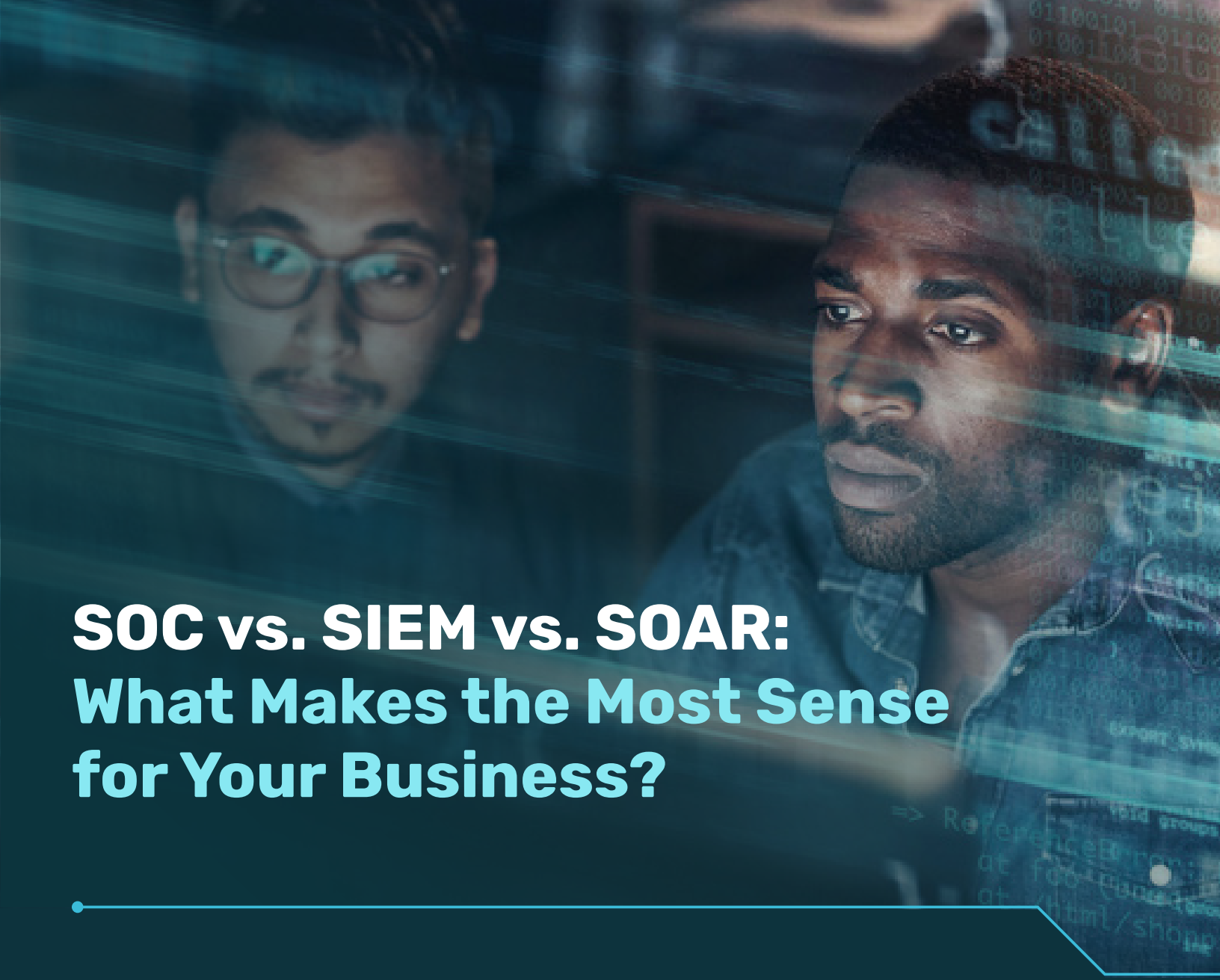

SOC vs. SIEM vs. SOAR: What Makes the Most Sense for Your Business?

2021 was a record-setting year for cyberattacks, and this year is proving to exponentially continue that trend with over 92% of data breaches in Q1 alone by cyberattacks. It's time for organizations to invest in sophisticated cybersecurity tools, but it can be challenging to know where to start, regardless of whether your company has an in-house security team. Security Operations Center (SOC), Security Information and Event Management (SIEM), and Security Orchestration, Automation and Response (SOAR) are some of the most effective threat detection and response capabilities, but where should you start to protect your organization? In this blog, we'll explore the differences between SOC, SIEM, and SOAR, how they integrate with one another, and the best combination for your organization.

CYBERLEAF
Managed Cybersecurity Service

What is SOC?

A Security Operations Center, or SOC, monitors, prevents, detects, investigates, and responds to cyber threats around the clock. It performs ongoing monitoring of an organization's network and addresses potential threats to sensitive data, computing systems, and an organization's other digital resources. With the growing threat of cyberattacks, a SOC is vital to an organization's ability to sustain operations, remain profitable, and achieve and maintain compliance with applicable regulations. Achieving a solid security position relative to your risks via an in-house SOC can be expensive and time-consuming, which is why many organizations turn to SOC-as-a-Service as a managed threat detection and response solution.

