Top 5 Use Cases for Splunk

Enterprise Security

splunk>

turn data into doing®

It's not easy to detect and respond to security events quickly. A security analyst can spend minutes (sometimes hours) on an alert. Now, multiply that by the hundreds of security alerts they have to deal with every day, and they're left with too many tickets and too few analysts. Starting to see the problem?

We need to help security teams speed up their response times while reducing the number of alerts they get. We can start by improving visibility into their environment, so they can detect and respond to threats faster. Better yet, an automated response to alert triage can turn minutes into seconds and hours into minutes — and who wouldn't want that?

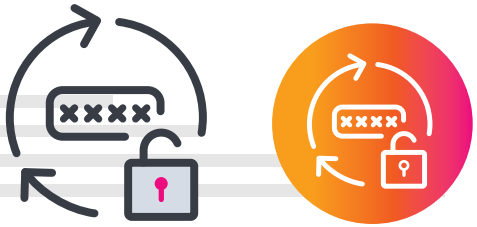
This gives hard-to-detect, insidious threats like malware fewer places to hide and propagate, and reduces the amount of damage they can cause — meaning stressed out security analysts become happier.

But even if a happy analyst sounds nice, life in the fast-paced world of security isn't always so easy, and security teams still have to figure out where to start their security journey. And, as we've established, knowing that any part of their organization is susceptible to intrusion — and that they have to identify security gaps well ahead of time — can be an overwhelming and difficult task for even the best of analysts.

Lucky for them — and security analysts everywhere — we've been working with Splunk customers for years on how to deal with this very issue. We've helped them with their toughest security questions by unlocking the answers hidden inside their data.

We've bundled those conversations into this quick guide on high-level security use cases and how to get started. These are the security issues we frequently get asked about, along with best practices for content, and ideas that will help security teams hit the ground running as they deploy or refine Splunk Enterprise Security (ES).

01



Compromised credentials

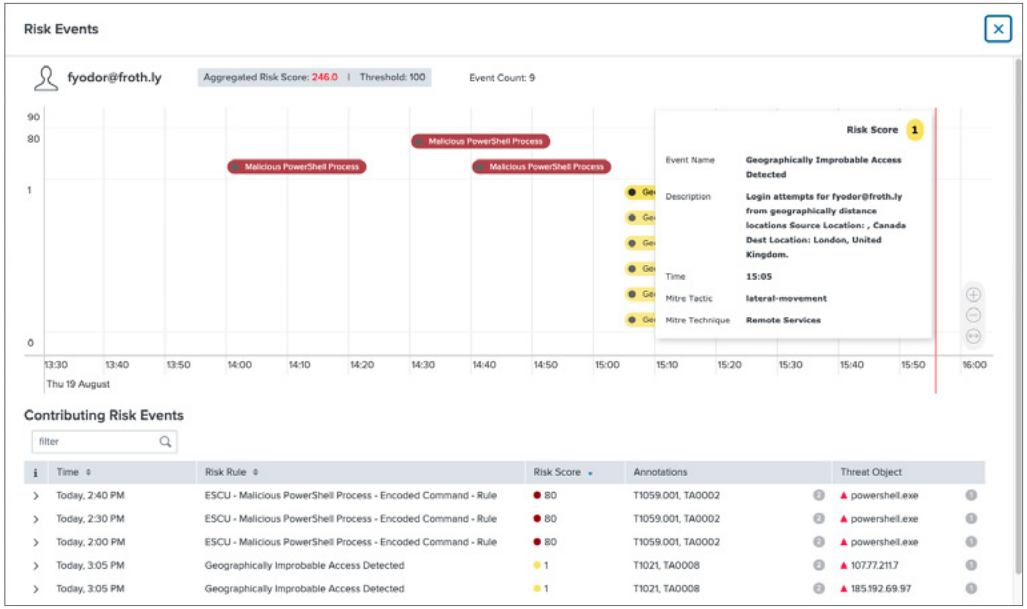
What is compromised user credentials?

Compromised user credentials is when an attacker obtains employee credentials through tried and true methods, like a phishing attack or business email compromise. Once the bad guys (and gals) have entered an environment with valid user credentials, they start looking for vulnerabilities to achieve their objective (and ruin a security analyst's day). Worst of all, since the threat actor managed to log in with valid credentials, they appear to be a totally legitimate user — making this a difficult threat to detect.

How does Splunk address compromised user credentials?

Splunk ES can identify instances where user credentials have been compromised and are being used by someone other than the authorized person or application. ES can also provide coverage for shared and generic account usage. Utilizing Splunk User Behavior Analytics (UBA)'s behavioral modeling notifies analysts when a user has unusual activity from what's been established as normal behavior. Detection encompasses identifying unusual or malicious Active Directory (AD) activity, such as operations on self, terminated user, disabled accounts and account recovery.

02



Splunk UBA helps score the severity of risk, using a baseline of normal behavior.

