Come spostare la Threat Detection and Response "left of boom": analisi predittiva per evitare il disastro

Manuela Santini | Docente Clusit, *Direttivo Women For Security*
Stefania Iannelli | Account Executive, Armis

Come spostare la Threat Detection and Response "left of boom": analisi predittiva per evitare il disastro

Security Summit

11 Marzo 2025

Manuela Santini

Clusit - Women For Security

Stefania Iannelli

Armis

+1/3

degli incidenti in Italia nel 2024 sono causati da Malware

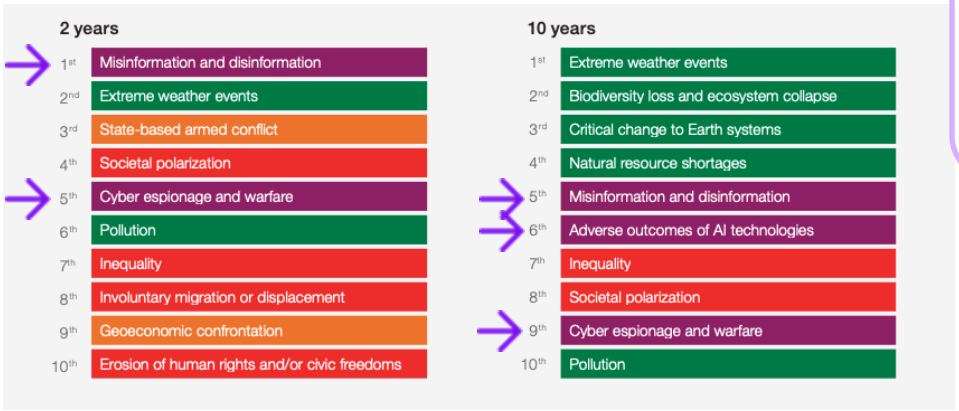
+90%

è la crescita degli incidenti in Italia basati su Vulnerabilities, dal 2023 al 2024

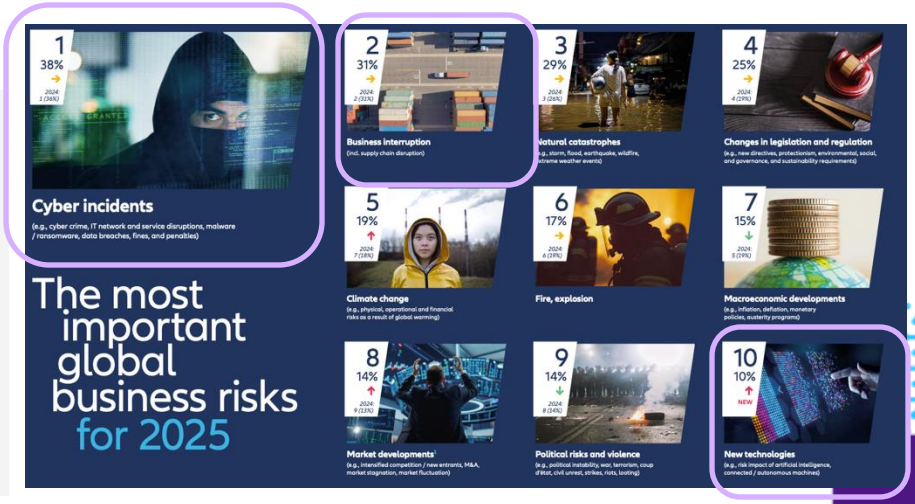
+35%

è la crescita degli incidenti in Italia basati su phishing e ingegneria sociale, dal 2023 al 2024

From Boardrooms to Davos: The Silent Crisis Everyone is Talking About



WEF Global Risks Report 2025



Allianz Risk Barometer 2025

The Growing Cost of Cyber Incidents

Average Cost of a Data Breach

In the millions
(Gartner: $4.88 million*)

*Gartner, Use Data Storage Management Services to Address Exponential Growth of Unstructured Data. Rizvan Hussain, Chandra Mukhyala, Michael Hoeck, 10 October 2024

+10% in 2024 compared to 2023

#	Country	2024	2023
1	United States	$9.36	$9.48
2	Middle East	$8.75	$8.07
3	Benelux	$5.90	–
4	Germany	$5.31	$4.67
5	Italy	$4.73	$3.86

*IBM's Cost of a Data Breach Report

90% of attacks are linked to cybercrime

*Clusit – Rapporto 2025 sulla Cybersecurity

If it was measured as a country, **cybercrime** — which is predicted to inflict damages totalling $9.5 trillion USD globally in 2024, according to Cybersecurity Ventures — **would be the world's third-largest economy** after the U.S. and China, surpassing the wealth of entire nations


GOVERNANCE DELLA SICUREZZA & GESTIONE DEL RISCHIO
Minacce crescenti e sofisticate
Monitoring, Incident Response, Supply Chain Security SSDLC, SecDevOps,
Resilienza Digitale & Fiducia
NIS2, DORA, GDPR, AI Act, Cyber Resilience Act, Direttiva CER
OT


ARMIS
BOOM!

