WHITEPAPER

How to deploy an AI Driven Collaborative Cyber Defence Platform

A Step-by-Step Guide for Financial Services

James Watts - Head of Financial Services and Operational Resilience

The Exponential Growth of Cyber Risk

As assets progress through their lifecycle the Information and Communications Technology (ICT) estate accumulates vulnerabilities. Limited asset visibility, manual processes, poor security hygiene, siloed data and time all contribute to cyber risk exposure. With this time the bad actors accumulate a rich array of assets to exploit, their dark web traded cyber arsenal grows, the Financial Institution (FI) cyber attack surface expands and Financial Services (FS) market systemic risk amplifies.

Armis' micro FI and macro FS view of the financial industry, combined with the world's largest cloud defensive Artificial Intelligence (AI) provides insight of global asset cyber risk. This allows FIs and the Bank of England (BoE) to identify weak spots in their business operations, strategy, and defense mechanisms and do so before a vulnerability becomes a cyber event.

By collaborating and combining data at scale, with the benefit of AI driven processes and the computing power of the cloud, this allows an industry to build global data models of market exposure, identifying new vulnerabilities and threat vectors as they form whilst automating FI data and response in real time. An attack on one becomes an attack on all.

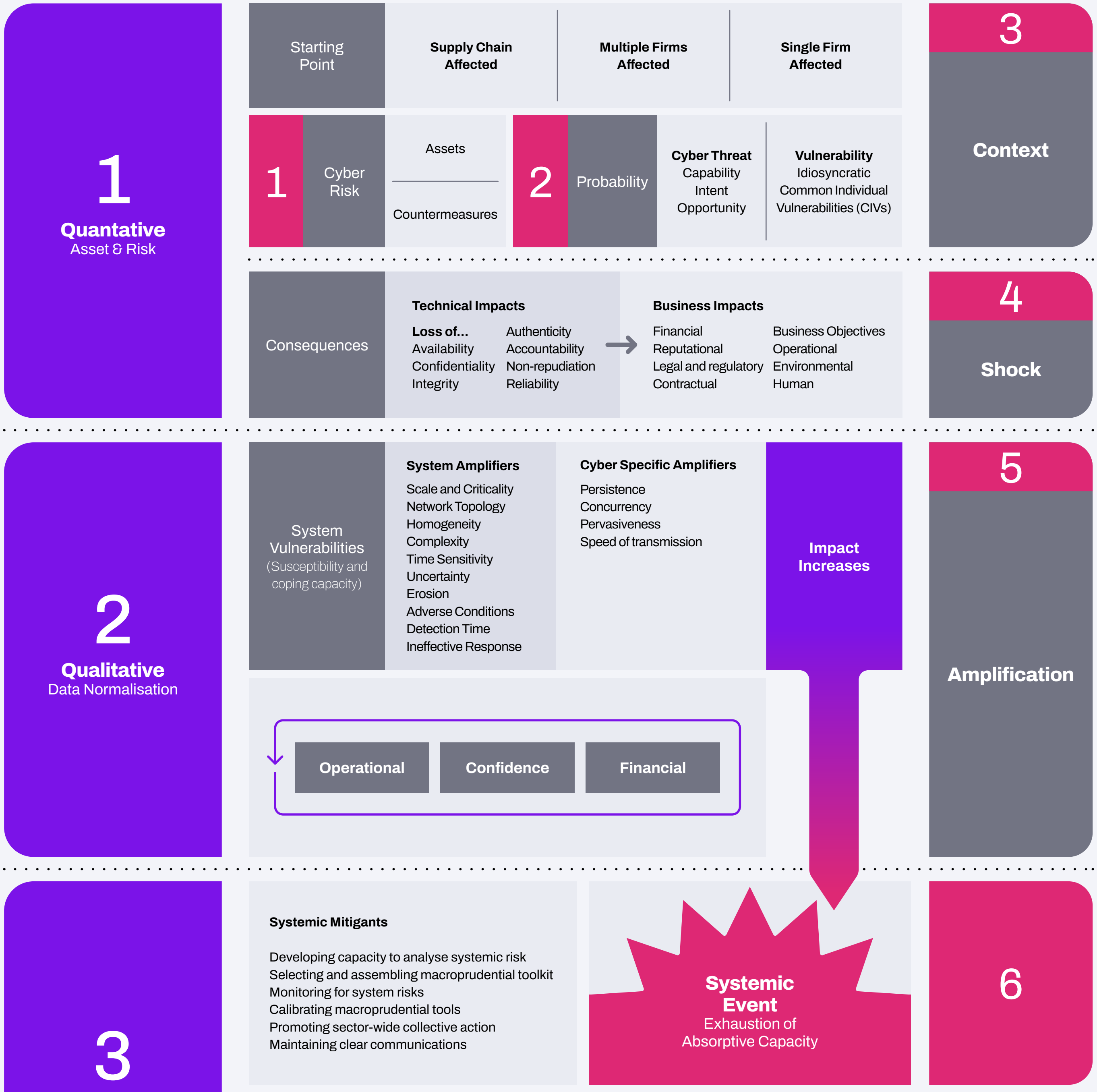
Defensive AI offers a transformative capability for the FS risk ecosystem, moving FIs from on-premise and manual to cloud and automated processes, from policy conflict to centralized control, from asset lifecycle mismanagement to security hygiene, and from data silos and voids to real-time visibility.

