The Big 8: Supercharging Your SIEM with the Right Data Types

Hurricane Labs has identified eight data types that are important for SOC engineers and managers to be aware of for a comprehensive SIEM implementation. The following list, which we refer to as "The Big 8," is a helpful reference during the Splunk Enterprise Security (ES) onboarding phase. Specifically, these sources cover the most ground in ES as well as in Hurricane Labs' base set of alerts.

Enter: The Big 8

1. Firewall

BENEFITS

- Firewalls can inspect all data that enter and exit the network.
- Having a detailed record of the allowed and blocked traffic flow can be useful from a SIEM perspective.

CHALLENGES

- Everything you want to see is not necessarily logged by default.
- Firewall data can take up a lot of space–the larger the network, the more data you will need to save.

2. Proxy

BENEFITS

- Proxy data provides greater insight into web activity (e.g., IP, Domain, and URL) than only using firewalls alone. Note: most malware activity is equivalent to web browsing from an application level.
- If the proxy decrypts SSL, it provides significantly more insight into communications and payload.

CHALLENGES

- With more insight into communications, however, comes more complications of privacy concerns due to the increase in data and the amount of logs it generates.
- Proxy logs often experience the same "true source" challenge that DNS logs do.

3. Antivirus/EDR Solutions

BENEFITS

- Antivirus (AV) software can help you identify sources of malware infections as well as threats that are flagged but unable to be cleaned.

  Note: Ensure file hashes, if any, are extracted. File hashes enable pivoting to external lookup sources (e.g., VirusTotal) to better assist in investigations.

- Newer antivirus solutions often look at malware behaviour as well as malicious file hashes. These can occasionally find activity that could have been bypassed by changing a files hash value.

CHALLENGES

- AV programs are still far from perfect. You'll want to keep the software up to date for the latest signatures to be added. It can't see a threat if it doesn't know about it.
- AV and Endpoint Detection and Response (EDR) solutions are NOT a catchall solution. Although they help prevent known infections, they often will not catch advanced malware designed to evade AV solutions.

4. DNS

BENEFITS

- Depending on your environment, DNS logs are packed with security-actionable data, but they are also often overlooked. Nearly every outbound communication first relies on a DNS query to obtain the correct IP address to use.
- With SSL, DNS remains an easy way to view system communication patterns in a human-readable way.
- DNS can identify the "patient zero" of a compromise (if the true source is logged. See below).

CHALLENGES

- Identifying the true source of the request can be a bit tough. For example, knowing your DNS server made the DNS request isn't as useful as determining what endpoint made the DNS request.
- The volume of data is huge, as is almost every communication requiring a DNS request. Consider filtering some requests to reduce data volume.
- DNS logging needs to be set up in a way where you can determine what end-device made the query. If you cannot determine this, the logs will not be anywhere near as beneficial.

5. Authentication

BENEFITS

- Authentication provides insight into account usage and user behavior.
- Authentication provides information that answers specific questions including:
  - What information is being accessed and/or modified in your environment?
  - What users are connecting successfully and from what locations?
  - Are there anomalous login patterns or a significant increase in activity?

6. IDS/IPS

BENEFITS

- Intrusion detection systems (IDS) or intrusion prevention systems (IPS) can identify threat types based on network activity (e.g., malware and ransomware). Logs from these tools are all rich intelligence sources for SOC analysts.

CHALLENGES

- Signature-based detection is inherently limited.
- To have effective IDS alerting, you need to spend time tuning it and adjusting it in your environment based on information about your critical assets.
- IDS alerts will continuously need attention and review to be effective due to new signatures constantly coming out. Note: you need to whitelist the signatures that do not pose a threat to your environment.

7. Email

BENEFITS

- Email can be powerful when it comes to identifying potential phishing/spam emails and can help you proactively block attack attempts.
- Email can also be leveraged for forensics purposes after a security incident.

CHALLENGES

- If you are attempting to alert on phishing attempts, it is quite difficult to do so without some sort of product like Proofpoint. End users are generally unreliable when determining what emails are spam versus what emails are legitimate phishing.

8. Vulnerability Management Data

BENEFITS

- Vulnerability scanners can be used to identify hosts running outdated or vulnerable software. Vulnerability data can be used to determine if certain (vulnerable) applications are worth keeping and/or necessary on all systems.
- Vulnerability management data can provide insight into the likelihood of a successful attack on a given host.
- Vulnerability data can be leveraged in tracking remediation efforts. It can provide metrics (e.g., time to remediation, which assets are most vulnerable, and alert severity percentages) for a better understanding of what areas need strengthening.
- Lastly, they can be leveraged to increase or reduce the severity of alerts.

Additional data sources worth noting

Asset and Identity Information

Asset and identify data sources include both server and user information. This source can help you determine who is who, what is what, and what or who does what. This item could actually be number “0” in the list.

Audit Logs

Audit logs are valuable as a means of examining what activities have occurred on a system–typically for diagnostic performance purposes. Often these logs are a prime target for attackers looking to cover their tracks, so administrators must configure audit logging to enforce strong access control around audit logs.

Audit logs are useful for establishing baselines as well as understanding the nature of security incidents, both during an active investigation and post mortem analysis phase.

Connection/Flow Logs

Some firewall logs include connection data, but others don’t. Having connection data is vital to confirm a connection’s successfulness, the duration of that connection, and the amount of bytes that were transferred during the connection.

Process Logging (Sysmon)

We have some big advocates for Sysmon here at Hurricane Labs. Any sort of EDR, like Sysmon, that provides process execution logs is advantageous for your SIEM. Also, Sysmon is basically a free EDR suite itself. It may be a bit challenging to set up, but the data returned is extremely valuable with proper tuning.

SSL Certificate Data

SSL certificate data is very valuable when investigating incidents. Many network security monitoring (NSM) suites offer the ability to passively collect SSL certificate information, referred to as x.509 data. Have you ever visited a website and asked your web browser to show you the SSL certificate? That is x.509 data. This information can help answer some of the following questions during an investigation:

- What is the subject name (e.g, to which server does this certificate apply)?
- Who issued the certificate (e.g., is it self-signed or was it provided by Lets Encrypt or another Certificate Authority)?
- Are there alternate DNS/hostnames the certificate applies to?

NSM products sometimes provide SSL connection logs as well. These logs may provide JA3 and JA3S hashes. Think of JA3/JA3S as a way to fingerprint SSL connections from a client (JA3) and responses from the server (JA3S). Simply verifying the JA3 fingerprints can be useful for uncovering new infrastructure related to existing

How Hurricane Labs can help

Our dedicated SOC team strives to empower you to get the most out of your SIEM solution–and prioritizing data types is a great place to start. With regular review, you will be able to identify which alerts need more context and expand from there. If you have any questions, don’t hesitate to reach out. Our security team is happy to help!

P. 216-923-1330 | 888-276-4106

E. sales@hurricanelabs.com