList output=grantee
| search “Grantee.URI”=*AllUsers
| table _time, Permission, Grantee.URI, bucketName, userIdentityArn | sort - _time
```
Find Multiple Infections on Host

STAGE 1

MITRE ATT&CK Tactics
- Initial Access
- Execution

MITRE ATT&CK Techniques
- Drive-by Compromise
- Spearphishing Attachment
- Spearphishing Link
- User Execution

Data Sources
- Anti-virus
- Anti-malware

Security Challenge
Viruses happen, but multiple viruses occurring on a single host all at once are a greater concern. Such activity could indicate an exploit kit that tries several techniques, where some might succeed, or a host with multiple unrelated viruses. Traditional anti-malware products can be effective in detecting known malware, but they can fail when faced with new or evolving malware types. Because malware variants can provide a backdoor to internal systems, allow for long-term persistence or exfiltrate data, you should immediately prioritize and investigate malware-infected hosts to determine what else might not have been caught.

Use Case
Security monitoring

Category
Endpoint compromise

Splunk Solutions Required
- Splunk Security Essentials
- Splunk Common Information Model Add-on
- Splunk Simple Search Assistant

SPL Difficulty
Basic

How to Implement
Detecting hosts with multiple infections requires the collection of logs from an antivirus solution. With Symantec logs onboard, for example, this search should work easily. If you have a different antivirus product, you can easily adapt the field names and sourcetypes for that product to the search criteria – especially if you use a Splunk Add-on that maps them to the Common Information Model (search on Splunkbase).

Alert Volume
Low

Known False Positives
No known false positives.

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

Find Multiple Infections on Host Help
To find hosts that have logged multiple infections in a short period of time using live data, our example uses the simple search and the below search processing language. First, we bring in our basic dataset, Symantec Endpoint Protection Risks, over the last 24 hours. While there are several approaches to grouping events – and stats is the fastest – we’re using transaction because it’s the easiest. This will let us group all the events based on the Computer_Name. Finally, we can filter for whether there are at least three events that spanned at least a few minutes. The screenshot below shows the results of a search on demo data.

```
index=* sourcetype=symantec:* earliest=-24h | transaction maxpause=1h Computer_Name | where eventcount >=3 AND duration>240
```

![Screenshot of search results](image)
Advanced Threat Detection

Detect Connection to New Domain

STAGE 2

MITRE ATT&CK Tactics
- Exfiltration
- Command and Control

MITRE ATT&CK Techniques
- Exfiltration Over Command and Control Channel
- Exfiltration Over Alternative Protocol
- Standard Application Layer Protocol

Data Sources
- Web Proxy
- NGFW

Use Case
Advanced threat detection

Category
Command and control, data exfiltration

Splunk Solutions Required
- Splunk Enterprise
- Splunk Security Essentials
- Splunk URL Toolbox
- Splunk Simple Search Assistant

SPL Difficulty
Medium

How to Implement
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. 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.

Implementing this search is relatively straightforward, as it expects CIM-compliant data. Start by ingesting 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 Splunk to parse out the domains. When scaling this search to greater volumes of data (or more frequent runs), we recommend leveraging acceleration capabilities.

Security Challenge
In most organizations, the domains that users visit today have a tremendous amount of overlap with the ones they visited yesterday. But what about the small percentage of domains that were requested from your network today, but are not previous destinations for your systems? Sure, there’s going to be some legitimate traffic going to a few domains today that haven’t been seen on the network before, but it’s likely to be a small percentage of the overall set of domains. The remainder of these new, never-before-seen domains represent a potential threat.

Knowing when users browse to new domains can be relevant in various scenarios, but the primary one is when your system connects to an attacker-controlled domain that is used as a hub for command and control communications or running a staging server for data exfiltration or delivery of malware. If you believe that a host is infected, investigating to see whether it hit new domains is a great indicator to check.

Alert Volume
Very high
**Known False Positives**
In most organizations, the percentage of new domains is small. However, if you sent all of these alerts to the analysts for investigation, it would be overwhelming because the majority of “new domain alerts” will be triggered by legitimate traffic. While there are no known false positives, per se, the value of any given “new domain” alert is so small that you want to treat these alerts differently from most correlation searches. These are mostly appropriate for contextual data or to correlate with other indicators.

**How to Respond**
New domain events are generally best viewed as contextual data for another event; for example, uncleansed malware, new services or unusual logins. The easiest way to accomplish this is to record the events in a summary index, and then include searching that index as a part of your investigative actions. Splunk Enterprise Security customers can do this easily with the Risk Management Framework. By creating a risk indicator adaptive response action when saving this search, 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 resource such as VirusTotal or ThreatCrowd.

**Detect Connection to New Domain Help**
To detect connections to new domains using live data we use the simple search and the below search processing language. First, we bring in our proxy dataset, leveraging Common Information Model fields and filtering for just events that actually have a URI.

Next we use URL Toolbox to parse out the domain from the URL. Finally, we exclude IP addresses from our search using the regex filtering command. This is an optional step, but we’ve found that the value to noise ratio when including IP addresses can be quite high given that some applications will connect to many ephemeral AWS instance IPs for normal operations. Lastly, we use the stats command to calculate what the earliest and the latest time is that we have seen this combination of fields and check to see if the earliest time we saw this event was within the last day (aka, brand new). The screenshot below shows the results of a search on demo data.

