WHAT ARE SECURITY OPERATIONS CENTERS (SOC)?

If you work in the technology field, you've probably heard of SOCs. And if you don't – well, it seems to be another acronym to throw in with the rest. Here's the thing, though: SOCs, short for security operations centers, are a vital component to most enterprises, whether a legacy company with a well-established footing in their field or a fledgling startup.

Monitoring your enterprise's security is vital. In their 2018 Data Breach Investigations Report, Verizon found that more than 58,000 cybersecurity events, such as breaches or exposed data, occurred around the world, 76% of which were financially motivated. Worryingly, the report details how a significant portion of these breaches involved the same methods that cyber criminals have been using for years.

SOCs are the best way to improve threat detection, so that you can respond to them faster, decreasing or even minimizing their risks. This article explores security operations centers. (Note that the term SOC is sometimes used outside of the IT and information security worlds, but we're focusing on the technology angle.)

Meet a security operations center

A Security Operations Center is basically exactly what it sounds like: a centralized unit that deals with security issues at both the organizational and technical levels. A balance of staff, technology, and processes aims to have the best and continuous situational awareness around enterprise security, whether its compliance and control issues or external threats and security breaches.

From an enterprise perspective, the SOC is typically a dedicated part of the IT department. SOCs can also be known as security defense centers (SDCs), security analytics center (SAC), network security operations centers (NSOC), and more.

The responsibility of an SOC is to monitor, detect, assess, respond, mediate, and report on IT threats within your company or enterprise. Such threats can include actual or potential cyberattacks or security breaches, and the SOC must determine which threats are genuine and malicious, and how actual security events are affecting business – all while stopping them in real time.

SOCs may also be responsible for ensuring your enterprise security meets a particular standard – either a self-determined standard or an industry standard for protecting data or complying with government protocol. This is particularly applicable in industries like medicine, healthcare, and finance, which by nature maintains sets of sensitive and personal data.

Importantly, SOCs typically are not built to develop security strategy, implement protection processes, or design architecture, which is usually the responsibility of one or more other IT departments.

How do SOCs work?

SOCs are comprised of a dedicated team of security analysts working together to monitor and shutdown security threats. Depending on the enterprise, SOCs may also include team members with specifics skills in forensic analysis, cryptanalysis, malware reverse engineering, and more.

The team then has actual tasks, like monitoring and analyzing activity across servers and networks, endpoints, databases, applications, websites, and more – always looking to identify anomalies in activity which may indicate a security event occurred or may soon occur. These tasks can be automated to certain degrees, too.

Sounds like a lot of work, which it certainly is, but there are ways to streamline it. Common SOC practices revolve around a SIEM system, which is a security information and event management system that provides both macro- and micro-level views into real-time enterprise activities and potential external breaches.

A SIEM system can include dozens of tools and processes to track and maintain security, such as:

- Data correlation from network discovery (data flows, telemetry, packets, syslog, etc.)
- Firewalls and antivirus detection
- Cyber threat intelligence
- Vulnerability and penetration tests
- Website assessment
- Data base scanners
- Intrusion detection systems (IDS)
- Intrusion prevention systems (IPS)
- Log management systems
- Governance and compliance systems

The way you structure your SOC varies depending on business need. Common focus areas can be combined or kept separate:

- **Control:** testing for weaknesses in penetration and vulnerability, ensuring compliancy

- **Monitoring:** events and response with log monitoring, SIEM admin, incident response
- **Operational:** identity and access management, firewall admin, etc.

SOCs in the cloud

As cloud computing continues to loom large over the tech industry, you may be wondering about cloud SOCs – and you wouldn't be the first. CloudSOCs can be established to monitor usage and security within the cloud. And if you're anything like most enterprises, you're spread across several cloud options, so monitoring suspicious activity is vital. Luckily, several SIEM technologies and actual machine data platforms are already on the market.

Best practices for SOCs

While the purpose of SOCs is nearly universal – to improve security and prevent breaches – the best way to do that can vary widely depending on your company's needs. Here are some best practices for operating a security operations center:

- **Stay up to date.** Security threats are agile, so your SOC must be ready to stay up to date on security intelligence to continuously improve detection and defense.
- **Seek out SOC services.** If you can't do it all internally, seek help from managed security providers that can help you establish an SOC and even offer some SaaS options.
- **Take advantage of automation.** Automating parts of security, such as XXX, helps you stay effective and efficient.
- **Don't skip the human element.** While technology alone might be able to stop small or basic threats, human system analysts ensure more significant issues are stopped and remediated as soon as possible.

While the time and upfront investment in an SOC is significant, consider the risks your enterprise is otherwise open to without one. As any business today, no matter your product or industry, is likely to be a digital business, you'll like want to – or have to – comply with security governance rules.