



# Shifting from a Reactive to Proactive Response

With Armis Centrix™ for Early Warning.

By leveraging AI-driven actionable intelligence, Armis Centrix™ provides insights into the vulnerabilities that threat actors are exploiting in the wild or are about to weaponize, allowing organizations to understand their impact and take preemptive action.

**98%** Reduction in the number of vulnerabilities you need to worry about.

Target **1**

## Dark Web Monitoring

Dive deep into the recesses of the dark web, monitoring and intercepting malicious chatter.

### OUTCOME

Invaluable insights into potential vulnerabilities still in the formulation stage.

Target **2**

## AI Honeypots

Dynamically deploy honeypots in “hotspots,” to observe malicious behaviors and techniques in real-time.

### OUTCOME

Honeypot attack hits and identifies known and unknown exploits in the wild long before they pose a tangible risk to your organization.

## 6 Months

The average time it takes organizations to discover a breach, and a further **69 days** to contain it.

## 800 Cases

Where Armis Centrix™ for Early Warning flagged CVEs as exploited **before industry benchmarks**.

Target **3**

## Armis Labs (HUMINT)

Targeting the humans behind the keyboard, HUMINT captures threat activity. Understands 200 different languages specifically about exploitation of vulnerabilities.

### OUTCOME

Armis ensures unparalleled coverage and accuracy, enabling organizations to stay ahead of evolving cyber risk and protect their critical assets with confidence.

**80%**

Of Exploits are published **before** the CVEs are released

**23 Days**

The average gap between the publication of an exploit and the corresponding CVE

**10x**

Broader and deeper view into the threat world with **Armis Centrix™** for Early Warning



An early warning feed on threat actor behaviors that constantly grows, enriches and strengthens the Asset Intelligence Engine for true proactive Exposure Management.