```
tag=web url=* | eval list=“mozilla” | `ut_parse_extended(url,list)` | regex ut_domain=“^\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}$” | stats earliest(_time) as earliest latest(_time) as latest by ut_domain, sourcetype | where earliest >= relative_time(now(), “-1d@d”)```
Find Emails with Lookalike Domains

STAGE 4

MITRE ATT&CK Tactics
Initial Access

MITRE ATT&CK Techniques
Spearphishing Link

Data Sources
Email

Security Challenge
Emails with lookalike domains are a common phishing tactic. Some attackers will switch easily mistakable letters, such as splunk.com receiving an email from spiunk.com. Or, they may use a believable subdomain (such as .help.com, .support, etc.) The problem is that people are more likely to open an email when they think it has been sent by a legitimate source. With the spoofed email, the difference is almost imperceptible.

Use Case
Advanced threat detection

Category
Endpoint compromise, SaaS

Splunk Solutions Required
Splunk Search Assistant
First Time Seen Assistant
UTL Toolbox app

SPL Difficulty
Advanced

How to Implement
Implementing this search is generally fairly straightforward. If you have CIM-compliant data onboarded, this search should work out of the box. You are, however, always better off specifying the index and sourcetype of your email data – particularly when you have multiple email log sources, such as a perimeter email security appliance and a core Exchange environment. It should work like a charm if you have installed the URL Toolbox and have the right index, sourcetype and src_user field.

Alert Volume
Very low

Known False Positives
This search will search through incoming emails for any domains similar to the domains usually requested by your organization, much like running dnstwist on a domain name. If there are any incoming emails with source domain names that are similar to – but not the same as – those generally seen on a daily basis, it’s possible for the search to create alerts that could be false positives. One might imagine a scenario where a company that manufactures wooden planks for pirate ships, plank.com, emails their sales rep at splunk.com. That would create a Levenshtein distance of two (where the ‘a’ in plank becomes a ‘u’ and we get an extra ‘s’) and it would be flagged (Arrrr!). To reduce the number of false alerts, you could filter known examples out of 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 of the mail and any attachments. 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.