ARMIS

The moment of the actual breach or attack – the point of failure where defences are penetrated

- EPP
- Firewall
- WAF
- IDS

ARMIS

RIGHT OF BOOM

Actions and responses taken after a cybersecurity incident or attack has occurred
Response-Recovery-Learning

Incident Response

Disaster Recovery

XDR

SIEM

ARMIS

LEFT OF BOOM

All the proactive measures taken before an attack to prevent it or minimize its impact

Threat Intelligence

Vulnerability Management

Threat Hunting

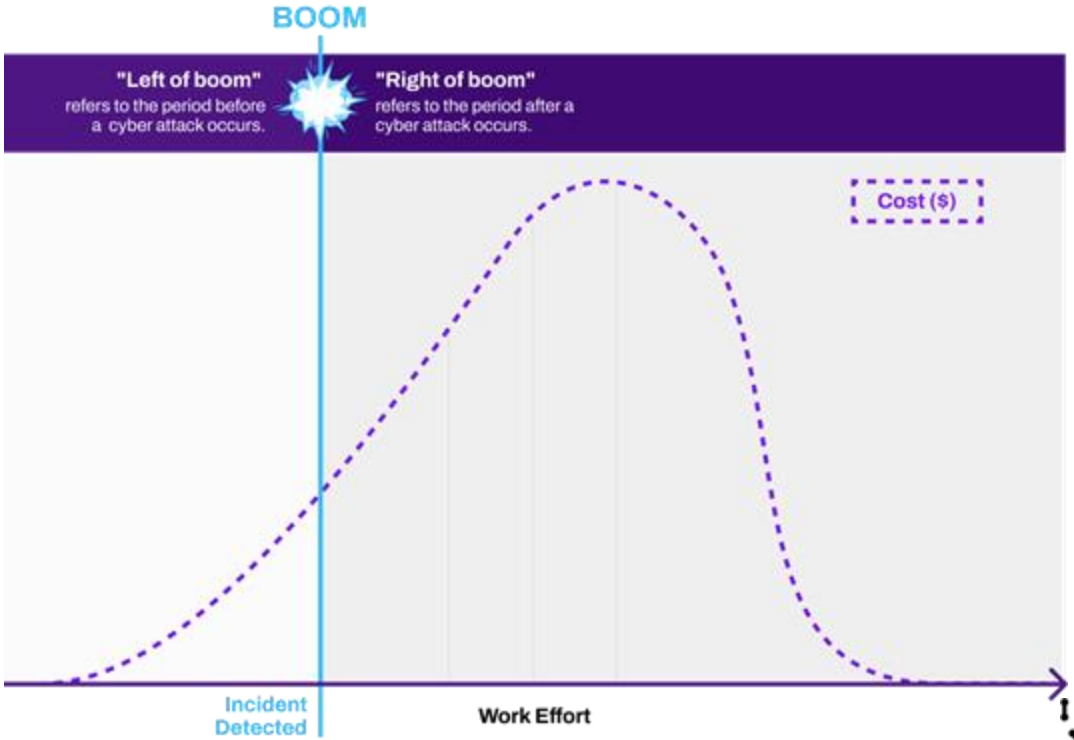
Exposure Management

In military terms, “left of boom” refers to actions taken to disrupt adversary plans before an explosive event occurs

In cybersecurity, it signifies a proactive stance to detect and mitigate threats before they penetrate defences.

Just as intelligence gathering is essential in military operations to foresee and thwart attacks, cyber threat intelligence plays a similar role in identifying potential weaknesses and threat vectors early on

