THE SOC ANALYST

Security. It's a big deal!

I badge in at the front door of my office building and greet the security guard who's there every day. From there, I head to the elevator for my floor, where my badge is needed once again to unlock it. Now on the SOC floor, I use my badge one more time to get to the common areas. This is where the sales and engineering teams sit, too. As I approach the center of the room, I see two doors within feet of each other. We call this area the "mantrap", which allows security to trap someone between the two doors and escort them out of the building, if needed. I swipe my badge at the first door, which lets me in, and as always, I fight a tiny bit of anxiety that I might get stuck between the doors. My badge opens the second door, though, and now I'm in the heart of security: the SOC. There are windows, but they're covered with blinds, making it dark. Looking up, I see TVs lining the ceiling which display what's going on in our global company and across the world in real time. I'm immediately sucked into my role, and after greeting my coworkers, I jump excitedly into my job.

Sounds top-secret and oh-so-cool, right?

Let's point our attention to the tools in an SOC.

Tools of the Trade

As a security analyst in the 2020s, you must know about **Security Information and Event Management (SIEM)**, which provides a real-time analysis of security alerts before they have a chance to disrupt business operations. SIEM means security specialists can look at their network through a larger lens, merging together security controls and infrastructure.

SIEM is the heartbeat of every SOC! Everything that's done on a device can generate a log, and without a log, there would be no security and no security analysts.

In fact, SOCs all over the world generate logs with the idea of sending them to a single point where the logs can be observed and measured. We refer to this concept as a "single pane of glass," ideally one screen that the SOC can operate without having to chain together multiple web browsers and sites to review security events.

In this description, the single pane of glass is the SIEM, so let's learn more about SIEM and other tools.

- SEIM completes the following tasks:
    - Normalizes logs and puts them in chronological order
    - Accounts for all logs and ensures they're in a the proper format
    - Creates rules that will sound an alarm if any logs match the given criteria

SIEM is working toward taking on the following tasks in the future:

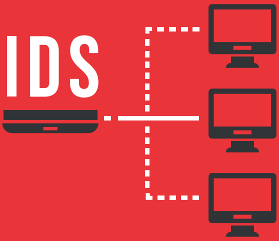
- Acting as case managers by combining and tracking multiple alarms for investigations in a way that's meaningful and easy to use
- Automating integration through **Security Orchestration, Automation, and Response (SOAR)**, which allows predefined playbooks to run automatically for common security issues, freeing up staff to work on more challenging and interesting items

Examples of SIEM are Splunk, Elastic, LogRhythm, Qradar, FortiSIEM.

- Firewalls. In addition to SIEM and SOAR, firewall and firewall engineering are a specialty of their own. You'll want to be familiar with the big players in the firewall space, including Cisco, Checkpoint, Fortinet, Palo Alto, Juniper, and SonicWall.

  As an SOC analyst, you might be asked to perform a firewall block on an IP address. Part of your job will likely include using the appropriate tools and techniques to determine if something is wrong and then blocking that IP address from communicating with your internal network.

- Intrusion Prevention System/ Intrusion Detection System (IPS/IDS) provides protection and detection. Most IPSs can act as IDSs and vice versa, but the main difference is their location on the network. They might be host-based or network-based, and they may be referred to as HIPS/HIDS or NIPS/NIDS. Together, these are known as intrusion detection and prevention systems (IDPS).
    - The protection system, IPS, allows a device to take action as needed to control the flow of network activity. Placing an IPS in line allows it to control the progress of traffic and take preventative actions when needed.
    - The detection system, IDS, only allows for detection, not any interjection or intervention. Tapping the network allows the device to see the network traffic but not affect bandwidth.

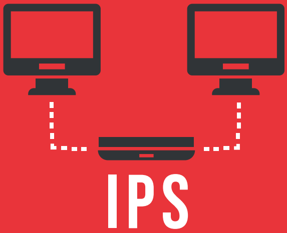


INTRUSION DETECTION SYSTEM

Intrusion Detection Systems can either be placed in line or through a network tap as seen here. intrusion detection systems are designed to detect and not take preventative measures.

Tapping the network allows the device to see the network traffic but not affect bandwidth. IDS placed through a tap can not take preventative action because they can not control the flow of traffic.

FIGURE 5-1: INTRUSION DETECTION SYSTEM



INTRUSION PREVENTION SYSTEM

Intrusion prevention systems must be placed in line as seen here. Placing an IPS in line allows it to control the flow of traffic and take preventative actions to protect.

IDS can be placed in line as well. Most modern IPS will have some rules set to take action and some set to monitor only. These are called Intrusion Detection and Prevention System (IDPS).

FIGURE 5-2: INTRUSION PREVENTION SYSTEM

- Sandboxing refers to executing the file or website in a protected environment to find out what it does. Endpoint detection software will detonate a file on your behalf, but even better is to use reports from Cuckoo, Hybrid Analysis, or Joe Sandbox. These tools will press every button and twist every knob to get execution information from a file.
- Other online tools for analysis include:
    - **Virustotal.com:** perhaps the most useful; put in a URL or hash to test it
    - **Domain Tools:** offers the whois tool, which is very easy to use

- **Talos Intelligence:** conducts reputational checks on IP addresses and URLs
- **IPVoid:** checks blacklists for a particular IP address
- **URLVoid:** checks URLs for safety reputations
- **Threat Crowd:** acts as search engine for threats and finds and researches artifacts related to cyber threats
- **TOR Exit Node List:** checks if the IP address is on a TOR exit node
- **IBM X-Force Exchange:** checks the IoC for information in X-Force Exchange
- **Search Engine:** checks a search engine for hiding suspicious items

As an important note, the value of a search engine like Google cannot be understated. Google may bring up something helpful that an SOC analyst never would've found if not for that search, so always keep that in your toolkit.

Definitions

Since cybersecurity terms often have vague meanings and aren't always agreed upon, let's specifically look at these crucial elements and how often they occur for your benefit.

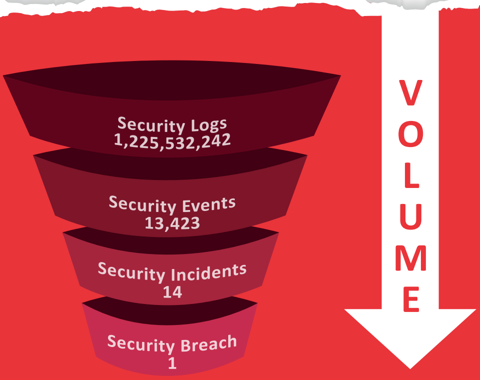


FIGURE 5-2: FUNNEL CHART

- **MOST COMMON:**
  - Security logs are the base of a security program. In your future job, you would want to capture logs like network flow, Windows Events, Unix Syslogs, and firewalls.
- **COMMON:**
  - Security events refer to the day-to-day routine security monitoring from tooling. Almost all security tooling notifications start as a security event generated from security logs. A security event must be escalated to a security incident before becoming a breach. The incident response then triggers the process of assigning an incident handler.
- **UNCOMMON:**
  - Incidents occur more often than a security breach. Once an incident is declared, the incident response process begins if there is suspected loss of sensitive data. Events that are not considered incidents are security events and vulnerabilities that haven't been escalated.
- **RARE:**
  - Security breaches contain a verified loss of data containing sensitive personal information. Breaches often require the legal department and CISO to declare a breach. Breaches start as incidents, require notification to clients and maybe the public, and are handled with careful sensitivity.
  - In your future career, it's advised not to use this term unless told otherwise!