**Find Emails With Lookalike Domains Help**
To find emails with lookalike domains in live data we use the Simple Search Assistant, URL Toolbox and the below search processing language. We start by pulling email logs, where we have a source address, and aggregate per source address. Next, we extract the domain and aggregate per actual domain that we will analyze. We also filter out any domains that we own and from which we expect to receive email. Using the free URL Toolbox app we parse out subdomains from the top level domains. Because the field we are going to pass to the Levenshtein algorithm is domain_detected, we add each subdomain to the multi-value field domain_detected. URL Toolbox is given two multi-value fields, and it does the cross checking to calculate the Levenshtein score for each combination. We pull out the lowest score from this group. Finally, we filter for a Levenshtein score less than three. The screenshot below shows the results of a search on demo data.

```plaintext
index=* sourcetype=cisco:esa* OR sourcetype=ms:o365:*:messagetrace OR sourcetype=MSExchange*:MessageTracking OR tag=email src_user=* | stats count by src_user | rex field=src_user "\@(?.*)*" | stats sum(count) as count by domain_detected | eval domain_detected=mvfilter(domain_detected!="mycompany.com" AND domain_detected!="company.com" AND domain_detected!="mycompanylovestheenvironment.com") | eval list="mozilla" | `ut_parse_extended(domain_detected, list)` | foreach ut_subdomain_level* [eval orig_domain=domain_detected, domain_detected=mvappend(domain_detected, '<>' . ut_tld)] | fields orig_domain domain_detected ut_domain count | eval word1=mvappend(domain_detected, ut_domain), word2 = mvappend("mycompany.com", "company.com", "mycompanylovestheenvironment.com") | lookup ut_levenshtein_lookup word1 word2 | eval ut_levenshtein= min(ut_levenshtein) | where ut_levenshtein < 3 | fields - domain_detected ut_domain | rename orig_domain as top_level_domain_in_incoming_email word1 as domain_names_analyzed word2 as company_domains_used count as num_occurrences ut_levenshtein as Levenshtein_Similarity_Score
```

![Screenshot showing search results](image)
SOC Automation

Automate Malware Investigations

STAGE 5

Data Sources

- Authentication
- Windows Security

Security Challenge
When the same malware occurs on multiple systems, you may be on the brink of a major incident (seen frequently with worms, ransomware and broad phishing campaigns). Investigating and responding to malware alerts can take 30 minutes or more—each. By automating this investigation and response, Splunk Phantom validates that the process is malicious and takes immediate action to block the hash on the infected endpoints.

Use Cases
- Security monitoring
- Advanced threat detection
- SOC automation

Category
- Endpoint compromise, lateral movement

Splunk Solutions Required
- Splunk Phantom

SPL Difficulty
- Not applicable

How to Implement
Ingest malware events from your data source into your SOAR platform. Perform investigative actions, like retrieving reputation intelligence on applicable IPs, urls and files to help you make decisions faster. These context gather actions are great candidates for automation. Based on your decisions, execute containment and/or remediation steps, either manually or using automation playbooks.

Alert Volume
- Very low

Known False Positives
- Not applicable

How to Respond
The playbook investigates and remediates malware infections on the endpoint. By automating these responses you'll save time having to respond yourself and more immediate actions will be taken to block infected endpoints. You'll begin to automate the investigations and detections around use cases, such as, hiding files and directories, shim database file creations execution of a file with multiple extensions, single letter process on an endpoint and more.
Alert Context Enrichment Help

**Automate Phishing Investigations and Responses**

**STAGE 5**

**Data Sources**
- Audit Trail
- AWS

**Security Challenge**
Phishing emails can be detrimental to an organization if not detected. Investigating each email can be time consuming as an analyst may need to investigate what is in the body of the email, but also the attachments, as well as, any users that may have received the email. By automating the investigation, analysts can respond much faster to these attacks.

**Use Cases**
- Security monitoring
- Advanced threat detection
- SOC automation

**Category**
- Phishing, adversary tactics, account compromise

**Splunk Solutions Required**
- Splunk Phantom

**SPL Difficulty**
- Not applicable

**How to Implement**
Ingest suspicious emails into the SOAR platform. Perform investigative actions, like retrieving reputation intelligence on applicable IPs, urls, and files to help you make decisions faster. These context gather actions are great candidates for automation. Based on your decisions, take action to delete any copies of the phishing email from your mail system using an automation playbook.