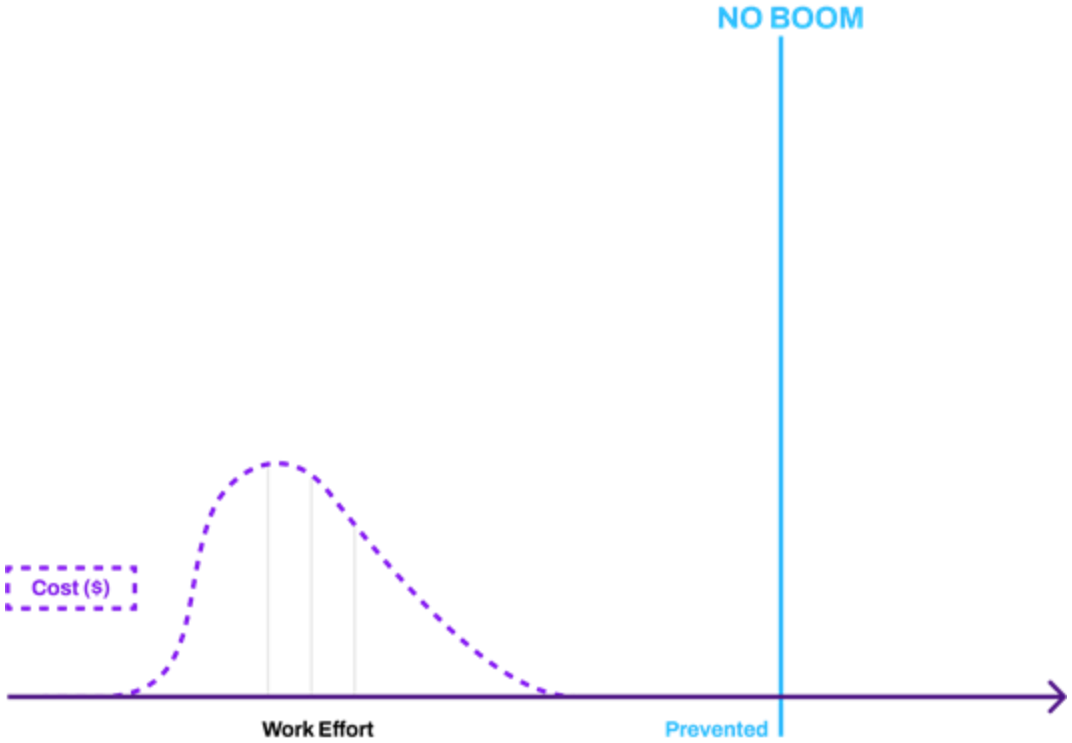
The Growing Cost of Cyber Incidents



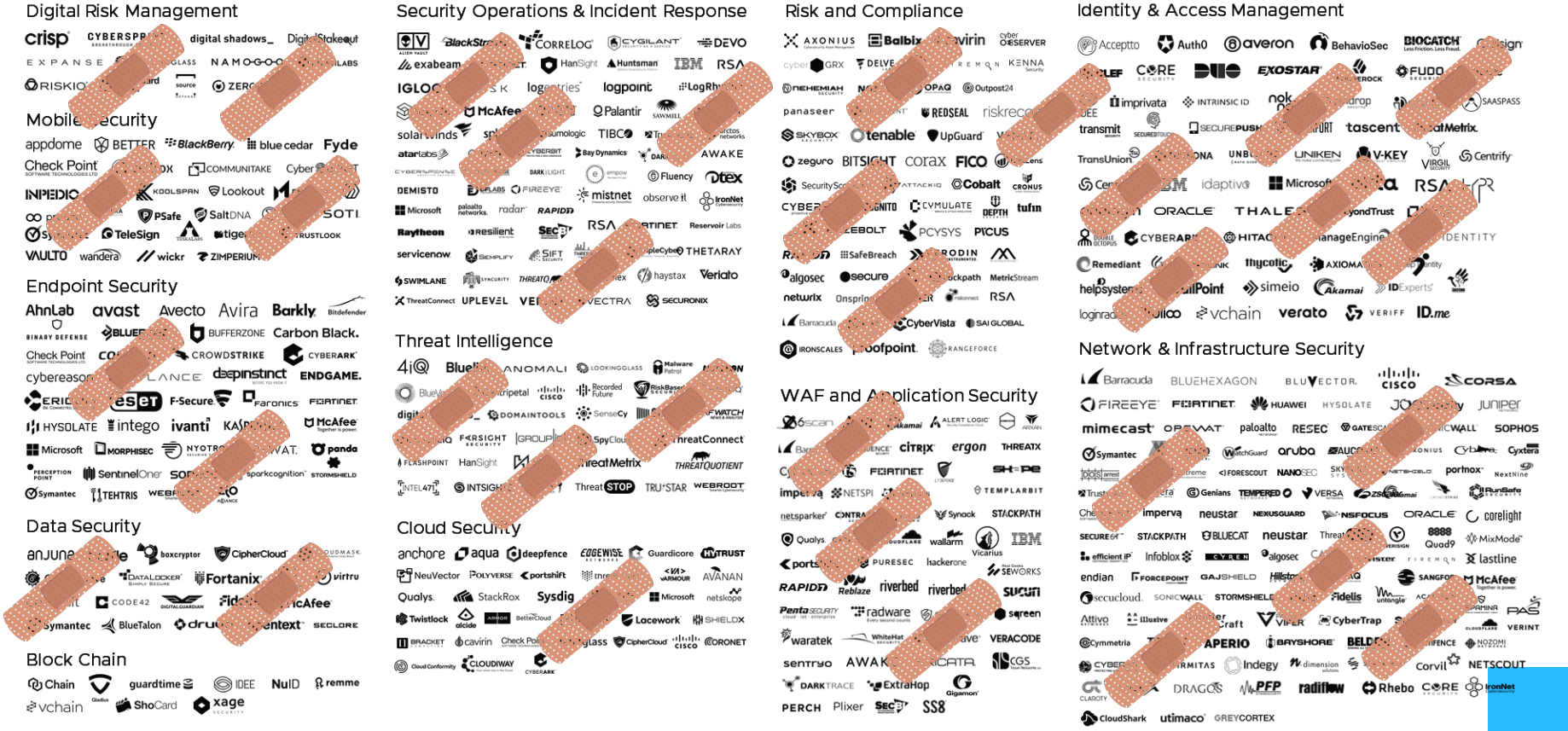
Moving to Early Prevention Mitigates Risk

