SECURITY ESSENTIALS

# Essential Security Foundations:

## Monitoring Basic Security Posture

splunk>
turn data into doing™

Most cybersecurity tools are designed to help identify and alert on a particular type of malicious activity. But usually the burden lies with the organization to figure out whether the alert is meaningful in a broader context.

Splunk helps centralize analysis and visibility across a multi-layered security environment, enabling security teams to quickly gain insight into whether they need to investigate deeper.

This is the first step in effectively improving your organization's security planning and preparedness, or security posture.

With Splunk, you can quickly get answers to some of your more pressing questions about security posture, including:

- How secure are my endpoints?
- What's happening on my network?
- Where is it critical to apply updates?
- Are user accounts configured properly?
- Is there any suspicious traffic going out?
- Are there unexpected changes in my AWS environment?

## Fast Track to Better Security Posture

Start with collecting and analyzing host, network, antivirus and cloud activity, which are common to nearly every IT environment.

Windows and Linux/*nix host activity can reveal potential security and compliance issues. Login activity and process-related events are a great place to begin.

Firewall, proxy and email logs can provide critical insights into communication activity that might warrant deeper investigation — for example, theft of intellectual property or personally indentifiable information/ personal data, as well as command and control, or phishing attempts.

Antivirus (AV) and endpoint detection and response (EDR) logs can provide key insights into process-level, file-level and user-level activity, which can help identify a range of threats spanning viruses, malware and spyware.

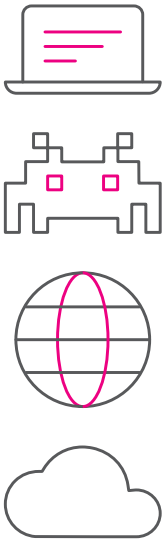
Unexpected AWS activity or misconfigurations can help identify whether there's a security issue that needs deeper investigation (e.g., user activity, change to topology or security policies, utilization).

## Key Areas to Start With

*Basic Network, Basic Windows, Basic Malware and Basic AWS*

Security architectures typically consist of multiple layers. Three commonly deployed layers can be leveraged immediately to gain critical security insights into security posture, including Windows and Linux hosts, firewalls and antivirus. These are common to nearly every IT environment. Many organizations also use AWS Monitoring activity in this environment to provide valuable security insights from an overall cloud context, as well as in relation to overall security posture.

Leverage these four basic data sources to improve security posture quickly




## Basic Windows and Linux Posture

Starting with Windows and Linux hosts, analyzing login activity and process-related events can reveal an early indication of malicious intent. Authentication is the basis of lateral movement, as well as access to assets and intellectual property.

### Login success/failures

Patterns found within login success and failures can point to unusual or malicious activity — such as brute force attempts, and attempts to discover internal or external resources — either as a stepping stone to a more valuable asset, or with the intent to take over administrative control.

### New account logins

Unexpected "new accounts" or "first-time-seen" logins can point to privileged credential abuse, or credential sharing.

### Anomalous logins

Anomalous activity may show up as a higher number of login attempts than normal, a sudden flurry of login activity to multiple assets from the same account, or login attempts from multiple locations at the same time. These can indicate the unauthorized sharing or abuse of credentials, or a compromised account.

### New processes

Once unauthorized access to a host has occurred — or once malware has established a foothold — new processes may appear that seem legitimate. Examples of this include fake system processes that appear to be part of the operating system, which evade traditional detection mechanisms via "legitimate" filename or signature-based parameters.

## Basic Network Posture

The network is a critical domain to inform on how to maintain and improve security posture — since all communications between devices, applications and users need to traverse the network. Firewall data in particular can provide critical insights into these communication patterns that might point to an actual security issue that needs investigation or remediation, such as theft of intellectual property or beaconing to a command and control server.

### Top apps consuming bandwidth

Applications that suddenly exhibit a change in the amount of bandwidth consuming can indicate a compromise. The root cause may be data exfiltration or command and control activity to a known bad host.