A collaborative cyber defense platform offers both a current and a real world capability to transform the FS risk ecosystem. Placing AI in a global, collaborative data cloud will migrate FIs from a reactive, after-the-incident cyber defense to a proactive "lean-forward-posture". Armis Centrix™ identifies anomalies and vulnerabilities, then continuously monitors the estate as FI risk exposure grows, providing the FI and the FS regulator with forewarning to prepare their cyber, regulatory and policy defenses. Participants can identify risk when it's identified in the collaborative cloud and before the cyber event, not after it's behind your firewall and the cyber payload is deployed.

Utilizing AI to Deliver Cyber Resilience and DORA Compliance

A collaborative platform must meet the needs of several key stakeholders spanning banks, financial institutions, critical third party partners, central banks and regulatory bodies. The scoping, building and management of the platform requires a considered approach, careful planning, a scalable infrastructure, strong collaboration, incorporation of legal and compliance frameworks, advanced AI capabilities and of course data.

Breakdown of Systemic Cyber Attack Event



1 **Quantative** Asset & Risk

Starting Point | **Supply Chain Affected** | **Multiple Firms Affected** | **Single Firm Affected**

1 Cyber Risk: Assets / Countermeasures

2 Probability: **Cyber Threat** Capability, Intent, Opportunity | **Vulnerability** Idiosyncratic, Common Individual Vulnerabilities (CIVs)

3 **Context**

Consequences

Technical Impacts

Loss of... Availability, Confidentiality, Integrity, Authenticity, Accountability, Non-repudiation, Reliability

→

Business Impacts

Financial, Reputational, Legal and regulatory, Contractual, Business Objectives, Operational, Environmental, Human

4 **Shock**

2 **Qualitative** Data Normalisation

System Vulnerabilities (Susceptibility and coping capacity)

System Amplifiers

Scale and Criticality
Network Topology
Homogeneity
Complexity
Time Sensitivity
Uncertainty
Erosion
Adverse Conditions
Detection Time
Ineffective Response

Cyber Specific Amplifiers

Persistence
Concurrency
Pervasiveness
Speed of transmission

Impact Increases

5 **Amplification**

Operational | **Confidence** | **Financial**

3 **AI & Automation** Proactive Posture & Collaboration

Systemic Mitigants

Developing capacity to analyse systemic risk
Selecting and assembling macroprudential toolkit
Monitoring for system risks
Calibrating macroprudential tools
Promoting sector-wide collective action
Maintaining clear communications

Systemic Event Exhaustion of Absorptive Capacity

6

7 **AI**

National Risk Register (NRR) 2023

AI officially classed as a security threat to the UK for the first time.
AI classed as a "chronic risk".
AI technology could pose a significant security threat if it were used to launch a cyberattack against the UK.
The NRR places the risk of such an attack at 25%.