Saves **time, effort and money**

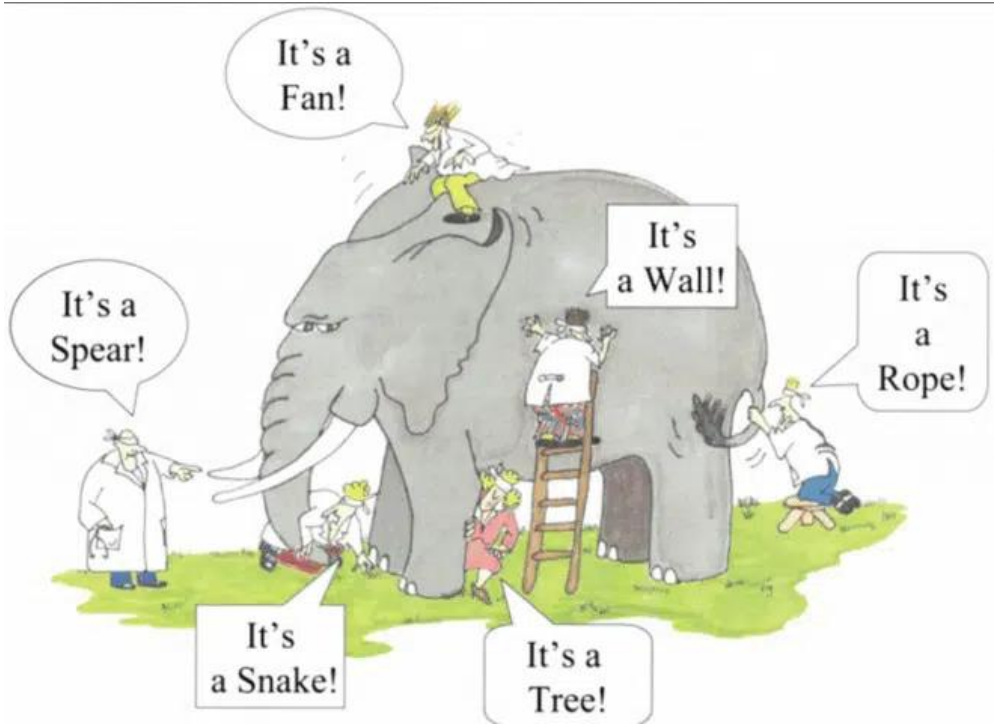
Stop Threat Actors in their Tracks!



