The Essential Guide to Protecting Against Supply Chain Attacks

How to detect and protect against the top 5 threats associated with cyberattacks like SolarWinds
### Table of Contents

- **Introduction** ................................................................................................................. 3
- **Understanding the Analytics-Driven Security Journey** ............................................. 4
  - Splunk Helps You Get There .......................................................................................... 5
- **How to Detect the Top 5 Supply Chain Attack Threats** ............................................ 6
- **The Top 5 Supply Chain Attack Threats** ..................................................................... 7
  - Threat 1: Lateral movement .......................................................................................... 7
  - Threat 2: Privilege escalation ...................................................................................... 9
  - Threat 3: Command and control .................................................................................. 10
  - Threat 4: Malware deployment .................................................................................... 12
  - Threat 5: Data exfiltration ......................................................................................... 13
- **Splunk Helps You Turn Data Into Action** ................................................................... 16
Today’s organizations are sharing more of their data with trusted partners and vendors than ever before. But near-instantaneous collaboration comes with a price: potential increases in security vulnerabilities as attack vectors and entry points multiply. As the recent SolarWinds supply chain attacks demonstrated, even the most sophisticated security defenses can be breached through legitimate third-party processes — and the severity of supply chain attacks cannot be overstated.

So how can you help protect your organization against them? In this guide, you’ll learn how to detect and defend against the five most relevant security threats associated with supply chain attacks, the data sources you need to detect them, and how to use Splunk to turn those insights into action. Before we dive in, it’s helpful to have an understanding of the different stages of the security journey and how Splunk is there to help every step of the way.
Understanding the Analytics-Driven Security Journey

Cybersecurity is a journey, not a destination. Like any expedition, there are always challenges along the way, and having the right equipment and expertise readily available can make all the difference. First, you must understand your environment and where to begin. What specifically needs to be protected? Where should you look for threats, what data will be critical, and how will you respond to threats along the way?

Understanding the six stages of the security journey will help you answer these questions and equip you with the tools and information you need to understand where you’re vulnerable to supply chain attacks so you can take defensive and offensive steps to protect against them.

STAGE 1
Collection
You have the data onboard — what to do now? First, collect basic security logs and other machine data from your environment.

STAGE 2
Normalization
You’ve applied the common information model, opening you to detections shared by others and premium apps. Now apply a standard security taxonomy and add asset and identity data.

STAGE 3
Expansion
You’re ingesting advanced data sources and running better investigations. Next, collect additional high fidelity data sources like endpoint activity and network metadata to drive advanced attack detection.

STAGE 4
Enrichment
You’re business aware, with Splunk aware of assets, identities, vulnerabilities and threat intelligence. Now is the time to augment security data with intelligence sources to better understand the context and impact of an event.

STAGE 5
Automation and Orchestration
You’re monitoring your SOC with Splunk, so you can establish a consistent and repeatable security operation capability.

STAGE 6
Advanced Detection
You have the highest level of detection. You’re ready for sophisticated detection mechanisms like machine learning.
Splunk Helps You Get There

Just as no expedition can be successful without packing the proper equipment, no security journey can be successful without the right technology. Splunk, the Data-to-Everything™ Platform, offers solutions to help you quickly identify, investigate and respond to threats in dynamic, digital environments, whether you’re a tier one analyst doing basic research or an advanced analyst performing complex correlations and forensics, or building analytic models.

With Splunk® Enterprise Security (ES), you can then add threat intelligence specific to supply chain attacks to your SIEM and ingest them easily. It comes preloaded with relevant threat intelligence data out of the box, so instead of doing all the manual work to set it up, you can just click a few buttons and get started. And it’s easy to add new sources of threat intelligence from the internet — just follow these steps. Once you’ve added them to your feed, Splunk ES will download and ingest the data.

When you’re ready to stay ahead of advanced and insider threats, machine learning (ML) can help. Splunk® User Behavior Analytics (UBA) is designed to find anomalies and threats involving users, applications and devices using unsupervised ML. UBA discovers anomalies from the data sources you likely already have in Splunk, and stitches them together into threats. It also provides risk scoring so that analysts can quickly understand which threats to investigate first. A rich visual environment allows analysts and threat hunters to pivot through and investigate the anomalous behavior. UBA also supports bi-directional integration with Splunk ES to drill further into the data from user behavior threats and anomalies.

