MSSP, SOC AND SKYBOX

CASE STUDY

AirITSystems puts Skybox alongside SIEM in importance to establishing a successful SOC and managed services for their customers

PARTNER PROFILE

AirITSystems is a managed security service provider (MSSP) based in Hanover, Germany delivering IT and security solutions to customers of all sizes in a variety of industries. As part of their comprehensive services, AirIT helps their customers establish a cost–effective security operations center (SOC) for 24x7 monitoring and rapid response to their most critical security issues.

BUILDING A SUCCESSFUL SOC

SOCs are a hallmark of mature security management programs, ensuring IT systems are monitored, assessed and defended around the clock. But establishing a native SOC comes with many challenges, which can drive up the cost of such an initiative.

First, organizations need to gain visibility of their attack surface — all the ways in which they are susceptible to cyberattacks. But a variety of vendors, tools, processes and teams, as well as the scale of the network itself, stand in the way. Without proper visibility, organizations will lack the foundation on which to build their SOC.

Second, SOCs need to be abreast of the cyber risks within their organization. System information and event management (SIEM) systems give SOCs the data they need to know what's happening in their network. However, SIEMs often churn out more data than can be acted upon. Their results need to be contextualized in order to accurately set priorities, as task which can take a great deal of time and resources if done manually.

Lastly, SOCs require highly specialized IT security professionals whose expertise extends beyond simply firewall management. In light of the current cybersecurity skills shortage worldwide, qualified talent can come at a premium.

HURDLES TO BUILDING A SUCCESSFUL SOC

Gaining visibility and understanding of the attack surface

Analyzing, contextualizing and prioritizing SIEM info and threat advisories

Hiring security experts amid a global cybersecurity skills shortage

SKYBOX & MSSP SOC SERVICES

Because of the challenges mentioned above, AirIT developed a service where customers could partially or entirely outsource their SOC functions to security specialists. AirIT's SOC services act as a filter, communicating only critical alerts and emergencies to the customer organization, doing so concisely and with remediation guidance.

To successfully deliver these services, AirIT recommends companies enlist two core technologies: a SIEM and Skybox Security for vulnerability management. As mentioned above, the SIEM provides up-to-date information on the state of the network. Skybox then contextualizes that data by correlating it to a model of the organization's attack surface encompassing its security controls, network topology, assets, vulnerability and threat information. This visual, interactive model assesses if an issue identified by the SIEM is already neutralized, or if its severity level should be raised based on the surrounding environment and activity in the threat landscape.

The use of a SIEM in conjunction with Skybox will cover nearly 80 percent of the SOC workload, according to AirIT estimates, and will focus SOCs on the most critical advisories and incidents. AirIT also views this approach as the only economic solution to establishing a successful SOC, reducing the need for investment in more point solutions and the niche talent to manage them.

> "Nearly every IT asset should be able to integrate with these **2 core technologies** Skybox Security and the SIEM. Configuration data is sent to the Skybox server, and log data to the SIEM. From a security standpoint, **nothing else is needed** for an efficient, suceessful SOC."
>
> —Tim Cappelmann
> Head of Managed Services, AirITSystems

SKYBOX-POWERED SOC BENEFITS

- Complete, detailed and seamless visibility across physical IT, virtual, cloud and operational technology networks
- Focused attention on truly critical issues thanks to intelligently contextualized SIEM results
- Reduced costs from decreased reliance on point solutions and the talent needed to manage them

VULNERABILITY MANAGEMENT BEYOND THE SCAN

Threat-centric vulnerability management from Skybox combines attack surface visibility, up-to-date threat intelligence and attack vector analytics to pinpoint and eliminate the vulnerabilities putting you most at risk.

Discover vulnerabilities anywhere in your network on demand with our scanless assessment technique. Combine scanless assessment results with scan data for complete awareness of your vulnerabilities at any time.

Correlate vulnerabilities with the network model to understand which are exposed and which are isolated from attack paths.

Use security analyst research on available and active exploits to understand which vulnerabilities are most likely to be targeted.

Prioritize vulnerabilities based on the threat they pose. Those exposed or exploited in the wild should be dealt with immediately, while others can be dealt with in time.

Get remediation guidance of available patches, IPS signatures or rule changes that can neutralize the vulnerability.

Track remediation to ensure imminent threats are addressed quickly, and monitor remaining vulnerabilities for changes in exposure or exploitation to ensure their threat levels don't escalate.

About Skybox Security

Skybox provides the industry's broadest cybersecurity management platform to address security challenges within large, complex networks. By integrating with 120 networking and security technologies, the Skybox™ Security Suite gives comprehensive attack surface visibility and the context needed for informed action. Our analytics, automation and intelligence improve the efficiency and performance of security operations in vulnerability and threat management and firewall and security policy management for the world's largest organizations.

REQUEST A DEMO

www.skyboxsecurity.com | info@skyboxsecurity.com | +1 408 441 8060

SKYBOX™ SECURITY