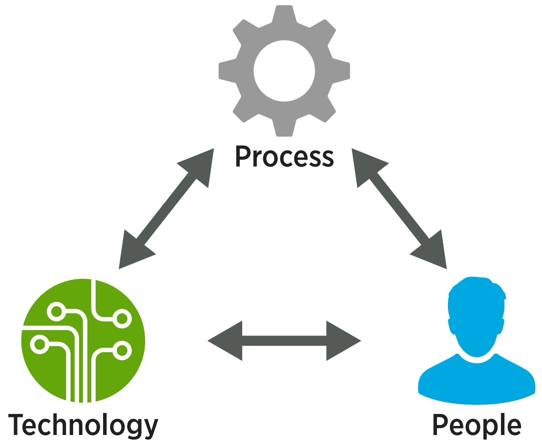
splunk>

TECH BRIEF

BUILDING A SOC WITH SPLUNK®

Splunk software can make your SOC more effective and improve your security posture

- **A SOC requires an investment in process, people and technology**
- **Splunk software can be used as a security intelligence platform to power your SOC**
- **Splunk software makes SOC personnel and processes more effective**
- **Splunk software can complement an existing SIEM in a SOC**



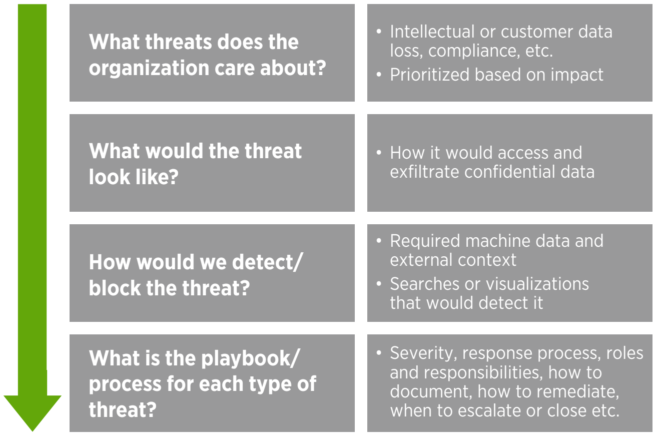
Getting Started with a SOC

A Security Operations Center (SOC) helps improve security and compliance by consolidating key security personnel and event data in a centralized location. Incident detection and response can be greatly accelerated and enhanced as a result.

Building a SOC is not a trivial exercise, as it requires a substantial upfront and ongoing investment in people, process and technology. However, the resulting benefits of having an improved security posture greatly outweigh the costs.

Process

Building a SOC starts with threat modeling (see Figure 1). This is a process where IT security and business people gather to determine key cyberthreats, prioritize them, model out what they would look like in machine data, and then determine how to detect and remediate them.



What threats does the organization care about?	• Intellectual or customer data loss, compliance, etc. • Prioritized based on impact
What would the threat look like?	• How it would access and exfiltrate confidential data
How would we detect/ block the threat?	• Required machine data and external context • Searches or visualizations that would detect it
What is the playbook/ process for each type of threat?	• Severity, response process, roles and responsibilities, how to document, how to remediate, when to escalate or close etc.

Figure 1: A basic threat modeling process.

A critical part of any SOC is the process for responding to alerts and incidents, and most SOCs use a multi-tier approach (see Figure 2). Alerts are generated through a variety of avenues, including SIEMs and SIEM-like solutions, and they go to the first tier of analysts for initial review. If the first tier cannot resolve the incident, it gets escalated to the next tier, which is staffed by personnel with more advanced knowledge and incident response tools.

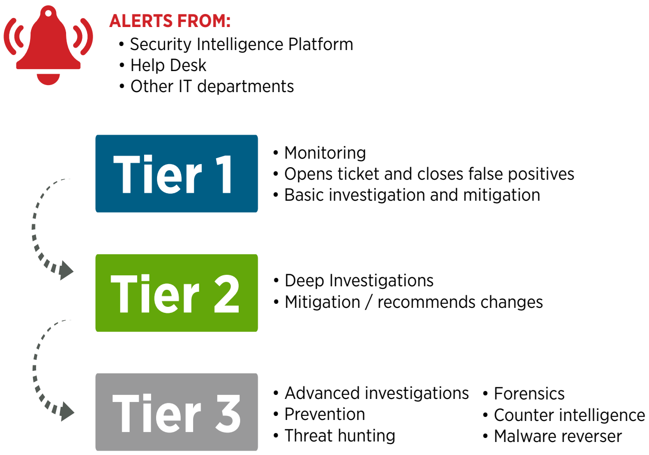


Figure 2: Example of a three-tier SOC and related responsibilities.