**Alert Volume**
Very low

**Known False Positives**
Not applicable

**How to Respond**
Implementing and automating the correct investigations when building a playbook can enable you to limit the amount of human response necessary to carry out actions, since the response you’ll want implemented in the playbook will help streamline phishing investigations enabling faster remediation and action to be taken.

**Automate Phishing Investigations**
Incident Response
Detect New Data Exfil DLP Alerts for User

STAGE 3
MITRE ATT&CK Tactics
- Exfiltration

MITRE ATT&CK Techniques
- Exfiltration

Data Sources
- DLP

Security Challenge
When a user who normally does not generate data exfil DLP alerts suddenly starts, it is more notable than a traditional alert. For crucial rules or high-privileged users, investigate these events to determine whether sensitive company intelligence is leaving the organization.

Use Case
Insider threat

Category
Insider threat

Splunk Solutions Required
Simple search assistant

SPL Difficulty
Medium

How to Implement
Implementation of this rule is straightforward – the only requirement is to be able to record which DLP alerts represent data exfiltration. That nomenclature or configuration can vary wildly from one organization to another, so this will require coordination with your DLP team. Beyond that, as long as you have a user field and a signature field defined, the search will work.

Alert Volume
High

Known False Positives
This is a strictly behavioral search, so we define “false positive” slightly differently. Every time this fires, it will accurately reflect the first occurrence in the time period you’re searching over (or for the lookup cache feature, the first occurrence over whatever time period you built the lookup). But while there are really no “false positives” in a traditional sense, there is definitely lots of noise.

How to Respond
Because this is a behavioral alert, you should generally not use this in isolation unless:
- The severity of the alert or the priority of the user dictate that it is so crucial it must be looked at in isolation, or
- Your DLP is so carefully tuned that alerts are rare.

For everyone else, most alerts should only be considered when in conjunction with other alerts, via a risk aggregation mechanism in Splunk ES or the threat models in Splunk UBA.
Detect New Data Exfil DLP Alerts for User Help
This example uses the Simple Search Assistant. Our dataset is a base dataset of DLP events. For this analysis, we are filtering for data exfiltration alerts. The screenshot below shows the results of a search on demo data.

```
index=* tag=dlp tag=incident
| stats earliest(_time) as earliest latest(_time) as latest by user, signature
| where earliest >= relative_time(now(), "-1d@d")
```

Identify Basic Dynamic DNS Detection

STAGE 1

**MITRE ATT&CK Tactics**
- Command and Control
- Adversary OPSEC
- Establish & Maintain Infrastructure

**MITRE ATT&CK Techniques**
- Dynamic DNS
- Standard Application Layer Protocol

**Data Sources**
- Web Proxy
- NGFW
- DNS

**Security Challenge**
Attackers desire flexibility in their command and control capabilities, and dynamic DNS can provide that flexibility. While there are legitimate uses of dynamic DNS (many IT professionals use it to access home networks), the risks of not monitoring the practice can be significant. Fortunately, between Splunk and a list provided by Malware Domains, finding dynamic DNS in your environment is easy.

**Use Cases**
Security monitoring, advanced threat detection

**Category**
Command and control
How to Implement
The first step in implementing this detection is to acquire a list of dyndns providers. Once you download a list, you will need to format it to fit the Splunk lookup format. Once you have the file in place, the rest should move on smoothly.

Alert Volume
Medium

Known False Positives
Production services that use dynamic DNS, while rare, do happen. Those will cause some base level of false positives, although they should never be business-critical services. The most common scenario for dynamic DNS is users reaching out to their homes to see their dogs via webcam, and the like. Whether to allow – and thus tune out – these users or prohibit that activity is ultimately a policy decision.