Cybersecurity Market is Complex

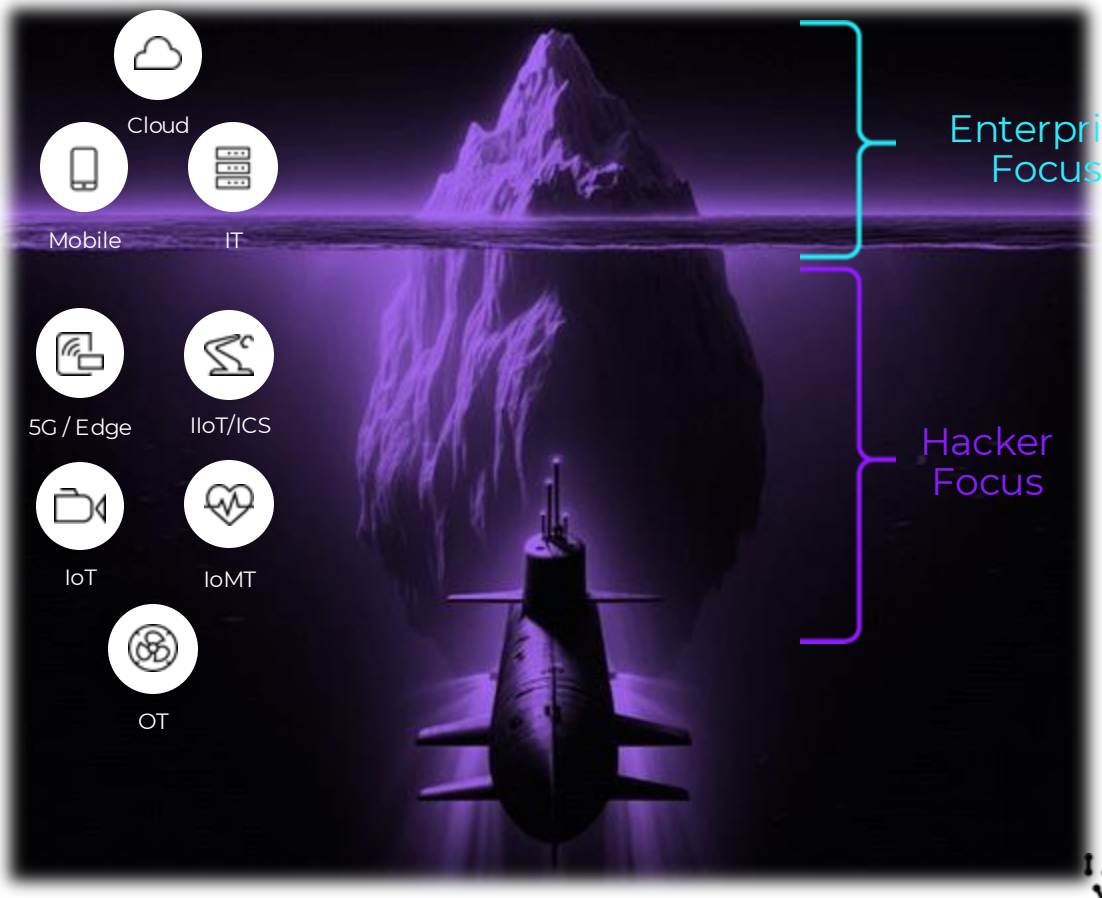


Lack of Visibility and Contex



Each security tool generates different data, leading to a fragmented view

Attack Surface



40%

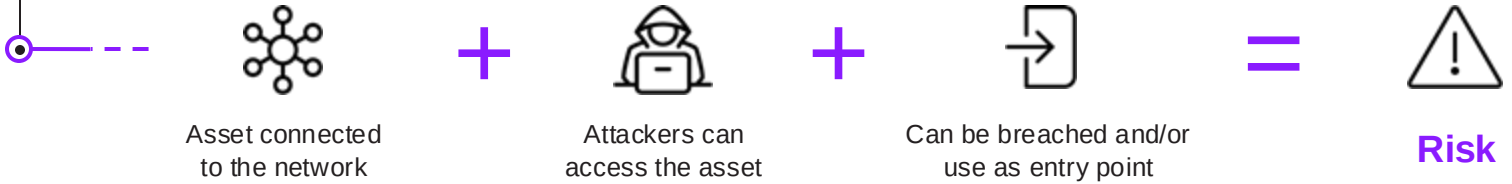
of the assets that are connected to the network are **unmonitored**

Armis research commissioned with Vanson Bourne, October 2023

Every Connected Asset expands the **Attack Surface**

ARMIS

Assets



Security Findings

The Landscape of Cybercrime: Emerging Threats and Attack Vectors

Cybercriminals Remain Opportunistic: Legacy Attack Vectors

3 out of 4 attacks exploits vulnerabilities from before 2022

> ‘A new breed of actors is emerging on the cyber battlefield: cyber mercenaries and proxy groups. These private contractors operate in the shadows and often conduct operations on behalf of nation-states, often with plausible deniability.’