If you’re ready to supercharge your security operations, you can harness the full power of your existing security investments with security orchestration, automation and response (SOAR). With Splunk Phantom, you can work smarter, respond faster and strengthen your defenses. Splunk Phantom automates repetitive tasks to better focus your team’s attention on what’s most critical. It also reduces dwell times with automated investigations, and response times with playbooks that execute at machine speed. Splunk Phantom allows you to integrate your existing security infrastructure so that each part participates actively in your defense strategy.
How to Detect the Top 5 Supply Chain Attack Threats

No matter where you are in the security journey, Splunk Security Essentials (SSE) can be your guide, helping you identify the top threats associated with supply chain attacks. Once the SSE app is installed on Splunk Enterprise, you can see your organizations’ security strengths and weaknesses in real time and get recommendations to implement more proactive security practices. You can then export those searches into Splunk to detect and respond to the threats, and even automate future detection and response playbooks.

Every organization should make full use of SSE in their Splunk environment. It contains a security content library with over 600 pre-built detections and analytic stories that are mapped to Cyber Kill Chain and MITRE ATT&CK, two of the leading cybersecurity frameworks. It also includes a customized MITRE ATT&CK matrix that visualizes active detections and what is currently available to deploy. SSE includes all the content from Splunk ES, Enterprise Security Updates and User Behavior Analytics (UBA) mapped to the same frameworks, making it easier to turn those insights into action.

As well as searching for signs of attacks that have already occurred, you can also take proactive steps to detect and protect against supply chain attacks as they unfold in real time. While the SolarWinds attacks hit, FireEye released a white paper with indicators of compromise for the Sunburst malware that were mapped to MITRE ATT&CK. These MITRE ATT&CK IDs can be used through the search function in SSE to protect yourself from the associated tactics and techniques while companies like Splunk or MITRE work on pushing out an update.

In this next section, we’ll cover the top five supply chain attack threats in detail and how you can use Splunk to detect them at different stages of the security journey, including the specific data sources you’ll need to search for them and the MITRE ATT&CK techniques for each.
The Top 5 Supply Chain Attack Threats

**Threat 1: Lateral movement**

Lateral movement describes various techniques a hacker uses to enter and control remote systems in order to move around your network. In order to find their target and gain access, adversaries often creep around the network, pivoting through multiple systems and accounts in order to gain access. They might install their own remote access tools to accomplish lateral movement, or, even stealthier — as was the case with the SolarWinds attacks — use legitimate credentials with native network and operating system tools.

**Detection:** You can detect lateral movement with techniques such as rare access or expanding resource usage monitoring. By monitoring the number of users interactively logged into assets, you can identify anomalies that may indicate the compromise of an asset or credentials. A spike in users on a particular asset could indicate that the asset has been compromised and additional system-level user accounts are being created for malicious purposes. If they’re valid credentials, accounts may have been compromised and the adversary could be testing them against a particular asset or group of assets, or escalating privileges to gain deeper access to critical assets and infrastructure. Other signs of lateral movement are when users log into new domain controllers or when there are spikes in users who log into more hosts than they typically do.

Here’s how Splunk can help you detect lateral movement at each stage of the security journey:

**STAGE 1:**

Look for instances of users logging into new domain controllers and users who log into more hosts than they typically do.

- **Data sources:** Windows security, authentication
- **MITRE ATT&CK tactic and techniques:** lateral movement, remote services

**STAGE 2:**

Search for brute force activation behavior, which can detect an excessive number of failed login attempts along with a successful attempt that could indicate a successful brute force attack. Outbreak alerts will indicate a possible outbreak based on newly infected systems all exhibiting the same infection.

- **Data sources:** authentication succeeded, authentication failed
- **MITRE ATT&CK tactics and techniques:** credential access, brute force, execution

**STAGE 3:**

N/A
**STAGE 4:**

Track employee, vendor and supplier access to systems to ensure that they’re authorized to view the data they can access. Look for suspicious network exploration and activity, such as when a user accesses a number of systems and that number increases systematically over time, as well as other unusual network interactions. With Splunk UBA, you can also look for unusual Windows Security events such as rare process, rare resource or even a rare process name for a given process, based on user baseline and enterprise baseline.