People

Hiring the correct personnel is critical to a successful SOC. A diverse set of personnel is required, each with different skills, qualifications, personalities and pay grades (see Figure 3). It's also important to make sure on-the-job and ongoing training occurs, and to also establish clear promotion paths so analysts can advance through the tiers in a SOC. Lastly, SOC personnel need to be collaborative in nature so they can work as a team to remediate incidents.

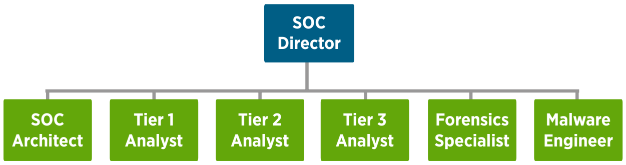


Figure 3: Example of the personnel required in a successful SOC.

Technology

A critical piece of technology in a SOC is a security intelligence platform (see Figure 4). This platform must be able to index all relevant machine data and log files from security and non-security sources in real time. The platform must also be able to take the data and enrich it with external data, such as data from Active Directory, asset databases, third-party threat feeds and more. This external enrichment adds crucial context that can be used in real-time correlation rules to protect the most critical assets and users, as well as to paint a more complete picture in an incident investigation.

The resulting indexed data and external lookups can then be leveraged to meet key SOC needs, including real-time correlation rules and alerting, incident investigations, custom dashboards and reports, and advanced analytics including anomaly and outlier detection.

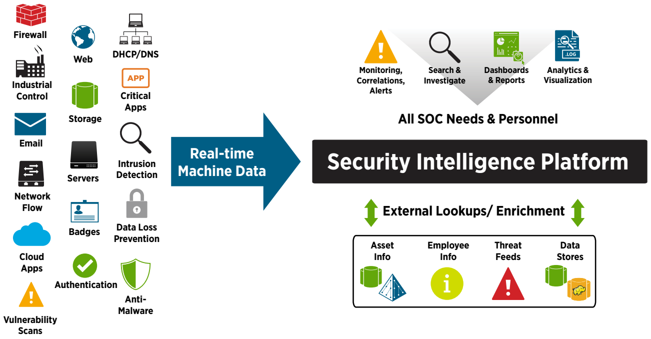


Figure 4: Security intelligence platforms use a wide range of data to meet SOC needs.

For correlation and alerting needs, it's important that the platform has the flexibility to detect threats through a range of highly accurate, customizable detection methods including correlation rules, risk scoring and anomaly detection, and then automatically assign a severity level to the incident.

This enables the platform to automatically filter through hundreds or thousands of daily security events and to only alert SOC personnel on the most critical incidents. Without flexible, accurate detection methods, threats will be missed and/or SOC personnel will be overwhelmed with false positives.

The platform must also be user-friendly enough to be used by all SOC personnel and flexible enough so it can be customized to meet the specific needs of every process and role in the SOC.

There are a number of data sources that security intelligence platforms need to index and leverage (see Figure 5). While the specific data sources for a given organization will drop out of a threat modeling exercise, typically the data needed will come from four major categories: threat intelligence, network, endpoint and authentication. With this data, specific information and clues can be gleaned on a threat, helping to connect the dots and track a threat all the way from entry to exfiltration.

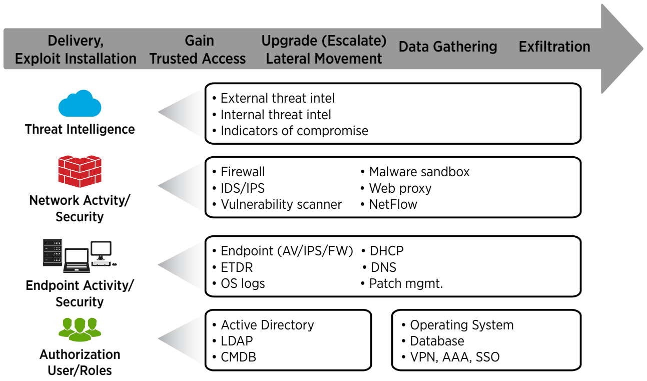


Figure 5: Example data sources needed to detect advanced threats.

There are a number of differences between a security intelligence platform and a traditional SIEM (see Figure 6). A security intelligence platform offers flexibility, speed and scale that traditional solutions struggle with.

	SIEM	Security Intelligence Platform
Data sources	Limited	Any technology device
Add intelligence and context	Difficult	Easy
Speed and scalability	Slow and limited scale	Fast and horizontal scale
Search, reporting, analytics	Difficult and rigid	Easy and flexible
Anomaly/outlier detection & risk scoring	Limited	Flexible
Open platform	Closed	Open with API and SDKs

Figure 6: Security intelligence platforms offer flexibility, speed and scale.

