E-Guide

Virtual SOCs: Enterprise-Run vs. Fully Managed

In this Eguide:

In this e-Guide:

Go in-depth on the two available types of virtual security operations centers (SOCs) – enterprise-run and fully managed.

Understand the responsibilities of a SOC, learn why virtual SOCs are growing in popularity and see 4 key challenges that a virtual SOC can help your security team address directly.

Benefits of virtual SOCs: Enterprise-run vs. fully managed

ASHWIN KRISHNAN, CHIEF DIVERSITY AMPLIFIER

The security operations center has evolved to meet current enterprise demands. Multiple SOC options exist today that may meet your organization's needs. Carefully considering each option and its benefits is critical to finding the best fit.

In-house SOCs are the traditional SOC model -- a dedicated group of security professionals are responsible for monitoring, analyzing and protecting against cyber attacks.

A newer option is the virtual SOC, which has two suboptions. An enterprise-run virtual SOC is a SOC that is fully controlled by enterprise employees but hosted in the cloud without the overhead of a physical location. A subscription-based virtual SOC, also known as *SOC as a service* (SOCaaS), is when enterprises outsource some or all SOC responsibilities to a managed service provider.

The terms can get confusing. Read on to learn more about the two types of virtual SOCs, their benefits and when one might be a better option than the other.

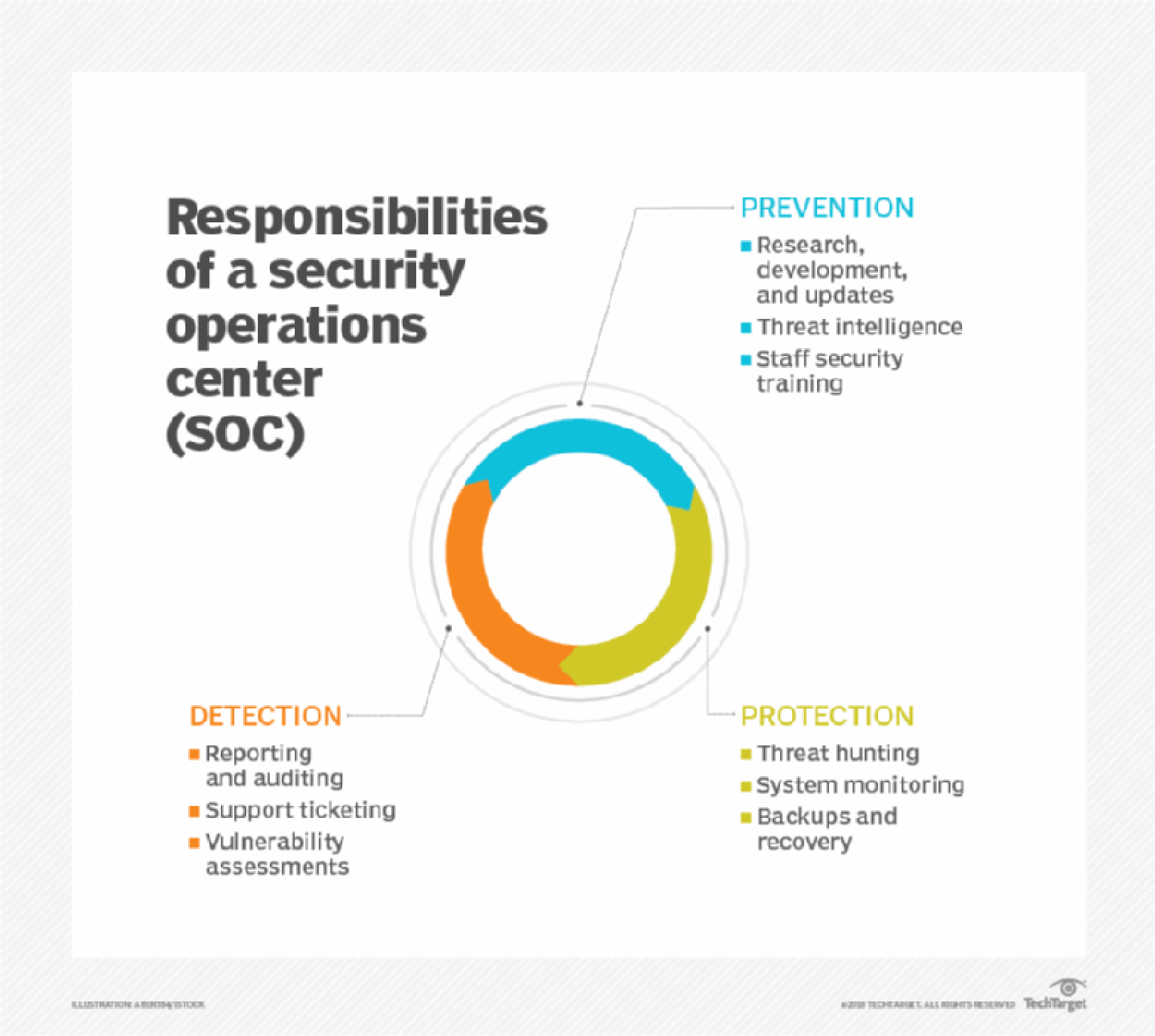
EXPLAINING THE VIRTUAL SOCS

In both iterations, a virtual SOC, also known as *SOC 2.0*, is an online security command center that is available 24/7, year-round.