Privileged user compromise

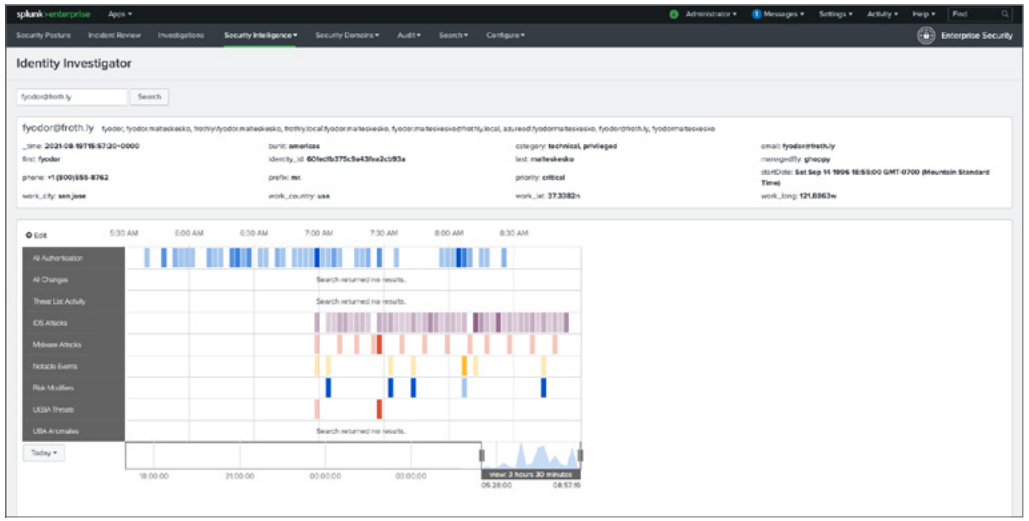
What is privileged user compromise?

Privileged user compromise is when a hacker gains access to a privileged user account through social engineering techniques or zero-day exploits. In these attacks, hackers usually target high-priority users who have administrative access to sensitive assets, or executive-level authority. This is why it's important for security analysts to immediately identify when a privileged account has been compromised. The actual technique usually involves the hacker getting around traditional security tools — like firewalls or legacy security information event management (SIEM) solutions — that are built to defend against known threats. Once the hacker is in, they start looking for ways to get more access by gathering other sensitive information, like passwords or SSH keys.

How does Splunk address privileged user compromise?

Splunk ES utilizes risk-based alerting (RBA) to detect sophisticated threats by attributing risk to users and entities, and only triggers an alert when behavioral thresholds are exceeded and certain MITRE ATT&CK tactics are observed. By building a comprehensive collection of attributions with RBA and Splunk UBA creating a baseline of the behavior of each account, it makes it easy to identify irregularities compared to the user's baseline behavior. This usually indicates excessive usage, rare access, potential sabotage or someone trying to cover their tracks. As user behavior continues to differ from known normal behavior, UBA's confidence grows, increasing the likelihood and severity of risk. Examples of detections include using service accounts to access VPN or interactive logins, data snooping, deleting audit logs and accessing confidential information.

03



An example of a Splunk dashboard to help identify insider threats.

Insider Threat

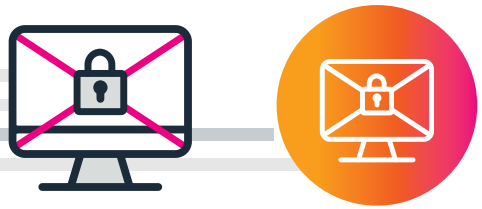
What is an insider threat?

Insider threat is when an employee or contractor with access to privileged information purposely — or accidentally — misuses their access to hurt the company they're working for. It's such a common issue that insider threats account for two-thirds of attacks or data loss. Compromised user credentials, privileged user compromise and insider threat are all related to the same general behavior, where valid credentials are exploited for nefarious reasons.

How does Splunk address insider threats?

Splunk ES and UBA captures the attacker's footprint as they move across enterprise, cloud and mobile environments. Their activity is analyzed by advanced machine learning algorithms to create a baseline, detect deviations and find anomalies in near real time. The totality of the hacker's actions within an environment are stitched into an illustrative sequence that uses pattern detection and advanced correlation to reveal the kill chain so security teams can take action immediately.

04



Ransomware

What is ransomware?

Ransomware is a type of malware that is sadly rising in popularity. This threat has even caught President Joe Biden's attention. This attack happens when hackers employ phishing attacks to force unsuspecting users into giving away their privileged access. Then the malware springs into action, encrypting some (or all) of the user's files. The bad guys then demand a ransom — thus the name — of tens of thousands (or sometimes millions) of dollars through cryptocurrency, in return for unlocking the files.

How does Splunk address ransomware?

Splunk ES receives updates from the Splunk ES Content Update (ESCU), which gives security analysts pre-packaged security content that helps them fight ongoing time-sensitive threats, attack methods and other security issues. There are currently 35 ransomware use cases provided in the ESCU, and as new threats are spotted, the Splunk Threat Research Team reverse engineers them to push out automatic updates via ESCU to ensure detections remain up to date.

05

Cloud security

What is cloud security?

Cloud security is founded on the principle that cybersecurity should move away from the perimeter, and retire its network-centric approach (which many traditional security solutions still subscribe to). For that, you can thank COVID, and our collective large-scale migration to the cloud as we moved to WFH.

Because of the rise of cloud computing — and because more companies are migrating critical parts of their business to one of the public clouds, like Google Cloud Platform (GCP), Amazon Web Services (AWS) or Microsoft Azure — it's important that organizations easily analyze their data in real time, to better obtain the visibility required to stay one step ahead of hackers.

How does Splunk bolster cloud security coverage?

Splunk ES makes it easy to onboard GCP, AWS and Azure assets and identities (A&I) information so it can seamlessly populate A&I tables within Splunk. Splunk ES also provides out-of-the-box detections for the big three cloud providers across authentication, network traffic and configuration changes. Through mapping the aforementioned cloud providers data models to Splunk's Common Information Model, a company's existing detection and investigation workflows are infused with vital cloud data coverage.

Ready to supercharge your security operations with a cloud-based data-driven SIEM solution?

Learn how to get started with Splunk.

Learn More

22-20968-Splunk-Top 5 Use Cases for Splunk Enterprise Security-LS-105

splunk> turn data into doing®