How to Respond
When this alert fires, look for the common allowable scenarios, particularly that of users who are accessing their home networks. If that does not seem to be the case:

1. Consult data from Splunk Stream or from your packet capture to determine what type of data was sent
2. Review the DNS name and IP in open source intelligence to see if there is anything of note (although that is often hard for this scenario).
3. If this is a critical host, consider endpoint logging via Microsoft sysmon or other endpoint response mechanisms to identify the process that is creating these connections.

Identify Basic Dynamic DNS Detection Help
This example uses the simple search and the below search processing language to detect outbound communication to dynamic DNS servers on live data. First, we bring in our dataset of proxy logs. To locate dynamic DNS providers, we separate out subdomains from the registered domain using URL Toolbox. Next, we can use our lookup of ddns domains. This will add a field called inlist with the value “true” for any matches. Lastly, we can look for those records that are matches. The screenshot below shows the results of a search on demo data.

```bash
index=* sourcetype=pan:threat OR (tag=web tag=proxy) earliest=-20m@m earliest=-5m@m
| eval list="mozilla" | `ut_parse_extended(url,list)`
| lookup dynamic_dns_lookup domain as ut_domain
| search inlist=true
| table _time ut_domain inlist bytes* uri
```

<table>
<thead>
<tr>
<th>Domain</th>
<th>Inlist</th>
<th>Bytes*</th>
<th>URI</th>
</tr>
</thead>
<tbody>
<tr>
<td>ddns1.com</td>
<td>true</td>
<td></td>
<td><a href="http://ddns1.com">http://ddns1.com</a></td>
</tr>
<tr>
<td>ddns2.com</td>
<td>true</td>
<td></td>
<td><a href="http://ddns2.com">http://ddns2.com</a></td>
</tr>
<tr>
<td>ddns3.com</td>
<td>true</td>
<td></td>
<td><a href="http://ddns3.com">http://ddns3.com</a></td>
</tr>
<tr>
<td>ddns4.com</td>
<td>true</td>
<td></td>
<td><a href="http://ddns4.com">http://ddns4.com</a></td>
</tr>
<tr>
<td>ddns5.com</td>
<td>true</td>
<td></td>
<td><a href="http://ddns5.com">http://ddns5.com</a></td>
</tr>
<tr>
<td>ddns6.com</td>
<td>true</td>
<td></td>
<td><a href="http://ddns6.com">http://ddns6.com</a></td>
</tr>
<tr>
<td>ddns7.com</td>
<td>true</td>
<td></td>
<td><a href="http://ddns7.com">http://ddns7.com</a></td>
</tr>
<tr>
<td>ddns8.com</td>
<td>true</td>
<td></td>
<td><a href="http://ddns8.com">http://ddns8.com</a></td>
</tr>
<tr>
<td>ddns10.com</td>
<td>true</td>
<td></td>
<td><a href="http://ddns10.com">http://ddns10.com</a></td>
</tr>
</tbody>
</table>

This example uses the simple search and the below search processing language to detect outbound communication to dynamic DNS servers on live data. First, we bring in our dataset of proxy logs. To locate dynamic DNS providers, we separate out subdomains from the registered domain using URL Toolbox. Next, we can use our lookup of ddns domains. This will add a field called inlist with the value “true” for any matches. Lastly, we can look for those records that are matches. The screenshot below shows the results of a search on demo data.
Compliance

Detect New Data Exfil DLP Alerts for User

STAGE 1

MITRE ATT&CK Tactics

- Defense Evasion
- Persistence

MITRE ATT&CK Techniques

- Valid Accounts
- Create Account

Data Sources

- Audit Trail
- Windows Security

Security Challenge

Local admin accounts are used by legitimate technicians, but they’re also the Holy Grail for attackers. Once an attacker gets inside the network, he or she will most likely want admin privileges to gain undetected and unfettered access to desired accounts and assets. One easy way to achieve this is to compromise an existing account and then elevate the privileges.