> *60% of compromises are from known vulnerabilities*

Ponemon

Legacy Vulnerability Management Is Failing

160 hours per week to monitor and track threats

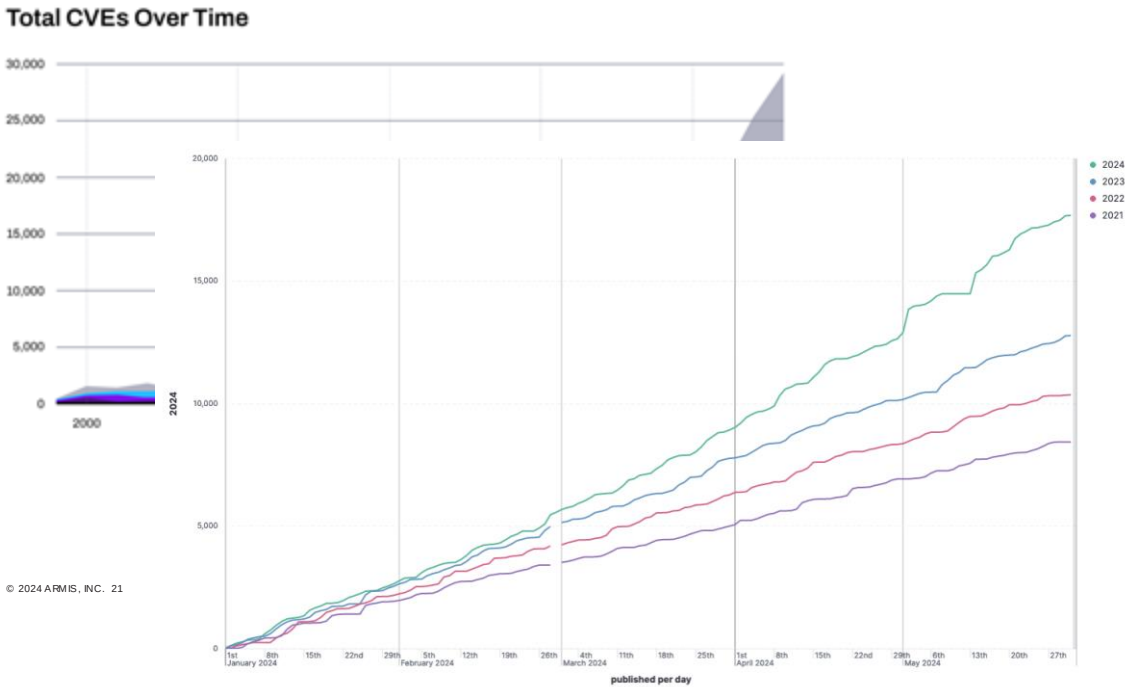
It takes more than 20 minutes of manual effort to review a CVE

> *CVSS is not a measure of risk.*
>
> - **NIST**

Because of ineffective processes and inconsistent risk prioritization, security teams can't achieve sustained clarity on **what** to fix, **who** should fix it, and **how** it should be fixed.