> "A delayed reaction while cyber attackers have already begun stealing, compromising or destroying assets is simply not acceptable."
>
> 1.2.1 CBEST Intelligence-Led Testing. Understanding Cyber Threat Intelligence Operations. The Bank of England

The Cyber Exposure Management Platform Toolkit

1 The 8 Foundations of Cyber Resilience

The Cyber Exposure Management Platform technical features should include Cyber Assessment Frameworks for FI & Systemic Risk Management. The platform should include discovery, management and reporting capabilities for each of the "8 Foundations of Cyber Resilience".

In order to combat the rising threat of traditional cyber and AI driven attacks, it is imperative that a robust technology design is in place that can continue to outlearn and defend against weaponized AI. An effective AI driven Cyber Exposure Management Platform must deliver the following:

1. Asset: All Assets relevant to the secure operation of Important Business Services (IBS) are identified and inventoried. The asset data should be gathered via:

- API: Utilize existing IT investments to identify "managed assets". Cut through the noise by correlating data from hundreds of tools including endpoint security solutions, vulnerability scanners, SaaS applications, asset inventory solutions like CMDB and more.
- Scanning
- Non-intrusive Telemetry Data: A combination of agentless, passive and active techniques of collecting data and mapping out the connections and communications between various assets and services in the environment.
- Continuous Monitoring: In perpetuity with automated inventory and data updates.

2. Risk: Assets are prioritized according to their importance to the operation of the Important Business Services (IBS) and operational resilience regulated services. Contextual intelligence allows IT and Security teams to prioritize remediation efforts based on threats, risks and criticality.

3. Context: Associated data and dependencies on supporting infrastructure (e.g. network, power, cooling etc) are recognised, recorded and built into centralized security policies.

4. Service: Connections and dependencies are mapped between assets, partners and IBS.

5. Automation: Data supporting the IBS is automated and real time where possible.

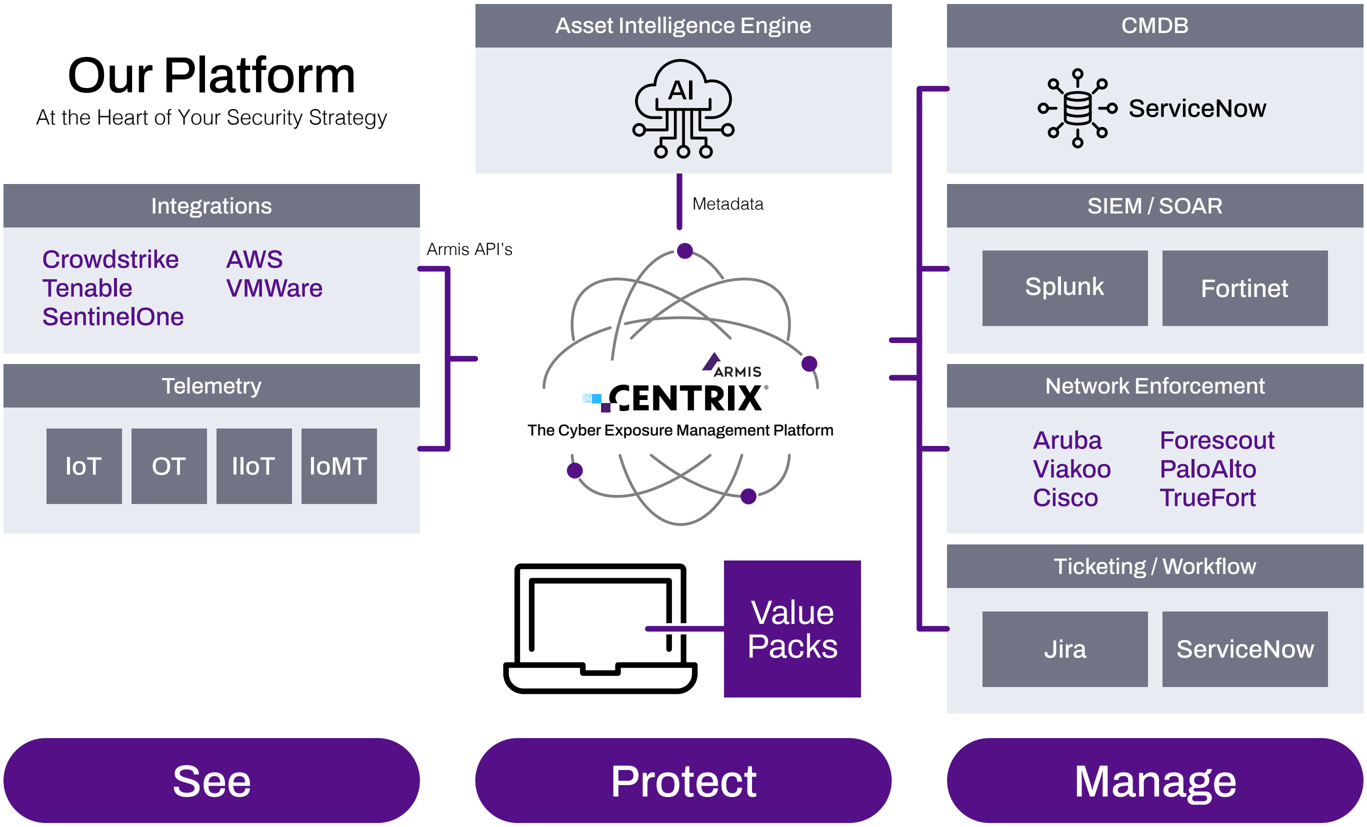
6. Data Normalisation: Data is aggregated, deduplicated and normalized; both for the utilization of the platform and also to feed cleansed and high accuracy data to third party enterprise and cyber applications such as CMDB, SIEM, NAC, Firewall etc.

