WHITE PAPER

Operationalizing Early Warning Intelligence for The Security Operations Center (SOC) and Risk Management

Introduction

Cyber threats are evolving at an unprecedented pace, putting critical infrastructure and enterprises alike in the crosshairs of both criminal operations and state actors. To protect employees, customers, and critical assets, Security Operations Centers (SOC) and Vulnerability Management teams (VM) must integrate early warning intelligence into their operations. By doing so, organizations and government agencies can take a proactive approach to the threat before it impacts your organization.

This whitepaper aims to provide SOC and VM teams with a comprehensive guide on how to operationalize early warning intelligence to enhance their ability to protect their organizations.

What is Early Warning Intelligence?

Early warning intelligence refers to the proactive gathering, analysis, and dissemination of information regarding potential threats before they materialize into actual attacks. By anticipating these threats, security teams can take preventive measures to mitigate their impact.

This intelligence is derived from leveraging AI to act with various sources, including but not limited to, deception technology, threat feeds, dark web monitoring, open-source intelligence (OSINT), and internal telemetry. The primary goal is to find what vulnerabilities or attacks threat actors are exploiting in the wild or are about to weaponize.

Understanding the Threat Landscape

To effectively defend against cyber threats, it's crucial to understand the threat landscape. Here are some key questions that threat intelligence can help answer:

> **Who are the adversaries targeting your industry?**

> **What tools and tactics do they use?**

> **Where and when do they focus their offensive operations?**

> **How do they execute these operations from a behavioral analysis perspective?**

By utilizing early warning threat intelligence solutions to assess and analyze the above questions, security teams can develop timely, accurate, and evidence-based intelligence that guides better strategic and tactical decisions to secure vital assets and protect human life. Early warning empowers organizations to prioritize risks based on unique business needs and on what attackers are actually targeting.

Historically, most organizations and government agencies have attempted to answer these questions and mitigate risks by using the Common Vulnerability Scoring System (CVSS) to score vulnerabilities (CVEs). However, CVSS scores are often disconnected from actual risk as they fail to differentiate the urgency of vulnerabilities to the business. Notably, 80% of exploits occur before a CVE is even released. Threat actors are not concerned with CVSS scores; their focus is on exploiting vulnerabilities. A threat actor can easily target a mid- or low-level CVE, as these may not receive the same urgency to patch as high-level vulnerabilities.

Concurrently, organizations maintain an ever increasing pool of assets, where they are simply unable to consistently patch them all due to the sheer volume of assets and the maintenance windows which are often not sufficient to address all the issues. According to Ponemon, "60% of compromises are from known vulnerabilities." This problem is top 3 for CISOs today (according to the YL Ventures CISO Survey). A Fortune 100 CISO recently stated, "There are millions of vulnerabilities in our organization, but only a small percentage matter." Organizations need a better way to handle this real problem and address the risk that causes the most significant threat to the organization in question.

Enter Early Warning Intelligence…

By utilizing early warning solutions to assess and analyze the above questions, security teams can develop timely, accurate and evidence-based intelligence that guides better strategic and tactical decisions to secure vital assets and protect human life. Early warning empowers organizations to prioritize risk based on unique business needs and based on what threat actors are actually attacking.

Benefits of Early Warning Intelligence

Proactive Defense: Anticipate threats before they materialize, enabling preemptive measures.

Reduced Incident Response Time: Quicker identification of threats allows for faster containment and remediation (MTTR).

Enhanced Situational Awareness: Understanding in real time the latest threat landscape for your organization and emerging attack vectors.

Just Imagine…

What if you could buy two more months to act in order to handle an attack like log4J?

What if you could be ahead of CISA KEV by 11 months?

What if you could get early warnings to any potential threats before they impact your environment?

Necessary Components for Early Warning Threat Intelligence

Coverage Intelligence should provide the evidence needed to guide decision-making.

Accurate Faulty intelligence leads to bad decisions. It should originate from trusted sources and be vetted.

Relevant The threat should matter to the organization; irrelevant intelligence wastes resources.

Timely Intelligence should be timely enough to impact decisions effectively.

Questions to ask yourself while considering Early Warning Intelligence

Do you have “boots on the ground” knowledge of what is happening in your organization in real time?

Are you in the dark about what vulnerabilities you should prioritize first?

Are you experiencing an increasing backlog of vulnerabilities and patching that you cannot get to?

Are you experiencing an increase in MTTR metrics?

Does CVSS scoring provide insufficient guidance on the criticality of the vuln to your business operations?

What would you do differently if you had more time to prepare before an attack was launched?

Data Sources for Early Warning Threat Intelligence

Effective early warning intelligence starts with data. Here are the primary data sources SOC and VM teams should consider:

First-Party Data

This includes information from your organization's networks, devices, logs, policies, risk assessments, and incident data. It forms the foundation of intelligence as it can be enriched with other sources to turn the data into actionable information.