### Top protocol use

This is a key indicator in determining whether protocol use is beyond what is expected — for example, if there is a large amount of traffic headed to a TOR network, or SMB traffic leaving the corporate network. This may be caused by malware establishing a command and control channel or attempting to download additional malware components such as ransomware encryption modules.

### Top bandwidth consumers

Sudden changes in bandwidth usage can indicate data exfiltration or other unauthorized activity, such as malware delivery.

### Top blocked executables

Variants may pass through undetected if they're not a match on a signature, hash value or filename — at least until a sandbox detonation can occur to verify the results. This metric provides context into what malware strains are most commonly being deployed in a phishing or malware campaign, and insight into the subsequent behavior of successful infection attempts.

## Basic Malware Posture

Antivirus solutions can provide key insights into process-level, file-level and user-level activity, such as system or host-level information — including process, network, file info and, depending on the solution, a range of threat types spanning virus, malware and spyware, to whitelisting and behavioral evidence. The endpoint is a data gathering and launch point for most malware-based exploitation, so this is another critical data source that should be viewed as foundational to immediately gain improvements in security posture.

### Top risks detected

Antivirus can calculate the risks associated with particular vulnerabilities and their known exploits, and this metric can help inform prioritization on handling large volumes of suspicious and abnormal events.

### Top processes blocked

Having full visibility into known and unknown applications is a critical endpoint methodology. This metric can provide deep insights into malicious activity and what it can mean, especially when looked at in the context of frequency, time, users and other parameters that can help determine whether there is a larger issue at hand, such as a targeted phishing campaign.

### Top viruses/spyware detected

Viruses and spyware are still important to filter out, especially in environments that use older or unsupported operating systems that may not be patchable. Additionally, new malware that leverages delivery mechanisms of older virus or spyware strains continues to evolve and be used in recon or delivery attempts, including ransomware and bitcoin mining payloads.

### Malware client version reports

This is a critical metric not only in terms of protection, but also in adhering to compliance requirements and other regulatory standards or mandates.

### Malware virus definitions version reports

Knowing whether endpoints have installed updates for virus definitions is critical to maintaining compliance and ensuring that uncleaned infections don't propagate, and/or that cleaned infections do not reinfect the host.

Security Posture Defined

## Basic AWS Posture

Real-time monitoring and visibility into your cloud or multicloud environment can help provide critical security insights. Whether it's one service or many, cloud solutions and infrastructure can offer challenges amid their benefits. Not being able to monitor and control data in and out of the cloud could cause security headaches down the road. For instance, just having real-time visibility into your AWS environment can go a long way. Unexpected changes in network ACLs, security groups, IAM activity; or S3 could indicate a security issue that needs to be investigated.

### Security groups

Security groups act as firewalls to control inbound and outbound traffic for an EC2 instance deployed within a VPC. Monitoring security group activity for unusual or unexpected changes can provide key security insights. For example, a sudden change in the number of security group rules could indicate an issue worth investigating.

### Network ACLs

Network ACLs are an optional layer of security, and can provide high-level security insights related to how traffic is going into and out of VPC subnets. A sudden change in the number of ACL modifications can often indicate an issue worth investigating.

### IAM activity

Monitoring IAM activity can help determine whether there are any issues related to how users are accessing AWS services and resources. For example, if there is a spike in unauthorized attempts to perform certain actions (e.g., creating/ deleting access keys or user accounts).

### S3 buckets

Monitor S3 buckets to ensure they are properly configured — for example, S3 buckets should not be publicly accessible.

## Implementing Basic Monitoring Techniques Within Splunk

*Here are some straightforward techniques you can apply within Splunk, to help you get started:*

### Basic Brute Force Detection

Discovering a user's credentials is a key strategy for attackers. A common technique is to guess a weak password by trying hundreds of commonly used ones. Since most environments use Active Directory as their central storage repository for credentials, looking for brute force activity in Windows Security logs should be a component of any security strategy.

**Data source(s):** Windows Security

**What to look for:** Failed login attempts by a source followed by a successful login from the same source.

### Basic Scanning

Scanning is a way for adversaries to discover the attack surface of an organization's network. It should only ever come from an authorized source (e.g., vulnerability scanners). If someone else is scanning your network, this typically warrants verification and a deeper investigation.

