ARMIS® Onyxia

PARTNER BRIEF

Advancing Proactive Cyber Defense

How Armis and Onyxia combine asset intelligence and AI-driven automation to transform cyber exposure management.

Overview

In a world where the digital attack surface is expanding, organizations require a comprehensive Continuous Exposure Management (CEM) solution that delivers predictive intelligence and automated governance. The integration between Armis and Onyxia empowers CISOs and security teams to manage their cyber defense programs with confidence. By feeding the Armis Centrix™ complete asset inventory and intelligence detail into Onyxia's Cyber Defense Platform, organizations can transform their security operations from firefighting mode to proactive organizational security. This joint partnership moves security governance from a manual, static exercise to a dynamic system that identifies potential "flash points," validates controls, mitigates critical exposures in a prioritized order, and proves compliance in real-time.

State of the Market

Security leaders today face a critical visibility, security and manageability crisis. CISOs and their teams often lack clear, real-time transparency into their security status because they are forced to track disparate data across dozens of tools. This frequently leads to a reliance on manual, spreadsheet-based processes to manage exposures and map controls to frameworks like NIST or ISO.

This traditional approach suffers from three fundamental flaws:

- **Inaccurate:** It relies on siloed tools like EDR or vulnerability scanners that remain blind to the unmanaged attack surface, including IoT, OT, and shadow IT.
- **Inefficient:** Static manual efforts become instantly outdated and fail to provide real-time insight into program gaps.
- **Reactive:** Point-in-time data lacks the contextualized intelligence teams need to predict and preempt emerging threats.

To survive, CISOs need deep situational awareness into asset behaviors, status, and pathway data that reflects their entire environment.

The Joint Solution

The partnership between Onyxia Cyber and Armis addresses these challenges by integrating the Armis Centrix™ Cyber Exposure Management and Security platform with Onyxia's AI-powered Preemptive Cyber Defense Platform. The joint solution provides a single, automated, and data-driven system for managing cyber defense based on a complete and accurate attack surface assessment, prioritization, and mitigation plan.

This integration solves the core challenge of visibility by replacing manual guesswork with automated governance. By combining the comprehensive situational awareness of Armis with the strategic automation of Onyxia, organizations can move from assumed security to provable operations. Security teams gain a dynamic view of their posture, allowing them to confidently identify control gaps, prioritize mitigation efforts, and assign fixes thereby optimizing stack investments and automating board reporting to eliminate unacceptable cyber risk.

How It Works: Combining Ground Truth with Actionable Intelligence

The solution functions by leveraging the distinct strengths of both platforms to create a closed-loop security ecosystem.

What Armis Brings: Deep Context and Early Warning. Armis Centrix™ provides the foundational "ground truth" for the organization. It discovers, classifies, and assesses the risk of every asset in the environment. Beyond simple inventory, Armis identifies potential exposures across assets, attack pathways, and applications. Upon identifying cyber risk, the platform works to deduplicate and contextualize findings, prioritizing them based on rich contextual details. This ensures that the intelligence fed into Onyxia is not just raw data, but a refined, actionable roadmap for mitigation.

What Onyxia Brings: Strategic Automation and Prediction. Onyxia acts as the strategic layer that ingests this comprehensive data. It automates security process workflows, maps controls to business and compliance frameworks, and utilizes AI-driven insights to reduce exposures and optimize security stack ROI. Using its predictive engine, OnyxAI, the platform forecasts performance trends up to 30 days in advance, providing early warning capabilities that allow teams to preemptively address future exposures before they become critical.

The integration is enabled via a pre-built API connector where Onyxia makes secure, read-only calls to the Armis Centrix™ platform. Onyxia queries the Armis API to pull the full asset inventory and context, serving as the definitive system of record that powers management and automation workflows.

Use Cases

Consider a CISO at a manufacturing company managing a complex hybrid environment. They must oversee a vast fleet of assets, ranging from standard IT endpoints to critical OT devices like PLCs and smart HVAC systems on the factory floor. The objective is to proactively address exposures and maintain alignment with the NIST Cybersecurity Framework (CSF) without relying on manual reporting.

The process begins with Armis Centrix providing a complete and deep assessment of the environment, identifying thousands of unmanaged and managed devices to provide full-spectrum visibility, identification, contextualization and prioritization of findings and recommended fixes. Onyxia ingests this inventory and transforms the findings into measurable Cyber KPIs, such as Mean Time to Resolve Vulnerabilities.

Through Onyxia's dashboard, the security team can:

- **Track Performance:** Monitor KPIs against industry benchmarks to identify off-SLA entities.
- **Map Compliance:** Automatically map Armis capabilities to a Security Stack Map aligned with NIST CSF controls to highlight coverage gaps.
- **Predict Risk:** Use OnyxAI to forecast KPI performance, allowing the team to fix future exposures before they impact the business.
- **Report Value:** Instantly generate customized board reports that link cybersecurity initiatives directly to business outcomes.

Solution Value and Key Benefits

Deploying the Armis and Onyxia solution delivers immediate security, operational, and financial benefits:

Complete Visibility and Context: Organizations gain a single, unified inventory of all assets (IT, IoT, OT, Cloud) directly within the management platform, eliminating blind spots.

Real-Time Compliance: The solution replaces periodic checks with continuous validation of security posture against frameworks like NIST, ISO 27001, or CIS.

Optimized ROI: Leaders can use the "Security Stack Map," powered by Armis's AI native asset intelligence, to identify redundant tools and eliminate critical coverage gaps.

Operational Efficiency: CISOs gain the contextualized intelligence needed to mobilize teams instantly against current and future risks, moving from reactive firefighting to strategic defense.

Conclusion

Onyxia Cyber is the AI-powered Preemptive Cyber Defense Platform for the modern enterprise, enabling security teams to leverage data to proactively improve strategies and mitigate exposures. By partnering with Armis, Onyxia ensures that this predictive power is based on the most accurate, comprehensive organization risk data available. This collaboration provides CISOs with the clarity and control they need to optimize operational effectiveness and confidently protect their organizations.