- **Data sources:** Windows security logs, authentication succeeded
- **MITRE ATT&CK tactics and techniques:** lateral movement, initial access, remote accounts, valid services, ingress tool transfer, credential access, privilege escalation and collection, execution

**STAGE 5:**

If you’re monitoring your Security Operations Center (SOC) with Splunk, you can use Splunk Phantom to automate malware investigation and response on the endpoint. Investigating and responding to malware alerts can take more than 30 minutes. By automating the investigation and response, Splunk Phantom validates that the process is malicious and takes immediate action to block the hash on the infected endpoints.

- **Data sources:** authentication, Windows security
- **MITRE ATT&CK tactics and techniques:** N/A

**STAGE 6:**

There are four advanced detections you can run at this stage in Splunk UBA that use unsupervised machine learning to detect lateral movement.

Detect activity from a user that looks like possible lateral movement in the network.

- **Data sources:** Windows security logs, authentication succeeded, basic traffic logs, app-aware traffic logs, DLP violations, HIDS events, IDS alerts, AV detection, email outgoing
- **MITRE ATT&CK tactics and techniques:** N/A

Detect a period with unusual Windows security event sequences.

- **Data sources:** Windows security logs
- **MITRE ATT&CK tactics and techniques:** persistence, privilege escalation, initial access, valid accounts

Detect suspicious data movement using multiple suspicious indicators such as users sending themselves emails and external DLP alarms.

- **Data sources:** DLP violations, email outgoing, removable storage file audit, proxy requests, app-aware traffic logs, user-aware traffic logs
- **MITRE ATT&CK tactics and techniques:** collection, exfiltration, data from information repositories, data from network shared drive, exfiltration over C2 channel, exfiltration over alternative protocol, exfiltration over other network medium

Detect rare or unusual machine access.

- **Data sources:** Windows security logs
- **MITRE ATT&CK tactics and techniques:** initial access, privilege escalation, valid accounts
Threat 2: Privilege escalation

Attackers are increasingly using privileged user credentials to access corporate resources and sensitive information and exfiltrate sensitive data. These are accounts with elevated privileges, such as users with domain administrator rights or root privileges. Hackers gain access to them by using social engineering techniques, malware, spear-phishing or “passing the hash” attacks. If an attacker gains privileged account access credentials, their activities appear more legitimate and become harder to detect. Effective privileged user monitoring (PUM) helps you protect critical assets, meet compliance requirements and mitigate both external and insider threats.

Detection: You can detect privilege escalation attacks when a new user logs on with local credentials that bypass most centralized logging and policy systems. Local credentials enable a user (or attacker) to bypass some auditing controls and maintain ongoing access. You’ll also want to search for modifications to registry keys that can be used to elevate privileges and look for any non-privileged users taking privileged actions they shouldn’t be.

Here’s how Splunk can help detect privilege escalation at each stage of the security journey:

STAGE 1:
Use Splunk ES to identify, search and report on the activities of users with privileged accounts and help protect your environment from malicious attackers. Search for when a user with administrator privileges has deleted, disabled or changed the passwords of multiple accounts. Also, because most interactive logins should use domain credentials, look for new users logging on with local credentials that bypass most centralized logging and policy systems (but not Splunk’s). And with Splunk UBA, you can be alerted when an anomalous account is created on a workstation or endpoint.

- Data sources: Windows Security, Azure, GCP, audit trail, user activity audit, AWS, authentication
- MITRE ATT&CK tactics and techniques: persistence, initial access, credential access, valid accounts, local accounts, account manipulation

STAGE 2:
N/A

STAGE 3:
N/A

STAGE 4:
N/A

STAGE 5:
N/A

STAGE 6:
N/A
Threat 3: Command and control
In a command and control attack, hackers take over a computer in order to send commands or malware to other systems on the network. With malicious software installed on the endpoint, the malware communicates with a command and control server to download additional software or to receive instructions. Instructions can include specific files or data to be stolen from the target organization. The communication between the victims and the command and control servers often uses common communications protocols that are hidden in plain sight in HTTP, FTP and DNS protocols. The communication may also be encrypted by using SSL over HTTP or by using remote control protocols like RDP.

Detection: You can identify compromised network endpoints that are infected by malware or are otherwise behaving suspiciously. A command and control attack is different than a compromised user account attack in that malicious activity might be detected on a host, but not necessarily linked to a specific user account. For example, command and control traffic can be identified from a system where no user is currently logged in.