**Data source(s):** Firewalls, proxies

**What to look for:** Attempt by a host to reach many hosts or ports in a short period of time.

### Successful Login by Former Employee

Typically, user accounts of former employees shouldn't show any activity once they've left the organization. If they've logged in since, it could mean their credentials were compromised, or that they're trying to log in to perform unauthorized actions.

**Data source(s):** Authentication, Windows Security

**What to look for:** Any login activity from a user account of a former employee.

### Large Web Upload

Data exfiltration usually occurs over standard channels, with insiders uploading data to Google, Dropbox, Box, smaller file sharing sites or even unlisted drop sites. Because outbound HTTPS sessions are often allowed, exfiltration becomes relatively easy within most organizations.

**Data source(s):** Web proxy

**What to look for:** Uploads over a certain threshold to specific cloud applications.

### Public S3 Bucket in AWS

Open S3 buckets are commonly used in data breaches. Hosted files that should be deleted may not be, or permissions may be misconfigured on S3 buckets that are used as a backup for sensitive data. Newly created S3 buckets are monitored and data is quickly pulled. This is a basic methodology for any corporate AWS environment, and priority should be given to monitoring and analyzing any open S3 buckets.

**Data source(s):** Audit trail

**What to look for:** Any S3 buckets configured to be publicly accessible along with any associated activity.

### Basic Malware Outbreak

When the same malware occurs on multiple systems, this could indicate your organization is on the brink of a larger incident, as has been seen frequently with worms, ransomware and broad phishing campaigns.

**Data source(s):** Antivirus

**What to look for:** Any identical malware occurrences on multiple systems within a short timeframe.

## Disabled Windows Update Service

Keeping up with patch maintenance is a critical part of effective cyber-hygiene. Windows-based systems are especially at risk when unpatched, considering the number and frequency of exploits that use Windows vulnerabilities to establish a foothold, move laterally or propagate.

Windows-based systems that stop updating may be the target of malicious activity, or may simply be the result of an environmental change, other configuration issue on the host or scheduled downtime. If the update service itself it disabled on the host, then it may indicate a compromised system.

**Data source(s):** Windows events

**What to look for:** Windows systems with Windows Update service disabled.

## Multiple Infections on Host

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

**Data source(s):** Antivirus

**What to look for:** Hosts that have logged multiple different infections within a short time period.

## Fake Windows Processes

Malware and other malicious activity will often attempt to hide itself, often by running as a seemingly legitimate process. Malicious processes typically run from odd locations, instead of normal system directories such as Windows\System32 or Windows\SysWOW64.

**Data source(s):** Endpoint Detection and Response, Windows Security

**What to look for:** Processes with legitimate process names, that typically run out of Windows\System32 or Windows\SysWOW64, but instead are running from another location. For example, ransomware often spawns processes that use legitimate process names in order to disguise itself, but will run from odd locations such as the desktop or \temp folders.

## Emails With Lookalike Domains

Sending emails from a domain that is very similar to a legitimate one is a common phishing technique. For example, instead of coming from@splunk.com, the domain in the address will be @spiunk.com.

**Data source(s):** Email

**What to look for:** Incoming emails from domains similar to your organization's domain name(s), but with a slight variation (e.g., a missing letter or misspelling).

## New Local Admin Account

Local admin accounts are often used by attackers. This method looks for newly created accounts that are elevated to a higher level of privilege.

**Data source(s):** Audit trail, Windows Security

**What to look for:** Recently created accounts with local admin-level privilege.

### Start Improving Your Security Posture Now

Splunk enables better control over your organization's security posture, which in turn helps you get insightful answers that much quicker — including the root cause of an attack and its impact.

Quickly gain the visibility you need to assess posture, which in turn will help streamline investigations and enable you to make better, faster, more accurate security decisions.

splunk>

Learn more: www.splunk.com/asksales

www.splunk.com



20-13315-SPLK-Essential-security-foundations-106-WP