7. Asset Lifecycle Management: Assets relevant to essential functions are managed with cyber security in mind throughout their lifecycle; from creation, visibility and management through to eventual decommissioning or disposal. Effective life cycle management ensures that assets are up to date, compliant with regulations, and in line with evolving business needs. It also prevents the use of outdated or unsupported assets that could introduce vulnerabilities to the estate.

8. AI: The AI is cloud-based to:

- **Scale:** Provide the unlimited capacity and computing power of cloud Software as a Service (SaaS)
- **Train:** Perpetually leverage global “big data” and the competitive “machine learning” advantage that this AI training dataset provides
- **Collaborate:** Use a collective global cyber defense platform that spans 20% of the internet and 40% of the Fortune 100.
- **See:** “Distributed AI” monitoring of the global 3.5BN asset estate
- **Protect:** Automate cyber detection and collaboration, an attack on one is an attack on all.
- **Manage:** Deliver enterprise wide policies, reporting and compliance

This high level AI driven Cyber Exposure Management Platform design is shown below:



Armis Centrix™ is not a point solution, but sits at the heart of the exposure management process:

The platform receives and interprets intelligence through Integrations, Telemetry Data and our AI-driven Asset Intelligence Engine.

Our SaaS console protects the asset attack surface through easy-to-deploy Value Packs, with out-of-the-box recommendations on integrations, dashboards, reports, and policies for common use cases. And because we see what's happening on the network, we are able to detect and stop threats with great accuracy. We integrate with the tools you already have and feed 3rd party threat intelligence services to deliver end-to-end workflows. This includes enriching CMDB and SIEM, or remediation actions through network enforcement and ticketing tools.

2 Data and Reporting

A global data set plus effective AI design provides both a competitive defensive AI and a perpetual high quality real time data source to report upon. Though it is essential to build the appropriate data driven services upon the Cyber Exposure Management Platform, namely:

Technical Capabilities - FI Reporting and Alerting

Real-time Monitoring & Alerting: Implement continuous monitoring of application telemetry, network traffic, system logs, and user activities. Set up "automated alerts" for potential security incidents and "expedited alerts" for security incidents that may impact on critical, IBS and OpRes regulated services. These alerts can be configured to automatically route to the correct operator/s or pass into third party applications such as a CMDB, Firewall or Network Access Control.

Automated Incident Response: Design automated response mechanisms to mitigate threats in real-time. This may include simple alerting or where appropriate isolating and segmenting affected systems, blocking malicious traffic, and initiating incident response procedures.

Incident Reporting & Escalation: Define clear procedures for reporting incidents to relevant parties within the cyber defense consortium, as well as to regulatory authorities when necessary.