Legacy Vulnerability Management Is Failing

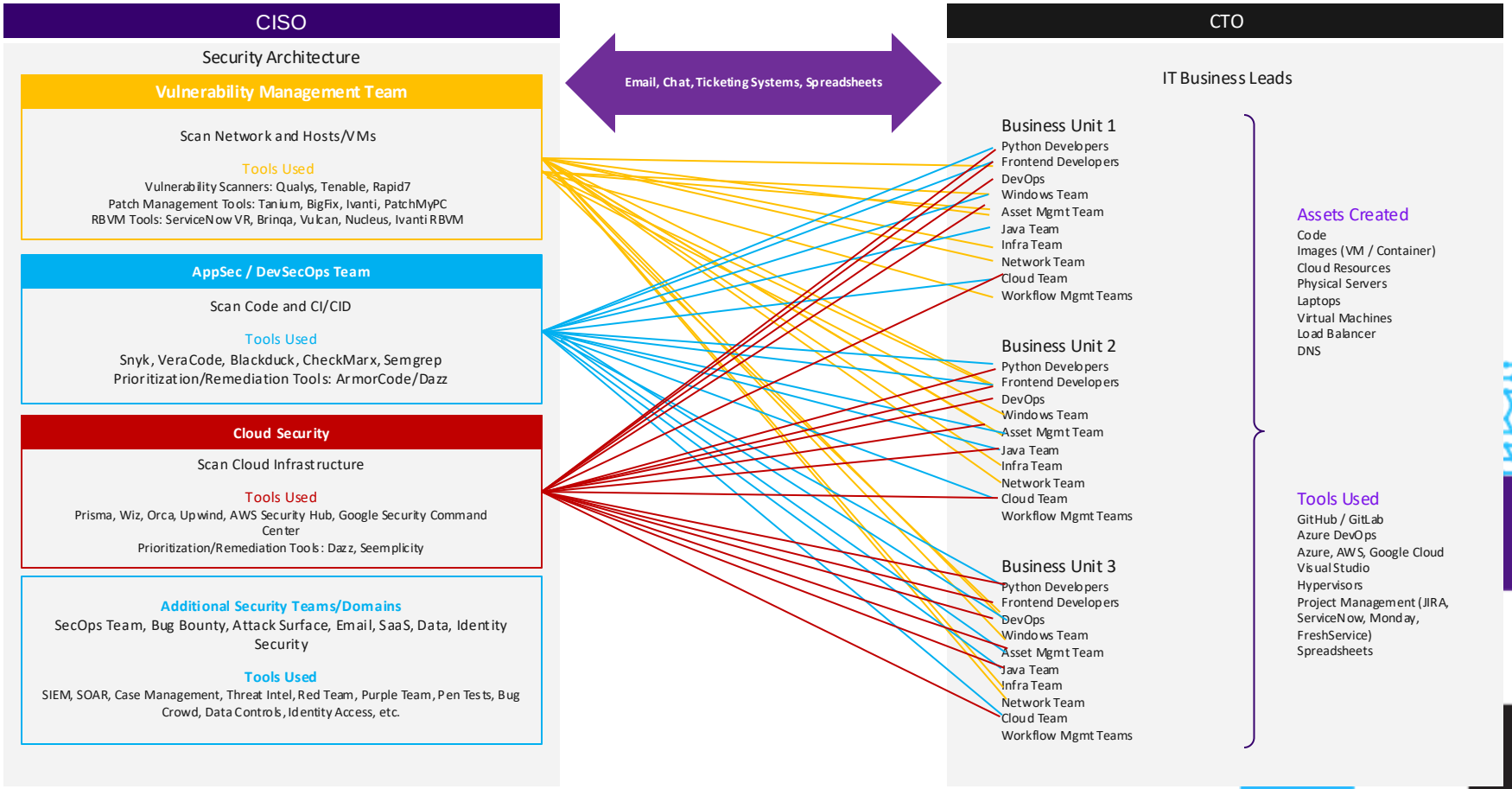
Does **Not** Address The Bigger Issue



The Current Workflow Process Is **Broken**

- Not built to handle huge data volumes from vulnerability, cloud, code, and AppSec
- Does not take into account security risk, asset profile, business impact
- Does not consider security gaps, such as compliance failures, misconfigurations, and operational blind spots
- Does not bridge the gap between teams identifying risk, and teams fixing risk

The ‘Spaghetti’ Challenge



GESTIRE UNA VULNERABILITÀ È COME GIOCARE A UN FLIPPER...

Leveraging Artificial Intelligence

Shifting “Left of Boom”

- **AI-Powered Tools**
- **Synthetic data**
- **Detection-as-Code (DaC)**

With AI-driven reasoning, organizations can achieve faster mean time to detect (MTTD) and mean time to respond (MTTR), streamlining incident response processes and bolstering overall threat management

The Evolution of Vulnerability Management

Shifting “Left of Boom”

The new model for vulnerability management

- **Contextualization: helps and translates a generic severity score to a prioritization based on the specific asset, environment and business impact**
- **Contextualization: helps security teams identify which finding represents the most urgent risk to the organization**
- **Holistic Approach: considers asset context, environmental factors, and threat intelligence**

Consolidating findings across various security domains, including cloud, code, host, and applications From enterprise IT to incorporate IoT, OT and critical infrastructure

The Power of Early Warning

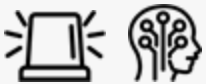
Shifting “Left of Boom”

The Ultimate Risk Prioritization Filter

- 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 of any potential threat(s) before they impact your environment?

© 2025 ARMIS

Early Warnings at Work

OBSERVE	VALIDATE	CONFIRM	ALERT
 **Threat actor discusses a CVE** on a dark web slack channel	 **AI Intelligence** Identifies threat actors, flaws in their operations and context of their discussions.  Create a working for **honeypot detection**.	 **Honeypot attack hits and identifies** known and unknown exploits in the wild.	 CVE added to **Early Warning list and customers alerted.**
EARLY WARNING		**EXPLOITATION**	

How Early Is Early Warning?

800

Armis Labs Early warnings before CISA KEV

10 Days Early

2 Months Early

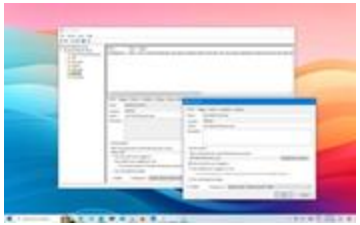
The golden source for IOCs for CERTs world-wide