Use Cases

Advanced threat detection, security monitoring, compliance

Category

Endpoint compromise

Splunk Solutions Required

- Splunk Security Essentials
- Splunk Enterprise

SPL Difficulty

Medium

How to Implement

First, verify that you have Windows Security logs coming in and that you have implemented account change auditing. Reference the Windows Security data source documentation if you need assistance.

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.

Alert Volume

Medium

Known False Positives

The only real source of false positives for this search would be help desk admins who create local admin accounts. If this is a 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:

- New account name
- Time of creation
- User accounts that created the account
- System that initiated the request
- Any other pertinent information
Contact the owner of the system. If the event 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. In addition to the investigation, now is a good time to ensure that the legitimate admin accounts truly need the assigned permissions and are protected by complex and long passwords.

Detect New Local Admin Account Help

This example uses the simple search and the below search processing language to look for newly created accounts that are elevated to local admin status. Our dataset is a collection of Windows Security logs with account creation events or account changes with group membership events. The screenshot below shows the results of a search on demo data.

```plaintext
index=* source="winEventLog:Security" EventCode=4720 OR (EventCode=4732 Administrators)
| transaction Security_ID maxspan=180m
| search EventCode=4720 (EventCode=4732 Administrators)
| table _time EventCode Account_Name Target_Account_Name Message
```

Find User Logged Into In-Scope System They Should Not Have

STAGE 4

MITRE ATT&CK Tactics

- Credential Access
- Privilege Escalation
- Collection

MITRE ATT&CK Techniques

- Valid Accounts
- Data from Information Repositories
- Account Manipulation

Data Sources

- Authentication
- Windows Security

Security Challenge

Under the General Data Protection Regulation (GDPR), organizations are required to maintain a complete audit trail about the authorized access of employees, vendors and/or processors to systems and applications that process personal data. GDPR gives individual citizens of the European Union and the European Economic Area the right to ask an organization where their data is stored and what entities are accessing the data.

To fulfill such a request, an organization will need to identify which employees, vendors and processors have accessed the personal data in question; and also identify and report on which other services regularly process said data. When processing personal data on behalf of a controller, there will also be a requirement to prove that only authorized individuals have accessed the data in question. If there is an audit trail that shows unauthorized access, then this will need to be documented and reported to the data privacy authorities.
By using data mapping that is reinforced by controls to detect violations, an organization can identify:

- Which employees, vendors and/or processors accessed the data;
- Where the data might be stored; and
- Which other services regularly process the data.

If you're processing data on behalf of a controller, this search can prove that only authorized individuals have accessed the data.

**Use Cases**
Insider threat, compliance

**Category**
GDPR, IAM analytics, lateral movement, operations

**Splunk Solutions Required**
Splunk Enterprise

**SPL Difficulty**
Basic

**How to Implement**
Start by using 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 on-boarded CIM-compliant data, everything should go smoothly!

**Alert Volume**
High

**Known False Positives**
This search will fire when someone who is not in the documented list accesses the data. The most likely scenario for false positives is that the documented list of authorized users is out-of-date.

**How to Respond**
Look for indications that someone should be added to the documentation, but validate with your data protection officer (DPO) or their team before making any changes. Consider automating the update of the authorized user list and pull it from the source where your DPO holds the definitive record of authorized users. Another option is to generalize and enrich the information to departments that are allowed access by enriching the username with the department names.

