ARMIS®

SOLUTION BRIEF

Empowering Security Operations Centers with Armis

Security Operations Centers (SOCs) face mounting challenges in safeguarding organizations against evolving threats. The proliferation of IT, IoT, OT and IoMT devices managed by the SOC and complex network environments they must keep secure poses a substantial visibility and manageability challenge. Sophisticated cyberattacks have also yielded significant hurdles to maintaining robust security postures. Armis Centrix™ enables SOC teams to overcome these challenges and achieve enhanced visibility, security, and control over customer environments.

Challenges Faced by Security Operations Centers (SOCs)

SOCs are responsible for maintaining operability of customer environments and encounter several key challenges that can complicate and may impede their ability to deliver promised SLAs to the customers:

1

Multi Device Proliferation

The exponential growth of a heterogeneous environment which may include IT, OT, IoT and IoMT devices that are both managed and unmanaged, introduces new security challenges. This is often most prevalent in the areas of real-time situational awareness and maintaining an optimal security posture for these novel attack surfaces and vectors. Simply put, many SOCs lack proper visibility and security controls within traditional monitoring solutions.

2

Complex Network Environments

Hybrid and multi-cloud infrastructures, combined with a variety of application requirements that must scale across distributed environments to a diverse device pool and endpoints, create complexities that challenge SOC teams' ability to maintain comprehensive visibility, control and capacity planning.

3

Advanced Cyber Threats

Sophisticated cyber adversaries continuously evolve their tactics, techniques, and procedures (TTPs), making it increasingly difficult for SOC teams to detect and respond to emerging threats in a timely manner. The result can be impacted service delivery or complete outages which can violate stringent SLA clauses that often promise "five nines" or more of flawless delivery. A successful security breach can cost a SOC even more, not to mention the potential financial loss to the end customer.

Armis Centrix™ For SOCs

Armis empowers SOC teams to overcome these challenges through its comprehensive cybersecurity platform Armis Centrix™. Armis Centrix™, is a leading cyber exposure management platform, which is powered by the Armis AI-driven Asset Intelligence Engine. It sees, secures, protects and manages billions of assets around the world in real time. The seamless, frictionless, cloud-based platform proactively mitigates all cyber asset risks, remediates vulnerabilities, blocks threats and protects your entire attack surface. Armis Centrix™ can be easily deployed in SOC environments and delivers the following key capabilities:

Complete Device Visibility

Armis automatically discovers and classifies all devices connected to the network, including IT, OT, IoT, and IoMT devices. Complete coverage includes managed, unmanaged, and shadow devices. Real-time monitoring and deep situational awareness of each and every device, its behavior, and any deviations from baseline operations delivers proactive threat detection and response thus virtually eliminating risk of undetected security incidents and possible impacts on service delivery. SOC teams gain unparalleled visibility and complete control of customer environments.

Risk Assessment and Mitigation

Armis constantly assesses device risk based on behavior, vulnerabilities, and context, enabling SOC teams to prioritize remediation efforts and mitigate high-risk devices effectively. Prioritization and threat mitigation is customized and based on asset criticality to the business. Automated policy enforcement ensures consistent security measures are applied across the network, reducing the attack surface and enhancing overall defense posture.

Advanced Threat Detection and Response

Leveraging artificial intelligence, machine learning and behavioral analytics, Armis detects anomalous device behavior and activity that may indicate potential security threats. This empowers SOC teams to respond swiftly and decisively. Automated response actions and playbooks facilitate rapid containment and mitigation of security incidents, minimizing the impact on customer environments.

Integration with Existing Security Infrastructure

Armis seamlessly integrates with popular security tools and platforms that are being used in SOC environments. Leveraging and working in conjunction with the existing security stack which includes but is not limited to SIEMs, EDR solutions, and firewalls, Armis creates an “ecosystem of trust” in the SOC, thereby enriching security data and streamlining incident response workflows. This cooperative security system delivers centralized visibility and management of security data and enables SOC teams to correlate alerts, investigate incidents, and orchestrate response actions more efficiently.

Why SOC Providers Choose Armis

Implementing Armis in the SOC delivers numerous key benefits, including:

Enhanced Visibility and Control

Armis provides SOC teams with complete visibility and control over customer environments, enabling proactive threat detection, rapid response, and effective risk mitigation.

Improved Security Posture

By comprehensively identifying the totality of all devices that are part of the customer's digital footprint and addressing security risks associated with them, Armis strengthens the overall security posture of customer environments, reducing the unacceptable risk of cyber attacks.

Increased Operational Efficiency

Automation and integration capabilities streamline SOC workflows, allowing teams to focus their resources on strategic tasks such as threat hunting and incident response, ultimately improving operational efficiency.

Compliance Readiness

Armis aids organizations in maintaining compliance with industry regulations and alignment with security frameworks by providing visibility into device security and facilitating risk-based decision-making.

Armis serves as a foundational component in the SOC environment, empowering teams to overcome the challenges of securing customer environments in the face of evolving cyber threats. By offering comprehensive visibility, security and manageability along with seamless integration capabilities, Armis enables SOC teams to deliver superior service to customers by achieving stellar security outcomes. This ultimately safeguarding organizations against cyber risks and vulnerabilities while also exceeding stringent SLA requirements set forth in customer contracts.

Armis, the asset intelligence cybersecurity company, protects the entire attack surface and manages the organization's cyber risk exposure in real time.

In a rapidly evolving, perimeter-less world Armis ensures that organizations continuously see, secure, protect and manage all critical assets.

Armis secures Fortune 100, 200 and 500 companies as well as national governments, state and local entities to help keep critical infrastructure, economies and society safe and secure 24/7.

Armis is a privately held company headquartered in California.

1.888.452.4011

Website

Platform
Industries
Solutions
Resources
Blog

Try Armis

Demo
Free Trial