64 Days Early

1,600+

Armis Labs Early Warnings not yet seen by CISA KEV

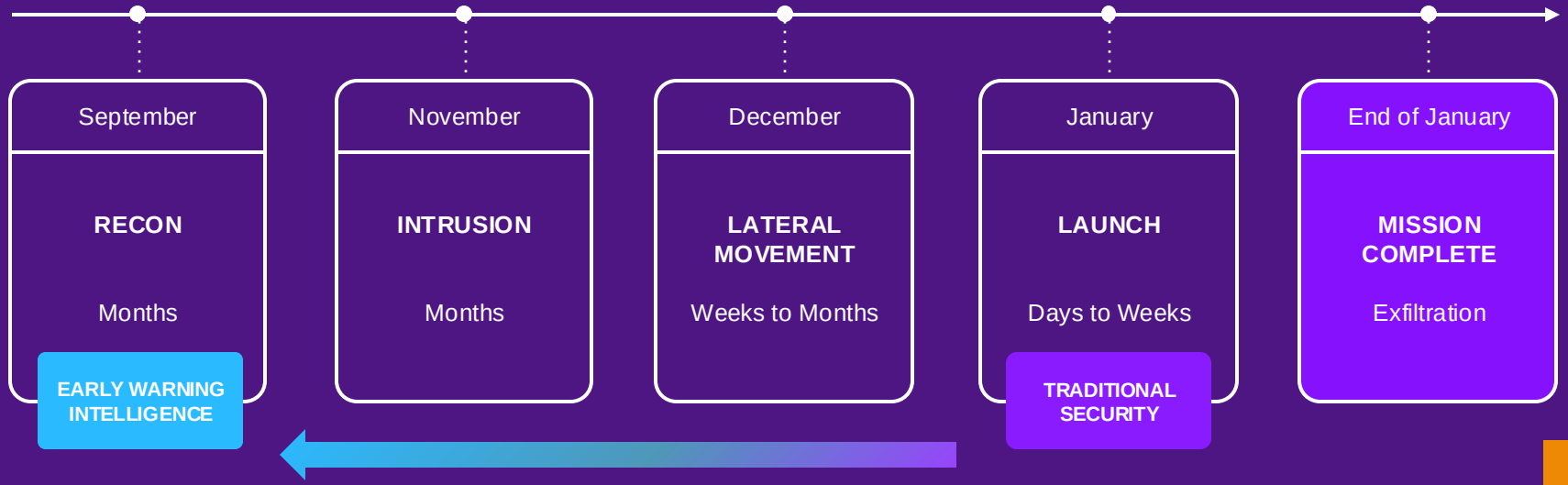
55 Days Early



2 Years Early

5 Years Early

Preempt Attacks with Early Warning Intelligence



Leverage AI-powered Discovery Tools for Extreme Visibility Across Your Attack Surface

Armis Reduces Attack Kill Chain Exposures Time

Time

Early warning of asset risk **buys you time** to address the threat before the attack is launched

Protection

Full visibility and contextualization of all assets and their behavior **reduces risk** across the environment

Remediation

Adaptable prioritization, grouping of findings, and AI-driven ownership assignment drastically **reduce MTTR**

Exposure Management

From understanding the attack surface, to intelligently reducing risk where it matters, achieving actual security

AI-Powered Asset Discovery: New assets real time detection and consolidation

Profile Classification: Deep learning of asset behavior and protocol attributes for profile classification

Asset Context: Aggregating and clustering additional asset-related context

Threat Detection: Anomalous behavior detection, malicious hosts and tunnelling classifiers

Risk Score: Asset criticality, graph-centrality and data exposure engines

Investigation: Alert investigative context and workflow suggestions

Manage Risk: Vulnerability criticality classifiers and unified prioritization

Take Action: Segmentation recommendations, ACL rules suggestions

Policies and Reporting: Personalized to the needs of the organization

Thank you!

Learn more about Armis at **booth** and at armis.com

Armis Centrix™ Cyber Exposure Management Platform

Asset Management and Security

Complete inventory of all asset types allowing any organization to see and secure their attack surface

OT/IoT Security

See and secure OT/IoT networks and physical assets

Medical Device Security

Complete visibility and security for all medical devices

VIPR Prioritization and Remediation

Consolidate, prioritize and remediate all vulnerabilities and security findings

Early Warning

Early warning system leveraging AI intelligence to stop attacks before they impact your organization

Recap: Challenges

Attacchi Cyber Sempre Più Sofisticati

Gli attaccanti sfruttano l'intelligenza artificiale, mentre molte aziende si affidano ancora ai fogli Excel per organizzare le proprie difese.

I malware basati su AI saranno in grado di **evolversi e adattarsi autonomamente**, rendendo gli attacchi **più rapidi, difficili da individuare e potenzialmente molto più distruttivi**.

Troppi Silo Organizzativi

I silo limitano la collaborazione tra i team di Information Security e IT, e riducono la capacità dell'IT di tradurre la sicurezza in azioni concrete e operative.

Gestione vulnerabilità vecchio stile

Gli attaccanti continuano a sfruttare vulnerabilità note, perché molti sistemi restano non aggiornati e non protetti.

Inoltre, la gestione tradizionale delle vulnerabilità non affronta altri aspetti critici della sicurezza, come errori di configurazione, sistemi a fine vita (EOL), problemi di licenze, vulnerabilità applicative, risultati di audit e altri rischi.

Troppi Strumenti di Sicurezza

Hanno portato a una crescente complessità, errori di configurazione e disallineamenti nelle difese.

Superficie di Attacco

Grazie all'innovazione digitale, la superficie di attacco è cresciuta.

La mancanza di visibilità e controllo sui dispositivi non gestiti connessi alla rete aumenta il rischio.

Compliance to Regulations (NIS2, DORA, GDPR, AI Act, etc)

Thank you!