LogicHub

7 Reasons

to Choose SOC-as-a-Service over DIY SIEM

Introduction to the Modern SOC

A SIEM platform is a cornerstone of a modern SOC operations. But the cost and overhead tied to deploying a Do-it-yourself (DIY) SIEM is high, from the up-front licensing and infrastructure costs to the extensive labor required to implement and tune simply to get it in a working state. And once a SIEM is deployed, it's time-consuming to configure and manage.

SOC-as-a-service lets you control these costs by offering a fully managed SIEM deployment that removes the operational overhead and licensing guesswork. It also delivers additional capabilities and benefits to augment and enhance your security operations, like 24x7 expert threat detection and response, and fully managed SOAR at a fraction of the cost it would take to deliver on your own.

Lower Operating Costs

1

DIY SIEM platforms require expensive hardware or cloud infrastructure that can require extensive time and effort to manage. And these infrastructure costs continue to grow as more data is collected and retained over time. This also requires expensive engineering resources to allocate and maintain the infrastructure, in addition to managing the SIEM deployment.

SOC-as-a-service eliminates this overhead by delivering a fully managed SIEM instance that that includes both infrastructure and management. Infrastructure and management are included in your licensing, controlling costs and lowering your operating overhead.

SOC-as-a-service benefits:

- **No required infrastructure**
- **No administration or management overhead**

Simple, Predictable Licensing

SIEM licensing is usually based on data volume or collection velocity. Your licensing costs increase as your data and collection requirements grow over time, making the cost of owning a DIY SIEM expensive and often unpredictable.

SOC-as-a-service uses predictable pricing based on the size of your organization and your security outcome requirements. No matter how much you use the service over time, your license will remain the same, keep your operating costs manageable.

SOC-as-a-service benefits:

- Predictable, simple licensing costs
- Fixed cost regardless of data volume or users

SOC-as-a-service benefits:

- 24x7 data management, from collection to analysis
- Verified data retention for compliance and forensics

Consistent and Reliable Collection of All Your Event Data

Managing your own DIY SIEM means continually validating that event data is being properly collected at all times. This is critical for both compliance-driven data retention requirements and accurate security analytics but can add significant overhead tied to ensuring that your SIEM is accurately and consistently collecting the right data at all times.

SOC-as-a-service includes 24x7 validation that all relevant data is being collected and analyzed at all times. A reliable, cloud-based infrastructure maintains data integrity and availability at all time, ensuring that all forensic data is available for investigations and compliance reporting.

Out of the Box Expert Threat Detection Content

One of the most time consuming and inefficient components of operating your own SIEM is the creation, configuration and tuning of detection rules. Out-of-the-box detection content shipped with most DIY SIEM solutions is either not applicable to your environment or requires extensive configuration to fit your requirements. And that's assuming you have the time it takes to work on customization.

SOC-as-a-service removes that burden by including expert content that is adapted to fit your environment and unique requirements. Automated playbooks that analyze and triage all SIEM alerts (and others) bypass the need for extensive configuration and tuning. This saves time and money, delivering significantly faster time to value without the overhead.

SOC-as-a-service benefits:

- **Extensive out of the box content that delivers value on day one**
- **Fully outsourced configuration and tuning**

Fully Outsourced Configuration and Tuning

SIEM rule engines are low fidelity by nature, generating hundreds or thousands of false positives every day. Few organizations are able to staff enough Tier 1 analysts to get through the basic analysis and triage necessary to cut through the noise. That means analysts are often spending as much as 75% of their day reviewing false positives while critical threats go unnoticed.

SOC-as-a-service uses automated alert triage to eliminate 95% or more of the false positives generated by SIEM and other solutions. That means our analysts spend their time investigating true threats and sending your confirmed cases to your team faster, eliminating the alert fatigue tied to false positives. And greater efficiency means lower operating costs that are passed on to you.

SOC-as-a-service benefits:

- Automated alert triage that eliminates false positives with 95% or better accuracy
- 24x7 virtual Tier 1 analysts to ensure all data is rapidly analyzed at a fraction of the cost

Deep Correlation and Data Enrichment

SOC-as-a-service benefits:

- Delivery of confirmed cases with complete event context and threat correlation
- Direct mapping to MITRE ATT&CK with associated recommended remediation

SIEM alerts rarely contain the comprehensive, deep context necessary to be actionable, only able to show event fields contained within specific logs. This leads to analysts spending significant cycles simply gathering the event details and threat context necessary to properly investigate and respond to an alert.

SOC-as-a-service delivers fully enriched cases, automatically collecting and consolidating all relevant event context. Deep correlation identifies all potential threat context tied to an attack and connects it to related threats to associate all potential vectors. And all cases are automatically mapped to the MITRE ATT&CK framework, identifying all Tactics and Techniques in use as well as any recommended remediations.

SOC-as-a-service benefits:

- Rapid, customized deployment and immediate time to value
- Automated alert triage, threat detection, incident response and threat hunting

Security Automation without the Overhead of a DIY SOAR Platform

SOAR platforms may look easy in a demo but building and maintaining automated playbooks is a time-consuming process that few organizations have the resources to complete. Industry analysts say that 90-95% of all out-of-the-box SOAR play books don't work for most organizations, meaning you will be on the hook to build your own. And that's assuming that you know where to start building out relevant use cases.

SOC-as-a-service is powered by a fully managed SOAR deployment for every customer. Extensive out of the box expert content is rapidly adapted to your environment to automate alert triage with 95% or greater accuracy, to execute accurate and consistent deep detection and incident response, and to perform continuous threat hunting.

1. What will your operating overhead be to deploy and manage your own SIEM?
2. What will your licensing cost be over time as your data requirements and volume grow?
3. How will you ensure that the right data is always being collected?
4. How much administrative effort will it take to guarantee that your SIEM's data collection is optimized for threat detection and response?
5. What content is available out of the box and will it meet your requirements?
6. How much time will it take to tune vendor-provided content to your environment?
7. Do you have the time and skillset to build out your custom SIEM rules?
8. How will you keep false positives to a minimum?
9. How well equipped will your SIEM be to perform deep correlation and enrichment?
10. Will your SIEM deliver SOAR capabilities to lower MTTD and MTTR?

10 Questions You Need to Answer When Choosing Between DIY SIEM or SOC-as-a-service