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

Proliferation of Diverse and Unmanaged Devices

The exponential growth of heterogeneous environments—including IT, OT, IoT, and IoMT devices—creates unprecedented challenges for SOCs. Many of these devices are unmanaged, lack native security controls, and operate outside traditional monitoring tools, leaving SOCs blind to potential vulnerabilities and risk. This can directly impact real-time situational awareness and the ability to ensure a strong security posture.

2

Sophisticated and Complex Ecosystems

The rise of hybrid and multi-cloud infrastructures have transformed SOC operations, by adding layers of complexity. These environments often include distributed architectures and diverse asset pools. Maintaining comprehensive visibility, security and control across these interconnected systems while also ensuring operational resilience is crucial.

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 cyber exposure management and security. Armis Centrix™ platform is powered by the Armis AI-driven Asset Intelligence Engine which 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 delivers a comprehensive suite of capabilities tailored to empower SOC operators and address the complexities of modern cyber exposure management and security. Armis Centrix™ provides complete device visibility, enabling automatic discovery and classification of every device within the network, including IT, OT, IoT, and IoMT devices. This includes not only managed devices but also unmanaged and shadow devices thus ensuring no asset goes unnoticed. With real-time monitoring, SOC teams gain deep situational awareness of device behavior, detecting deviations from baseline operations to proactively identify and address potential threats. This level of visibility allows SOC teams to maintain control over customer environments and significantly reduce the risk that could impact service delivery and business resilience.

Risk Assessment and Mitigation

Armis delivers unparalleled risk assessment and mitigation by continuously evaluating device risks based on vulnerabilities, behaviors, and contextual factors. SOC teams benefit from the ability to prioritize remediation efforts, focusing on devices most critical to business operations. Automated policy enforcement ensures that security measures are consistently applied across the network, reducing the attack surface and strengthening the overall defense posture. This capability enhances SOC efficiency by streamlining the identification and mitigation of high-risk, high impact assets.

Advanced Threat Detection and Response

Leveraging advanced technologies such as artificial intelligence, machine learning, and behavioral analytics, Armis provides sophisticated threat detection and response capabilities to SOC teams. By identifying anomalous device activities and behaviors that may signal security threats, SOCs are empowered to act swiftly and effectively. With automated response actions and preconfigured playbooks, Armis accelerates the identification, containment, and mitigation of incidents, minimizing their impact on customer environments and maintaining operational integrity.

Integration with Existing Security Infrastructure

Armis seamlessly integrates with existing security infrastructures, creating a cohesive and effective ecosystem within the SOC. By working in tandem with tools such as SIEMs, EDR solutions, and firewalls, Armis creates and "ecosystem of trust" that enriches security data, streamlines incident response workflows, and fosters a centralized view of security operations. SOC teams can efficiently correlate alerts, investigate incidents, and orchestrate responses, benefiting from a unified approach to managing security across complex and distributed environments.

Why SOC Providers Choose Armis

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

Enhanced Visibility, Security and Control

Armis offers unmatched visibility into all connected customer assets, including IT, OT, IoT, medical devices, and cloud 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.

Scalability For What's Next

For SOCs monitoring operations across multiple locations, Armis is built to scale accordingly. When business models or the threat landscape changes, Armis remains agile and responsive to evolving needs.

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.
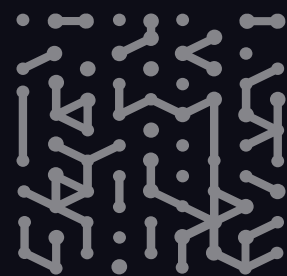
ARMIS

Armis, the cyber exposure management & security company, protects the entire attack surface and manages an organization's cyber risk exposure in real time.

In a rapidly evolving, perimeter-less world, Armis ensures that organizations continuously see, protect and manage all critical assets - from the ground to the cloud. 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 stay 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