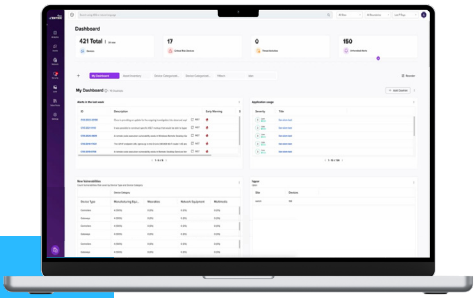
Armis Centrix™ for Actionable Threat Intelligence

Securing an organization from cyberattacks has traditionally been a reactive effort. This approach is fundamentally flawed because it means reacting to events only after an attack is in progress and damage is already done.

Redefining Security By Preempting the Attack

Armis Centrix™ for Actionable Threat Intelligence is the proactive cybersecurity solution designed to empower organizations with early warning intelligence to anticipate and mitigate cyber threats effectively. By leveraging AI-driven actionable threat intelligence, Armis Centrix™ provides insights into potential threats, allowing organizations to understand their impact and take preemptive action.



It's time to stop reacting to threats

With human intelligence, smart honeypots and state of the art research, Armis Centrix™ ensures timeliness, unparalleled coverage and accuracy, enabling organizations to stay ahead of evolving cyber threats and protect their critical assets with confidence. Armis Centrix™ for Actionable Threat Intelligence allows organizations to:

See

Potentially weaponized threats before CVEs are ever published and fully visualize your attack surface.

Protect

Preempt threat actors, address vulnerabilities that are actually being exploited.

Manage

Ongoing protection against evolving attack methods, establish workflows and track risk reduction.

Proactive Vulnerability Intelligence - Focus On What Really Matters

Early Warning

Early warning intelligence gives you the time to harden your environment before an attack is ever launched. Armis Centrix™ for Actionable Threat Intelligence can prove over thousands of instances where the early warning intelligence is ahead (at times, by up to a year) of CISA KEV.

SOC/VOC Risk Prioritization

Real-time vulnerability exploit data integrated directly into risk prioritization, empowering the SOC and VOC to focus on what truly matters and what threat actors are actually exploiting.

Third Party Risk Management

Discover and report on an assessment and quantification of risk from third parties by leveraging the Armis Centrix™ platform or by integrating the feed into your existing security stack.

IP Forensics

Empowers the SOC team by providing a measure of the reputation of an IP address at a certain point in time.

TTP Intelligence

Armis Centrix™ for Actionable Threat Intelligence Pro (ATI Pro) provides an enhanced offering for the SOC that provides organizations with meaningful, personalized detection from Tactics, Techniques and Procedures (TTPs), custom honeypots and curated threat hunting.

Threat Hunting Prioritization

ATI Pro provides an enhanced offering that includes automated, customized threat hunting using customer's data. TTPs (including SIEM/SOAR integrations) can be part of this process.

See, protect, and manage your attack surface with Armis Centrix™ Actionable Threat Intelligence

Visit **Armis.com** to find out more

Key features that make Armis Centrix™ the go-to platform for Total Exposure Management.

A seamless, frictionless, cloud-based cyber exposure management platform, with five AI-driven products, including Armis Centrix™ for Actionable Threat Intelligence.

The largest AI-driven Intelligence Engine tracking billions of assets.

A complete, always-on and accurate view of all your assets.

Prioritized vulnerabilities with shorter MTTR.

Accurate threat detection and response.

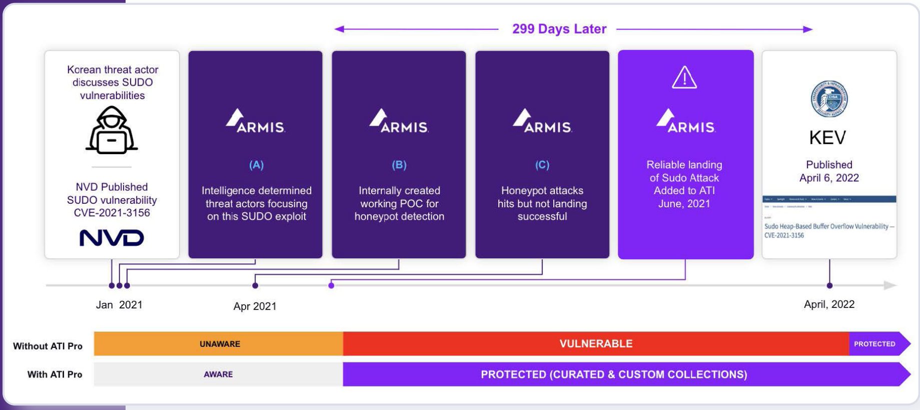
Dedicated vertical solutions for OT/IoT and medical device security.

> “The high fidelity intelligence is critical to us maintaining a secure environment and it’s easy for my team to focus on the most important things, prioritize those vulnerabilities and patch what is required.”

Pieter van der Merwe, CSO
Woolworths Group

Why Organizations Trust Armis Centrix™ for Actionable Threat Intelligence to Deliver Better Outcomes

1. **Early warnings** to any potential threats before they impact your organization.
2. Proof of over thousands of instances where the **early warning intelligence is ahead** (at times, by up to a year) of CISA KEV.
3. **Attacker Focused Insights** which fills a gap that exists today in intelligence feeds.
4. Focus on the **vulnerabilities that are being exploited** by threats before they hit the wild.
5. **98% reduction** in the number of vulnerabilities organizations need to worry about.
6. **AI-driven, automated** contextual risk determination and possible countermeasure actions.
7. **Redefine threat hunting** by proactively identifying CVE gaps and vulnerabilities that are still in the formulation stage.



299 Days Later

Korean threat actor discusses SUDO vulnerabilities

NVD Published SUDO vulnerability CVE-2021-3156

NVD

ARMIS (A) Intelligence determined threat actors focusing on this SUDO exploit

ARMIS (B) Internally created working POC for honeypot detection

ARMIS (C) Honeypot attacks hits but not landing successful

ARMIS Reliable landing of Sudo Attack Added to ATI June, 2021

KEV Published April 6, 2022

Sudo Heap-Based Buffer Overflow Vulnerability — CVE-2021-3156

Jan 2021

Apr 2021

April, 2022

Without ATI Pro: UNAWARE — VULNERABLE — PROTECTED

With ATI Pro: AWARE — PROTECTED (CURATED & CUSTOM COLLECTIONS)

See, protect, and manage your attack surface with Armis Centrix™ Actionable Threat Intelligence

Visit **Armis.com** to find out more