Behavior-based modeling enables Splunk UBA to identify malware activity regardless of the initial method of infection by tracking changes in communication patterns of devices, the nature of communication with external domains or IPs, or characteristics of the domains.

Threat 3: Command and control
Here’s how Splunk can help you detect command and control at each stage of the security journey:

STAGE 1:
The anonymity of TOR makes it the perfect place to hide command and control, exfiltration or ransomware payment via bitcoin. Basic TOR traffic detection looks for ransomware activity based on FW logs.

- Data source: network communication
- MITRE ATT&CK tactics and techniques: exfiltration, command and control, exfiltration over C2 channel, exfiltration over alternative protocol, application layer protocol and non-application layer protocol, proxy and multi-hub proxy

STAGE 2:
Look for browsing in new domains that users have never before used in your organization. Savvy threat hunters know that when users browse to new domains, it can mean the system connects to a command and control server or a staging server containing malware.

- Data source: web proxy
- MITRE ATT&CK tactics and techniques: exfiltration, command and control, exfiltration over C2 channel, exfiltration over alternative protocol, application layer protocol
STAGE 3:
Search for a long DNS TXT record response to detect attackers attempting to use DNS tunneling. Endpoints using DNS as a method of transmission for command and control can often be detected by noting unusually large volumes of DNS traffic. This is best handled in Splunk with the advanced Splunk ES feature Splunk Enterprise Security Content Updates (ESCU).

- Data source: DNS queries and responses unified
- MITRE ATT&CK tactics and techniques: exfiltration, command and control, commonly used port

STAGE 4:
Search for excessive DNS query failures by counting the number of DNS responses that don’t indicate success and trigger on more than 50 occurrences. This is also best handled in Splunk ESCU.

- Data source: DNS responses
- MITRE ATT&CK tactics and techniques: exfiltration, command and control, exfiltration over alternative protocol, commonly used port

STAGE 5:
Threat hunting can be a repetitive process to either enrich threat data or leverage curated data relevant to the network. Automating this process allows for deeper investigations. With Splunk Phantom, you can run an automated IP investigation and report playbook to determine if an IP address is malicious and automate threat hunting for internal sightings of malicious files or connections to malicious domains or IP addresses.

- Data sources: network communication
- MITRE ATT&CK tactics and techniques: N/A

STAGE 6:
N/A
**Threat 4: Malware deployment**

Countless types of malware exist, and threat actors are constantly developing unique tactics to deploy them. And hackers have an increasingly sophisticated range of tools to distribute malware, expanding and deepening their reach. Malware deployment is such a broad category of threat that it requires multiple searches and detection techniques at different stages of the security journey to find, depending on the particular attack.

**Detection:** To protect against malware deployment, use both Splunk ES and Splunk UBA for advanced stage threat detection and security monitoring. With Splunk UBA, you can find anomalies and threats involving user, application and device behavior using unsupervised machine learning. Splunk UBA discovers anomalies from the data sources you likely already have in Splunk and stitches them together into threats. It also provides risk scoring so that analysts can quickly understand which threats to investigate first. A rich visual environment allows analysts and threat hunters to pivot through and investigate the anomalous behavior.

Here’s how Splunk can help you detect malware deployment at each stage of the security journey:

**STAGE 1:**
N/A

**STAGE 2:**
N/A

**STAGE 3:**
N/A

**STAGE 4:**

At this stage, you can use Splunk UBA to run two searches that can detect malware.

Use Splunk UBA to search for privilege escalation occurring after a suspicious PowerShell command.

- **Data sources:** Windows PowerShell logs, Windows security logs
- **MITRE ATT&CK tactics and techniques:** N/A

With Splunk UBA you can also do a broad search for any unusual Windows security events, including unusual event code, process, directory, login type, return code and domain. This can contain things like rare process, rare resource, or even a rare process name for a given process, based on user baseline and enterprise baseline.

- **Data sources:** Windows security logs
- **MITRE ATT&CK tactics and techniques:** execution

**STAGE 5**

Use Splunk Phantom with automated threat hunting to search for internal sightings of malicious files or connections to malicious domains or IP addresses.