**Find User Logged Into In-Scope System Help**
This example uses the simple search and the below search processing language to find unauthorized users logging into in-scope systems in live data. The dataset is a collection of Windows Authentication logs that includes logins from Windows Security logs. Our search looks for the host in the GDPR categorization lookup and filters for only hosts that are in scope for GDPR. Next we look up the user in the GDPR categorization lookup, and finally look for users who don’t have a matching GDPR category or who aren’t authorized for any GDPR information. The screenshot below shows the results of a search on demo data.

```
index=* source=win*security user=* dest=*
action=succes
| bucket _time span=1d
| stats count by user, dest
| lookup gdpr_system_category.csv host as dest
OUTPUT category as dest_category | search dest_category=* 
| lookup gdpr_user_category user OUTPUT category as user_category
| makemv delim="|" dest_category | makemv delim="|" user_category
| where isnull(user_category) OR user_category != dest_category
```

<table>
<thead>
<tr>
<th>13</th>
<th>1,383</th>
</tr>
</thead>
<tbody>
<tr>
<td>13</td>
<td>1,383</td>
</tr>
</tbody>
</table>
Fraud Analytics and Detection

Detect Compromised User Accounts

STAGE 1

Data Sources
Application Logs  Web Access Logs

Security Challenge
Be it banking, credit card, email, medical or any number of accounts from myriad service providers, fraudsters can take over online accounts without your recognizing it. By leveraging phishing, spyware and/or malware scams, attackers obtain vital credential information to gain access to accounts. Some main uses of account takeovers are around credit card fraud, use of account entitlements and use of account subscriptions. By posing as the real customer, fraudsters can change account details, make purchases, withdraw funds and leverage the stolen information to access other accounts and even more sensitive data. Depending on the activity hackers may not make changes to an account and potentially will use it at the same time as the owner.

Use Cases
Fraud analytics and detection

Category
Account takeover, password list attack (credential stuffing)

Splunk Solutions Required
Splunk Enterprise

SPL Difficulty
Medium to high

How to Implement
Determine critical user accounts data and that the fields are properly extracted. You’ll also want to implement security enhancements, such as blocking bad authentications, two-factor authentications, use of Captcha on all authentications, machine learning or biometrics detections are some things you can implement. By having well thought-out enhancements it makes it more difficult to create a work around and adding any amount of friction can help prevent unauthorized access. Things like rate limiting, IP blocking and blocking bad requests can also help to limit the scale of attack.

Alert Volume
Medium

Known False Positives
None

How to Respond
These are mostly brute force attempts to take over user accounts. Investigate attacking IPs and subnets and adjust firewall rules accordingly to minimize the potential of account takeover. Notice spikes on a time chart and investigate accounts that are experiencing a high volume of attacks.
Detect Compromised User Accounts Help
Use web logs to show the behavior of a user or IP addresses, and authentication logs to help you know what accounts were actually compromised. This provides useful information in looking at high failure rates. Other account logs can also help understand if any other changes have been made, such as email changes. The data must contain information about login attempts and flag whether the attempt succeeded or failed. The search processing language is shown below. The screenshot below shows the results of a search on demo data.

```
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
```

Find Anomalous Healthcare Transactions

**STAGE 1**

**Data Sources**

**Application Logs**

**Security Challenge**
More than 400 people across the country have been charged with participating in prescription drug claim scams. Such fraud can impact regulations and requirements, making it more difficult for providers to conduct daily business and for customers to obtain prescriptions that are actually needed. This search finds nationwide and statewide anomalies in prescription drug claims.

**Use Cases**
Fraud analytics and detection

**Category**
Account takeover

**Splunk Solutions Required**
Splunk Enterprise, Splunk Machine Learning Toolkit (MLTK), Splunk Stream

**SPL Difficulty**
Medium

**How to Implement**
Datasets may be downloaded from [https://data.cms.gov/](https://data.cms.gov/). Data comes in CSV format, making it easily ingested. You can download the app in order to view the dashboard and drilldown for source SPL. However, the app already comes with CMS datasets packaged.
Alert Volume
Medium

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

How to Respond
Clicking on a provider name will open the detailed profile analysis dashboard. This allows you to investigate detailed prescription data and confirm that a provider's prescribing behavior is not matching the peer group behavior within a "nationwide provider profile versus this provider profile" chart.