Encryption & Data Protection: Implement strong encryption protocols to protect sensitive data both in transit & at rest, both between platform peers and the regulator.

Technical Capabilities - Regulator Reporting, Alerting, Audit and Review

The core Cyber Exposure Management Platform audit features should include:

Regulatory Compliance Mapping & Reporting: Automated tracking of compliance requirements and compliance gap analysis to identify cyber and regulatory risk posture. This will include real time reports for incident, peer and audit purposes.

Regular Audits & Compliance Checks: Preconfigured OpRes policy frameworks to verify compliance against multi jurisdictional regulations and industry best practices.

Reporting & Communication: Secure dashboard on the cyber and compliance risk posture for both the host and the market, to allow the FI and Regulator to assess the security & compliance posture at both the asset risk and FS market systemic risk level.

Continuous Improvement and Threat Intelligence Feeds: Centrally administered updates and threat intelligence feeds with regular and automated security assessments to identify risk and alert to new vulnerabilities.

3 Collaboration

As we see in the paper “Data as a Defence (DaaD) - Big Data and AI: Delivering Systemic Cyber Resilience”, your adversary is online and your FS competitor is now your cyber peer. Where a lack of visibility exists within an ICT network, amongst FIs and between the regulators; this is risk that a bad actor will exploit and a weaponized AI amplify. Through FIs working together, sharing threat intelligence, resources and data, FS can build a market wide collective cyber defense. Each member acts as part of a unified resilient system vs stand alone independent entities that propagate systemic risk. This need to collaborate permeates the defense; from data and design to operation and maintenance.

Needs Assessment & Working Group:

A market Cyber Exposure Management Platform starts with a need to understand the specific demands, challenges, and regulatory requirements of regulated entities and regulatory bodies in the context of cybersecurity and operational resilience. The platform provider will work with UK Finance (UKF), who in turn will engage the Bank of England (BoE), Prudential Regulatory Authority (PRA) and Financial Conduct Authority (FCA) to identify the relevant stakeholders, market audit data, needs and risk priorities. This work will be completed via a series of events coordinated in conjunction with UKF, their members, partners and technical and policy domain experts.

Regulatory Engagement:

As the Cyber Exposure Management Platform maintains a competitive edge via a perpetual stream of global cyber data, so too should there be a regular engagement with representative regulatory bodies like the UKF on behalf of the Bank of England, PRA & FCA. This being to ensure alignment with their guidelines, incorporation of standards and policies and to seek feedback on platform improvements.

Whilst the platform will be UK led, the relevant regulations will include UK Operational Resilience, but also the EU Digital Operational Resilience Act (DORA) and Network and Information Security 2 Directive (NIS-2) amongst others. This is because London is a global financial market, and FIs must therefore operate across regulatory borders and jurisdictions. It is not uncommon to find a FI's EU DORA cyber risk & legal compliance team are based in the UK. Hence all of the required regulatory policy & compliance models will be incorporated into the platform.

Executive Team and Board Engagement and Prioritisation:

Business and systemic resilience is directly proportional to the priority placed on cyber and regulatory risk by the Executive Team, Board and the "Accountable Executives". A FI management team with a prioritized view of weaponized AI risk will provide both stronger defenses and more complete incident response, reporting, remediation and regulatory compliance.