Second-Party Data

This includes common security frameworks by organizations such as the National Institute of Standards and Technology (NIST), The Center for Internet Security (CIS), ZeroTrust, MITRE and regulatory compliance requirements like FedRAMP, DORA, PSTI Compliance and C5 Compliance.

This also comes from trusted partners such as other organizations in the same vertical, industry trust groups, Information Sharing and Analysis Centers (ISACs), and trade organizations. These sources align closely with your organization's specific intelligence requirements.

Third-Party Data

This is provided by vendors and includes offerings like The Armis Asset Intelligence Engine is a collective AI-powered knowledge base, monitoring billions of assets world-wide in order to identify cyber risk patterns and behaviors. It feeds the Armis Centrix ™ platform with unique,actionable cyber intelligence to detect, prioritize and remediate real-time threats across the entire attack surface

Fourth-Party Data

Commonly referred to as "closed source" data, this originates from dark web resources. It can enable exercises like battle damage assessments to further contextualize a threat.

Understanding Early Warning Threat Intelligence Audiences

Strategic Audience

Focus on long-range considerations like industry threat landscape, policy and risk assessments, budgeting, tool acquisition, and security strategy.

Operational Audience

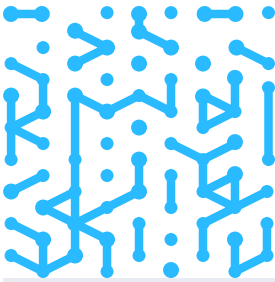
Focus on mid-range considerations like SOC team structure, operational directives, personnel assignment, and asset & network visibility.

Tactical Audience

Concerned with real-time execution, critical vulnerabilities, new indicators or behaviors targeting the industry, and immediate action items.

Technical Audience

Focus on toolsets and implementation of threat intelligence. Automation, searching for behaviors in SIEM systems, triaging alerts, blocking adversary infrastructure, tuning IDS/IPS, and enriching first-party data with novel intelligence.



Operationalizing Early Warning Intelligence

Step 1: Integration with Existing Systems

To maximize the effectiveness of early warning intelligence, it should be seamlessly integrated with your existing SOC and VM systems. This includes:

- **Security Information and Event Management (SIEM)** systems for real-time correlation and analysis.
- **Threat Intelligence Platforms (TIPs)** for centralized management of threat data.
- **Incident Response Tools** for streamlined workflows (ie: ticketing and remediation systems) and automated responses.

Step 2: Source and Curate Intelligence

Identify reliable sources of threat intelligence, both internal and external. These may include:

- **Commercial Threat Feeds**: Paid services offering high-fidelity threat data.
- **Open-Source Intelligence (OSINT)**: Publicly available information from forums, blogs, and social media.
- **Internal Telemetry**: Data from internal security tools such as firewalls, IDS/IPS, and endpoint protection.
- Curate the collected intelligence to filter out noise and focus on actionable insights relevant to your organization.

Step 3: Continuous Monitoring and Analysis

Employ continuous monitoring to detect early signs of cyber threats. This involves:

- **Automated Threat Detection**: Use machine learning and AI to identify anomalies and patterns indicative of potential threats.
- **Human Analysis**: Analysts review and validate automated alerts to ensure accuracy and relevance. Once this is performed, fine tuning of the system may be indicated to enhance future threat hunting efforts.

Step 4: Contextualize and Prioritize Threats

Contextualize the intelligence by correlating it with your organization's assets, vulnerabilities, and business processes. Prioritize threats based on their potential impact and likelihood. Factors to consider include:

- **Asset Criticality**: Importance of the affected asset to your operations.
- **Threat Actor Sophistication**: Skill level and resources of the threat actor.
- **Attack Vector**: Likely method of attack and its feasibility.

Step 5: Implement Proactive Measures

Based on the prioritized intelligence, implement proactive measures to mitigate identified threats. These measures may include:

- **Patching Vulnerabilities**: Apply patches to known vulnerabilities in your systems using prioritization as the means for mitigation.
- **Strengthening Defenses**: Enhance security configurations and deploy additional protective measures.
- **Conducting Red Team Exercises**: Simulate attacks to test and improve your defenses.

Step 6: Incident Response and Recovery

In the event of a detected threat, execute your incident response plan promptly. Key actions include:

- **Containment**: Isolate affected systems to prevent further spread via segmentation.
- **Eradication**: Remove the threat from your environment.
- **Recovery**: Restore normal operations and apply lessons learned to prevent future incidents.

Step 7: Continuous Improvement

Regularly review and refine your early warning intelligence processes. Gather feedback from SOC and VM teams, conduct post-incident analyses, and stay updated on the latest threat intelligence methodologies and tools.