Find Anomalous Healthcare Providers Help
Anomalies are shown on a map. Clicking on the yellow circle will show summary data on a specific anomaly. Clicking on a provider name will open a detailed profile analysis dashboard with specific data related to a given provider.

Insider Threat Detection

Detect Large Web Upload

STAGE 1

MITRE ATT&CK Tactics
- Exfiltration

MITRE ATT&CK Techniques
- Exfiltration Over Command and Control Channel
- Exfiltration Over Alternative Protocol

Data Sources
- Web Proxy
- NGFW

Security Challenge
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.

Use Cases
Security monitoring, insider threat

Category
Data exfiltration

Splunk Solutions Required
- Splunk Enterprise
- Splunk UBA
- Splunk simple search
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. This includes 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.

Alert Volume
Medium

Known False Positives
This search will fire for many innocent occurrences, such as uploading vacation photos and so on. 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 (executives, 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 alert fires, it will usually do so for perfectly legitimate reasons (uploading vacation photos, etc.). In response, many analysts will look to see where the data was sent and whether the user has previously uploaded data to that site. Often, analysts will call the user to confirm the activity, preferably with knowledge regarding the employee's status in the organization. For example, is the employee on a performance plan or reaching the end of a contract. Both scenarios would indicate a greater risk of data exfiltration. If you have SSL inspection turned on via your NGFW or DLP system for the destination site, you can sometimes see the actual files that were transferred, which can help provide context.

Detect Large Web Upload Help
This example uses the simple search and the below search processing language. The live search uses a dataset of proxy logs and looks for any events that are larger than 35 MB. The screenshot below shows the results of a search on demo data.

```
sourcetype=pan:traffic OR (tag=web OR tag=proxy) OR (sourcetype=opsec URL Filtering) OR sourcetype=bluecoat:proxysg* OR sourcetype=websense* earliest=-10m| where bytes_out>35000000| table _time src_ip user bytes* app uri
```
Detect Successful Login of Account for Former Employee

STAGE 4

MITRE ATT&CK Tactics
- Privilege Escalation
- Credential Access

MITRE ATT&CK Techniques
- Valid Accounts
- Account Manipulation

Data Sources
- Authentication
- Windows Security

Security Challenge
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.

Use Cases
- Security monitoring, insider threat

Category
- Account compromise, insider threat

Splunk Solutions Required
- Splunk Simple Search Assistant

SPL Difficulty
- Basic

How to Implement
If you have followed the data onboarding guides in the Splunk Security Essentials 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). If you use a mechanism other than the Splunk Universal Forwarder to onboard that data, verify the sourcetype and fields that are used. The rest is simple!

Alert Volume
- Low

Known False Positives
If your organization doesn’t 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 where acceptable post-termination activity can be expected to occur, 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 inactive. Further, try to limit the usage of accounts after the employee leaves.

How to Respond
When this alert occurs, the first thing to understand is whether it was a continuation of normal system operations (e.g., the desktop under the 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, make sure that there are no services or scheduled jobs running under that account where disabling the account outright might impact operations.
Detect Successful Login of Account for Former Employee Help

This example uses the simple search and the below search processing language to detect successful authentication activity on the accounts of former employees on live data. Our dataset is a collection of anonymized Windows Authentication logs with successful logins. A lookup shows the user status, allowing us to filter for users where either the expiration is at least a day ago or they are disabled. The screenshot below shows the results of a search on demo data.

```
index=* (source=win*security OR sourcetype=linux_secure OR tag=authentication) user=* user!="" action=success
| lookup user_account_status.csv user
| where _time > relative_time(terminationDate, "+1d")
```

Learn More.

Ready to learn more about how to improve your security posture using Splunk’s analytics-driven security? Learn to solve more than 300 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 there within your environment. Contact us to get started today!