Other technologies needed in a SOC include a ticketing system for the efficient handling of incidents across the various SOC tiers. Tier 2/3 analysts also require advanced incident response tools including packet capture, disk forensics and reverse malware tools.

Enter Splunk

Splunk products provide a flexible and fast security intelligence platform that makes SOC personnel and processes more efficient. With Splunk software, all SOC personnel have quick access to all of the data and information needed to quickly detect, investigate and remediate threats. Splunk products can be used by a tier 1 analyst to do basic research based on a time period, keyword, IP address or machine name. The same products enable advanced tier 2/3 analysts to perform advanced cross-data source correlations, build analytical models to detect anomalies and outliers, or to perform advanced forensics on a compromised machine. Splunk Enterprise Security is also available, providing pre-built rules, reports, threat intelligence feeds, anomaly detection, risk scoring and an incident investigation framework. Splunk User Behavior Analytics can also be used as an added layer of detection; it uses unsupervised machine learning to automatically detect unknown, advanced external and internal threats.

Furthermore, Splunk software can help automate incident response processes and playbooks to decrease time-to-remediate and increase efficiency. This can be done by customizing Splunk software to automate otherwise manual incident response processes. One example is to create user interfaces in Splunk Enterprise where an analyst can simply enter a date range and a single IP/user name/host name to get all the relevant information around the entity in question and more quickly investigate the incident. Users can also add one-click actions to the Splunk UI, such as clicking on an event of interest with an IP address to automatically retrieve a relevant PCAP file for that IP from a third-party packet capture tool.

Splunk software is built for scale and speed. It uses a flat file data store (not a structured relational database), distributed search and installs on commodity hardware. It also scales out horizontally to handle the largest and the most demanding needs of global SOCs. Splunk software can index over 100TB of data per day and searches across massive data sets return in seconds.

Complement an Existing SIEM

Splunk software can replace or complement a SIEM in a SOC (See Figure 7). Splunk software can be used completely stand-alone from an existing SIEM or feed a subset of its data directly into a SIEM. In these two scenarios, the existing SIEM is typically used for correlations, alerting and incident workflow, while Splunk software is used primarily for deep incident investigations/forensics and advanced analytics.

In a third scenario, the existing SIEM feeds data into Splunk software and the Splunk platform performs all use cases. This scenario usually exists when the SIEM collectors are already on hundreds or thousands of hosts, and removing or replacing them is difficult.

	Scenario 1	Scenario 2	Scenario 3
Integration	None	Splunk feeds SIEM	SIEM feeds Splunk
Logging	splunk> & SIEM	splunk>	SIEM
Investigations / forensics	splunk>	splunk>	splunk>
Correlations / alerting / reporting	SIEM	SIEM	splunk>
Compliance	SIEM	splunk>	splunk>
Notes	May have different data sources going to Splunk vs SIEM	Splunk typically sends just subset of its raw data to SIEM	Initially SIEM connectors are on too many host to be replaced

Figure 7: Splunk Software complements existing SIEM deployments.

Additional Considerations and Best Practices

There are also several other SOC process and personnel matters that need to be considered. These include:

- Single Location vs. Multiple Locations. There are benefits to managing a SOC from a single or multiple locations. There can be cost efficiencies to multiple SOCs by leveraging cheaper labor in lower cost labor markets, but most SOCs tend to be centralized in a single location for improved information transfer among SOC personnel.

- Hours of staffing. Many SOCs start with 8x5 staffing but move to 24x7 as they mature. If multiple shifts are to be used, processes should be in place to ensure shift overlap and a smooth transfer of in-progress activity from one shift to another.

Several general SOC best practices include:

- Involve IT and business groups outside the SOC into SOC processes so these outside resources can help with both threat modeling and incident investigations/remediation.

- Establish processes to ensure SOC learnings are incorporated back into the SOC and the rest of the organization where relevant. These learnings can drive changes such as adjusting software configurations, refining SIEM correlation rules, more end user education or fixing unsafe business processes.

- SOC processes should be automated and made more efficient where possible by using technology.

- Red team and simulation exercises can help ensure processes work correctly, and also can find security gaps that should be addressed.

Next Steps

Are you considering building or optimizing a SOC? Contact Splunk today to learn about our software and services offerings, and how we can help.

Download Splunk for free. You'll get a Splunk Enterprise license for 60 days and you can index up to 500 megabytes of data per day. After 60 days, or anytime before then, you can convert to a perpetual free license or purchase an Enterprise license by contacting sales.

splunk> Learn more: www.splunk.com/asksales www.splunk.com