- **Data sources:** host-based IDS, IDS or IPS, DLP, anti-virus or anti-malware
- **MITRE ATT&CK tactics and techniques:** N/A

**STAGE 6:**

N/A
Threat 5: Data exfiltration

Data exfiltration is the unauthorized transfer of data from a computer or other device, often automated through malicious programming over a network. These attacks are typically targeted to gain access to a network and locate and copy very specific data. Since even authorized users can commit unauthorized or malicious data exfiltration, even with the ability to detect compromised accounts and endpoints, you need to be able to search for data exfiltration as a distinct threat.

Detection: Data exfiltration is a broad threat area, so there are several searches you should run at different stages of the security journey to detect it. Detection can be difficult because it involves transferring or moving data both within and outside a company’s network and can closely resemble typical network traffic.

For advanced threat detection stages, Splunk UBA detects data loss or theft in an enterprise across multiple threat vectors such as network security infrastructure (including firewall and proxies), online cloud storage, attached storage (including USB devices) and email.

Here’s how Splunk can help you detect data exfiltration at each stage of the security journey:

STAGE 1:

There are four different searches you can run at the first stage in order to detect data exfiltration.

Look for common credential patterns in log files. Attackers may dump credentials into local files using OS credential dumping, or credentials might have been left in files by mistake. In cloud environments, authenticated user credentials are often stored in local configuration and credential files.

- Data sources: any Splunk logs
- MITRE ATT&CK tactics and techniques: credential access, unsecured credentials, exploitation for credential access, credentials in files, private keys

Search for high-volume printing. Though it may seem old-fashioned, users printing more pages than normal can be a sign of data exfiltration. You can also correlate this behavior to a watchlist which may contain the user IDs of personnel who are considered higher risk: contractors, new employees, employees who never go on vacation or employees with access to particularly sensitive data.

- Data sources: user activity audit
- MITRE ATT&CK tactics and techniques: exfiltration, exfiltration over physical medium

Look for large web uploads. 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.

- Data sources: web proxy
- MITRE ATT&CK tactics and techniques: exfiltration, exfiltration over C2 channel, exfiltration over alternative protocol

A sophisticated and increasingly common data exfiltration technique is to send out a huge volume of DNS traffic (in bytes) or ping requests embedding data into the payload, which is often not logged. One way to look for these attacks is to gauge the total bytes transferred and look for anomalies and deviations from normal DNS traffic levels.

- Data sources: network communication
- MITRE ATT&CK tactics and techniques: exfiltration, command and control, exfiltration over alternative protocol, application layer protocol, exfiltration over C2 channel
STAGE 2:

Look for users browsing to new domains, which can indicate that your system is connecting to a command and control server or a staging server containing malware.

- **Data source:** web proxy
- **MITRE ATT&CK tactics and techniques:** exfiltration, command and control, exfiltration over C2 channel, exfiltration over alternative protocol, application layer protocol

Search for users accessing a cloud storage provider they’ve never used before. Data exfiltration techniques vary across the world, but a common approach is to upload data to a non-corporate file storage solution. Identifying new file storage solutions in your environment will help you track where data flows in your organization along with the adoption of shadow IT.

- **Data source:** web proxy
- **MITRE ATT&CK tactics and techniques:** exfiltration, command and control, exfiltration over alternative protocol, web service

STAGE 3:

There are five different searches to run in stage three: first-time Git access, new Salesforce.com clients, public open cloud storage, security group ACL changes and outgoing email.

Search for first-time Git access. Your developers are often granted access to the Git (or another software life cycle repository) that their responsibilities require, but keep an eye out for users accessing an internal Git repository for the first time. Though it could be perfectly normal, if the repository contains code not relevant to the developer’s role, it could be an anomaly to investigate.

- **Data source:** web server
- **MITRE ATT&CK tactics and techniques:** collection, data from information repositories

Because Salesforce.com often contains an organization’s most critical information, run a search for users who connect to Salesforce.com’s reporting API with new clients.

- **Data source:** audit trail
- **MITRE ATT&CK tactics and techniques:** collection, data from information repositories

Search for when a new or existing public storage service, such as an AWS S3 bucket, is set to public. Open cloud storage (such as an S3 bucket or Azure Blob) is an extremely common way for breaches to occur these days. People host files for quick transfer but forget to take them down, or use storage for backups of sensitive data but inadvertently mess up permissions. Monitor and pull data quickly from newly created storage. If you have a corporate cloud environment, you should prioritize analyzing any open storage. You may even wish to automate their remediation through AWS functions or Splunk Phantom.