Virtual SOCs have all the capabilities and tools that physical SOCs have, including continuous monitoring and implementing tools to improve an organization's security posture through prevention, detection, analysis, response and triage techniques.

Where the two models differ is in the employees. An enterprise-run virtual SOC can be composed of solely company staff or a mix of company staff, on-demand workers and cloud-provided workers. With SOCaaS or an outsourced SOC, either all services can be outsourced to a third party or just some -- for example, some lower-level SOC tasks, such as information gathering, may be outsourced, leaving higher-priority tasks, such as analysis of that information, to the organization's security team.

In this Eguide:



Responsibilities of a security operations center (SOC)
PREVENTION
■ Research, development, and updates
■ Threat intelligence
■ Staff security training
DETECTION
■ Reporting and auditing
■ Support ticketing
■ Vulnerability assessments
PROTECTION
■ Threat hunting
■ System monitoring
■ Backups and recovery
ILLUSTRATION: A-BORTH/ISTOCK
©2018 TECHTARGET. ALL RIGHTS RESERVED
TechTarget

VIRTUAL SOC BENEFITS

Enterprise-run virtual SOCs are becoming increasingly popular for three main reasons:

1. **Cost.** The costs of building and maintaining a physical SOC is ever increasing. Beyond real estate, the number of employees needed to run the SOC can exhaust budgets. With constantly tightening security resources, CISOs are always on the hook to find ways to reduce Capex and Opex spend. The SOC is always on the CISOs radar to cut expenditures.
2. **Reliability and availability.** Cloud infrastructure has revolutionized modern cybersecurity, especially when it comes to reliability, scalability and availability. In some instances, the expertise and tools needed to maintain uptime and ensure the integrity of a virtual SOC in the cloud far exceed what an enterprise can do in a physical SOC.
3. **Uniqueness of the environment.** The work-from-home era has not only increased BYOD use, but also resulted in these devices being shared at home among family members and housemates. Though enterprise mobile device management software is still prevalent, it becomes nearly impossible to implement under these conditions. The pandemic caused an overnight surge in work-from-home employees, and a large portion of employees' traffic now goes straight to cloud applications versus being routed via the enterprise network first. An in-house SOC team is better able to recalibrate baselines and adjust false positives, which may happen as a result of this shift.

A partly or fully outsourced SOC may be the preferred option for some enterprises for reasons beyond these three benefits. For example, virtual SOCs can help with the following:

- **Targets on your back.** Attack targets are no longer solely high-net worth organizations, such as banks, or national critical assets, such as power grids. Increasingly, smaller companies and even school districts are being targeted by malicious actors. With neither the budget nor talent to manage or monitor a SOC themselves, many of these businesses and organizations are seeing an outsourced virtual SOC as a viable option.
- **Compliance and regulations.** In addition, stringent regulations, such as GDPR, CCPA and Privacy Shield, have an element of monitoring, reporting and incident response that must be adhered to and demonstrated to pass security audits. A fully or partially outsourced virtual SOC can be instrumental in helping businesses demonstrate compliance to not only pass audits, but also maintain enduring customer trust.
- **The talent gap.** A partially or fully outsourced virtual SOC can also help enterprises tackle the current talent shortage. With ransomware becoming more targeted and the number of malicious attacks ever increasing, the need for high-quality security talent who can manage the entire incident lifecycle has never been greater -- nor more difficult. And, with the cybersecurity skills shortage at an all-time high, an outsourced SOC has become the only option for some businesses.

- **Aggregate value.** Managed virtual SOCs can also provide better security detection and response than SOCs that are in-house or company-run. This can lead to a virtuous cycle: The more data and telemetry a SOC has, the better incident detection, response and remediation the SOC team can provide. Algorithms and human response capabilities will become more accurate. All customers of the managed virtual SOC benefit as a result because the managed SOC provider can gather more data based on the types of attacks it sees across its entire customer base. As a result, the provider can hone its detection and analysis capabilities for all clients.

Bottom line: Today's SOC has various incarnations. Choosing the model that best aligns with your organization's needs and budget requires careful consideration to result in the best outcome for the company and its customers.

Sponsor Overview:

DigitalXRAID are an award-winning managed security services provider with 50+ years' experience, dedicated to providing our clients with state-of-the-art cyber security solutions. We specialise in Vulnerability Management, Threat Intelligence, Information Security, PCI-DSS, Penetration Testing, Managed Security Services, Security Consultancy, and offer a fully managed Security Operations Centre (SOC) for your complete cyber security protection.

We're serious about security and compliance and have some of the highest qualified professionals in the country ready to safeguard your security. We are one of the elite few who hold both CHECK and CREST certifications alongside Cyber Essentials Plus, IASME Gold Standard, ISO 27001, and ISO 9001 accreditations.

With our cutting-edge tools and techniques, we'll protect your business 24 hours a day, 365 days a year. We'll shield you from cyber threats, safeguard your digital assets and ensure you stay two steps ahead of the criminals. We're your best defense against cyberattacks and when you choose DigitalXRAID, you're choosing the finest cyber security team for your business.

https://www.digitalxraid.com/