6 KEY FRUSTRATIONS WITH LEGACY SIEMS

And How SOCaaS Addresses Them

Traditional SIEM solutions are well-suited to log management and compliance requirements. But they aren't optimized for the level of threat detection and response required by today's business. This leads to a lot of frustration. **SOC-as-a-Service provides a solution.**

Key Signs of SIEM Frustration

1 SIEM **project is stalled or hung up** in the deployment and configuration phase.

2 **Analysts ignore or turn off alerts** because there's too much noise and too many false-positives.

3 Your **analysts are suffering burnout** or are leaving.

4 You've disabled most of the SIEM's default configurations **because they don't work**.

5 You're **ready to replace your SIEM with something better**. Or, you've already tried this and still aren't happy.

6 You've **suffered a data breach or a cyberattack** that should have been caught and stopped.

6 SIEM Frustrations and How SOCaaS Does It Better

1 Legacy Architecture

The architecture of traditional SIEM platforms follows an on-premises model that no longer meets the modern requirements of a cloud-driven environment.

How SOCaaS Does It Better

Built on a cloud-native, next-generation SIEM platform, SOCaaS eliminates the disruptions and management complexities associated with traditional SIEM, and enables rapid scaling and better resiliency.

2 Limited Functionality

SIEM may have been cutting-edge technology when it first entered the market, but threat detection and response practices have changed a great deal since then.

How SOCaaS Does It Better

Modern, next-generation SIEM combines essential SOC technologies into a single, unified SaaS offering, which improves the speed and efficiency of the detection and investigation process.

3 Unsupported Data Sources

The IT landscape has grown to encompass on-premise, remote, cloud/multi-cloud, IoT/OT, containerized and serverless environments. Legacy SIEMs were not designed for this transformed workplace.

How SOCaaS Does It Better

A SOCaaS provider with a vendor- and data source-agnostic model provides native support for a broad range of critical data sources and telemetry.

4 Weak Analytics

The alert fatigue associated with legacy SIEM platforms is the result of weak analytics that are based on a generalized approach and generic use cases. They rarely include a common information model (CIM) that would enable it to optimize the analytics.

How SOCaaS Does It Better

SOCaaS platforms combine data science and automation, a blend of multiple threat detection methods and contextual enrichment to optimize the process of tuning and configuration, dramatically reduce false positives, and accelerate the time to identify, detect, and remediate the threat.

5 A Lack of Experts

SIEM is not sustainable if you can't dedicate substantial staff resources to deploying, managing and monitoring the platform. All these functions require specialized skills, along with 24/7 staffing.

How SOCaaS Does It Better

As a co-managed service, you can have as much control as you'd like, with full transparency–without the expense of in-house staff to deploy, operate and maintain the platform.

6 Slow Time to Value

The all-in costs of the SIEM, including software licenses, storage, staff and additional professional services required to support specific data sources and use cases, can be steep and run into the millions very quickly and are often unpredictable.

How SOCaaS Does It Better

SOCaaS includes everything you need and can be fully operational in as little as one month. Your time to value decreases from many months or years to just weeks, and your bill is predictable, with an all-inclusive, pay-as-you-go monthly fee that covers the use of the technology, and access to the experts.

Cysiv solves your legacy SIEM frustrations with SOCaaS

Let's discuss how Cysiv can help you achieve better security with SOC-as-a-Service.

1.833.229.9800 | info@cysiv.com

CONTACT US