- **Data source:** audit trail, AWS, Azure, GCP
- **MITRE ATT&CK tactics and techniques:** N/A

Look for a large number of security group ACL changes in a short period of time for a user. This can be a sign that an IaaS environment has been compromised and security group (firewall) ACLs designed to protect an environment are thrown open, allowing outside connections in, data exfiltration or lateral movement from one group to another.

- **Data source:** audit trail, AWS, Azure, GCP
- **MITRE ATT&CK tactics and techniques:** persistence, privilege escalation, valid accounts, cloud accounts

Search for users with increases in outgoing email. When users are sending out dramatically more data than normal via email, it can be a sign of data exfiltration and compromised accounts.

- **Data source:** email
- **MITRE ATT&CK tactics and techniques:** exfiltration, exfiltration over alternative protocol
STAGE 4:

Detecting data exfiltration after data staging is best performed with Splunk UBA, using advanced threat detection methods that combine staging data and data exfiltration threats.

- **Data sources:** proxy requests, user-aware traffic logs, basic traffic logs, box logs, DLP violations, HIDS events, IDS alerts, AV detection, app-aware traffic logs, app logs, removable storage file audit
- **MITRE ATT&CK tactics and techniques:** N/A

Another search builds off of the search for new Git repositories access search to find users who accessed a Git repository for the first time, where their peer group also hasn’t accessed it before. Your developers are often granted access to the Git (or other software life cycle repository) that they require, but why would they be gaining access to other repos that other members of their team (e.g., peer group) never access? This could be an alertable condition. In order to perform searches like this you must map your users into peer groups, which can be done via a simple Splunk lookup, but could be done more easily via automation. Splunk UBA contains its own methods of discovering peer groups for individual users.

- **Data source:** web server
- **MITRE ATT&CK tactics and techniques:** collection, data from information repositories

Search for a high volume of outbound traffic from a high-severity or critical host, which may indicate that the host has been compromised. This can be done in Splunk Enterprise with a lot of effort but is more easily accomplished with Splunk ES.

- **Data source:** proxy requests
- **MITRE ATT&CK tactics and techniques:** exfiltration, exfiltration over alternative protocol, exfiltration over C2 channel

With Splunk UBA, you can search for users who are possible flight risks.

- **Data sources:** email outgoing, proxy requests, app-aware traffic logs, box logs, DLP violations, HIDS events, IDS alerts, AV detection, removable storage file audit, app logs
- **MITRE ATT&CK tactics and techniques:** N/A

Splunk UBA also helps you find unusual network activity through a large number of detections for rare or unusual network interaction.

- **Data sources:** basic traffic logs, app-aware traffic logs
- **MITRE ATT&CK tactics and techniques:** command and control, custom cryptographic protocol, custom command and control protocol, uncommonly used port

STAGE 5:

At this stage, you can use a Splunk Phantom playbook that executes multiple investigative actions to determine if an IP address is malicious and sends a summary of the output in an email. Using this playbook to investigate an IP address, security teams can quickly assess whether or not an IP is malicious as well as additional information if there are any domains pointing at it.

- **Data sources:** network communication
- **MITRE ATT&CK tactics and techniques:** N/A

STAGE 6:

Finally, at the most advanced stage of the security journey, you can search for excessive data transmission. A common sign of attempted data exfiltration is when there is more than expected data transfer for a user or device.

- **Data sources:** app-aware traffic logs, user-aware traffic logs
- **MITRE ATT&CK tactics and techniques:** exfiltration, exfiltration over alternative protocol, exfiltration over C2 channel
No matter where you are in your data security journey, Splunk, the Data-to-Everything Platform, offers you the data and insight you need to defend against supply chain attacks — or any other threat you encounter along the way. Our scalable and reliable platform provides the tools you need to investigate, monitor, analyze and act on your data, from any source, at any speed and on any timescale. We are the only company in the industry that can guide you through all stages of your data journey across IT, security and other core business functions, which means smarter technology investments, less complexity and fewer barriers between data and action.
Learn More.

To learn more about how to detect supply chain attacks with Splunk Enterprise Security, join us for this security tech talk.

Sign Up