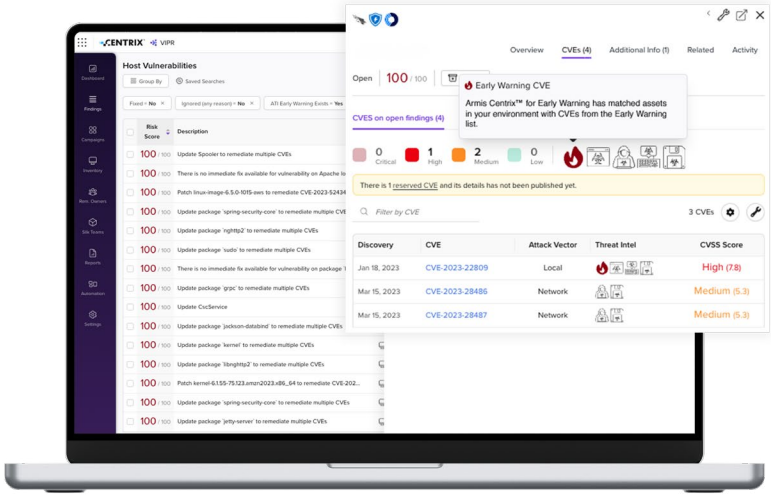
Conclusion

Operationalizing early warning intelligence is essential for SOC and VM teams to anticipate and mitigate cyber threats before they can impact your organization or government agency. By integrating AI/ML based intelligence with existing systems, sourcing and curating threat data, continuously deduplicating, monitoring, analyzing threats, contextualizing and prioritizing them, implementing proactive measures, and executing a robust incident response plan, organizations can enhance their cyber defense capabilities. Continuous improvement ensures that these processes remain effective in the face of an evolving threat landscape.

Introducing Armis Centrix™ for Early Warning

Armis Centrix™ for Early Warning 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 intelligence, Armis Centrix™ provides insights into potential threats, allowing organizations to understand their impact and take preemptive action.



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.

98% reduction in the number of vulnerabilities organization's need to worry about

Over 800 times where Armis Centrix™ for Early Warning has been ahead of CISA KEV

Over 1,600 vulnerabilities that CISA KEV doesn't know about

The Armis Solution & Results

With Armis Centrix™ for Early Warning you'll get:

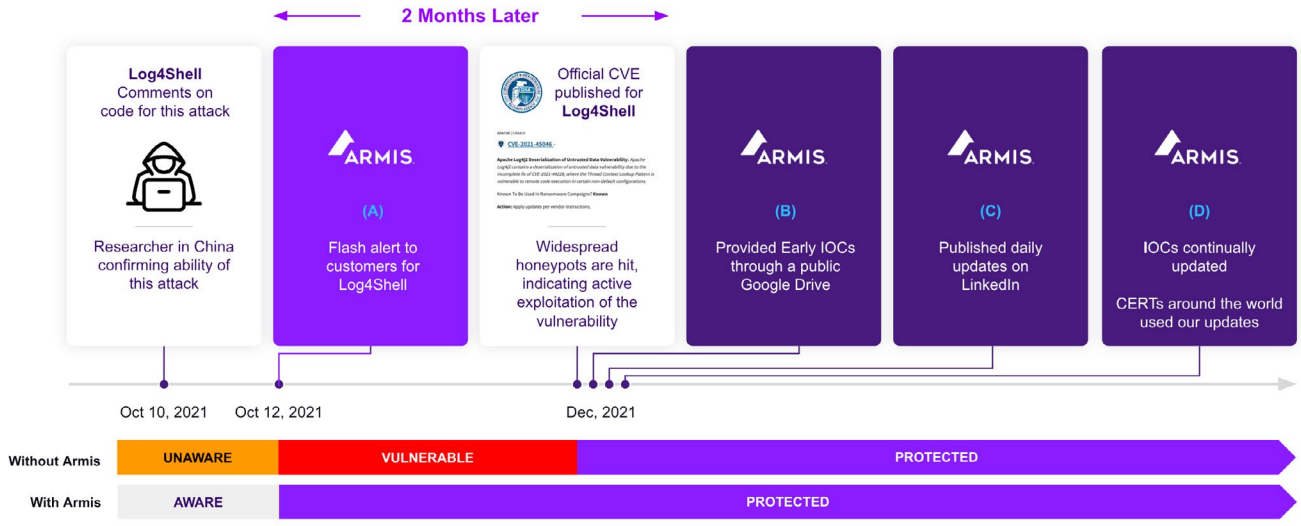
Early warning intelligence fills a gap that exists today in intelligence feeds. Focus on timely, accurate and evidence-based intelligence on the vulnerabilities that are being exploited in the wild or are about to be weaponized.

CVE Insights Breakdown has identified hundreds of CVEs prior to being published in CISA KEV.

Preempt an Attack gives you time to secure your environment before an attack is ever launched and before any damage has ever occurred.

Proactive Response that gives you the ability to prioritize your efforts and get out of reactive firefighting mode.

Threat Hunting Redefined AI capabilities that proactively identify CVE gaps and vulnerabilities that are still in the formulation stage.



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