What is SIEM?

Security Information and Event Management (SIEM) tools combines security information management (SIM) and security event management (SEM) to provide real-time analysis of security alerts generated by applications and network hardware. SIEM software can have a number of features and benefits for organizations, including:

- **Consolidation of multiple data points:** As organizations utilize a wide range of data sources, often with inconsistent, overlapping or incomplete information, it can be challenging for businesses to know whether they're looking at all the data and if it's accurate. SIEM consolidates the data from each element of your network environment into one centralized database. Simply put, the SIEM ingests data from protection tools like Extended or Enhanced Detection and Response (EDR, formerly antivirus), Remote Monitoring and Management systems (RMM), and other applications as well as the logs from endpoints, servers, firewalls, and much more. This live data enables advanced low-latency analytics for threat mitigation.
- **Custom dashboards and alert workflow management:** Every company has different priorities and different workflows for managing security protocols. Many SIEMs offer customizable dashboards to help monitor company priorities and timely alerts that coordinate within existing workflows.
- **Integration with other products**: Bringing in any new solution can be challenging if it doesn't play nicely with other tools. Many SIEM solutions are designed to seamlessly integrate within an existing technology stack, accessing vital data without interrupting established processes.
- **Insights and track records**: SIEM helps not only collect and compile security data, but also analyzes it to provide strategic data insights, event correlation, aggregation, reporting, and log management.

What is SOAR?

SOAR refers to security orchestration, automation, and response technology. This threat detection and response solution utilizes a combination of human and machine learning toanalyze diverse data from a variety of sources in order to correlate and prioritize incident response actions. What does this mean for organizations trying to protect themselves from cyber attacks? SOAR helps teams with:

- **Threat and vulnerability management:** Companies cannot easily remediate vulnerability risks without first having a system in place to identify them. SOAR helps businesses identify, evaluate, contextualize, and report on cyber threats and vulnerabilities.

- **Security incident response:** Many cyber incidents cannot afford to wait until the next scan to be mitigated. SOAR provides vulnerability alerts and helps companies prioritize efforts for coordinated incident response.
- **Security operations automation:** Responding to cyber attack threats can often be a lengthy process, especially for small or non-existent security teams within a company. With SOAR, businesses can automate security operations tasks to taking threat identity and remediation from months to minutes.

With these capabilities, SOAR offers unique and invaluable assets to small and large businesses alike. It will:

- **Consolidate process management, technology, and expertise:** SOAR helps organizations with key members on different teams to consolidate the technology and processes of security management into one system.
- **Centralize asset monitoring:** It can be challenging for organizations to discover and analyze assets from many different IT environments. SOAR provides a centralized system that catalogs, monitors, and reports on assets from many locations.
- **Enrich alerts:** A threat alert alone is only so useful without detailed information about the nature of the threat. SOAR enriches the power of timely alerts by also providing intelligent context, such as where the vulnerability is located and the severity of its exposure.

CSaaS: The Power of SOC, SIEM, and SOAR Together

While SOC, SIEM, and SOAR are important threat detection and response solutions on their own, when integrated together their power multiplies exponentially. In an end-to-end cybersecurity solution, such as the cybersecurity as a service (CSaaS) solution from Cyberleaf, security teams don't need to choose between several different tools—they can utilize SOC, SIEM, and SOAR all in one centralized system.

The Cyberleaf end-to-end CSaaS combines the power of:

- **Powerful SIEM:** The heart of your security infrastructure, the Cyberleaf SIEM, monitors activity across your endpoints, network, servers and cloud to detect unwanted activity through the application of AI-driven algorithms for pattern recognition and threat signature matching. Leveraging the renowned MITRE ATT&CK framework and ingesting over 1,000 threat intelligence feeds, the Cyberleaf SIEM speeds detection and response to advanced threats and provides access to real-time data.
- **Intuitive SOAR:** Cyberleaf's SOAR technology knows the response you need before you need it. Automated real-time responses and actions protect your information, aligned with your specific policies and working in concert with your internal responses. Automated SOAR response utilize an ever-growing library of playbooks and integrations to speed response across your environment.
- **24x7x365 SOC:** Continuous monitoring of security systems provides notifications and coordinates responses to threats and incidents. SOC support reduces low level alerts to enhance your team's ability to focus on what matters. We also offer AI and expert driven threat hunting, forensic analysis, investigation and incident response services on an as-needed basis all done in the USA and by vetted professionals.

Together, the Cyberleaf CSaaS capabilities become a force multiplier that work in concert with your existing resources to provide enhanced protection for your entire organization. To see how a holistic CSaaS solution benefits your organization, get a free assessment from the experts at Cyberleaf today.