3 Orchestrate and Deploy at Scale

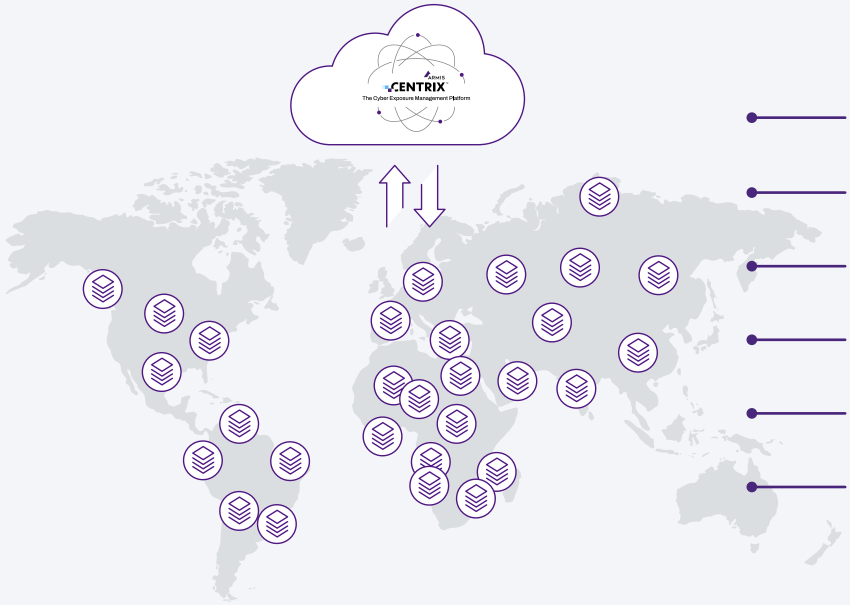
AI and Machine Learning (ML)

It's empirically clear that AI and ML will be the industry standard tooling for threat detection, systemic risk monitoring and real time automated response. Weaponized AI will have the capability to download publicly available product libraries, their historical vulnerability logs and the associated dark web sourced cyber weaponry in order to deploy their payload. A weaponized AI will complete this process in less time than it took you to read this sentence. Hence this amorphous, automated and real time AI adversary will necessitate the move from brittle, manual, moment in time xls driven data to resilient, automated, real time, defensive AI response. We've entered a new epoch in the era of cyber, when cyber & AI fuse the world will see both a new weapon and the commencement of a new cyber arms race.

> "When it comes to cybersecurity, fight fire with fire"
>
> https://www.ibm.com/thought-leadership/institute-business-value/en-us/report/ceo-generative-ai/cybersecurity

Cloud Scalable Infrastructure:

Global, multinational companies are utilizing both the cloud plus standardization & platforming of core ICT systems in order to drive efficiencies, centralize control and access data in real time. As stated previously, when seeking to build an industry wide Cyber Exposure Management Platform of this kind, it is essential to develop a robust & scalable technical infrastructure capable of handling billions of assets to train the defensive AI. The only viable solution for both this scale of data and associated AI computing power is the cloud. The cloud providing global scale collaborative platform capabilities with the necessary on demand Software as a Service (SaaS) to meet OpRes compliance deadlines.



- **Global Coverage**: 100K+ deployments 165 countries
- Handles **500 billion** events daily
- Tracks more than **4 billion** assets
- Stops **500,000 attacks** a month
- Contains rich context for **850 million** vulnerabilities
- Performs **5 million** security decisions daily

Armis operates the largest Cloud device security platform in the world, at over 4BN devices representing 20% of all online devices, having signed 40% of the Fortune 100 as customers in just 5.5 years. As a cloud solution, Armis can deliver at speed and scale.

To quote one customer:

> "When I was asked how long it took to deploy Armis; we didn't have Armis on the Thursday, but we had it on the Friday".

As well as deploy in a day instances; Armis has delivered its Cyber Exposure Management Platform to a European multinational company with 150 sites in 6 weeks, and a US retailer with 5,000 locations and 6 million network assets in 8 months.

Conclusion

The cyber exposure management platform is a solution that pays dividends at scale. The provision of real time dashboards and data gives the enterprise control, protects the FI from cyber risk, strengthens relationships with cyber peers, enables regulatory compliance, positions the FI as an OpRes lead vs laggard whilst protecting executives from corporate & personal fines, penalties & criminal charges.

Data plus AI delivers **FI resilience**.
Data plus collaboration delivers **FS systemic resilience**.

Armis is the leading unified asset intelligence and security platform designed to address the new threat landscape that connected devices create.

Our customers trust our real-time and continuous protection to see with full context all managed, unmanaged, and IoT devices, including medical devices (IoMT), operational technology (OT) and industrial control systems (ICS).

Armis provides passive and unparalleled cybersecurity asset management, risk management, and automated enforcement.

Armis is a privately held company and headquartered in California.

1.888.452.4011

Website
Platform
Industries
Solutions
Resources
Blog

Try Armis
Demo
Free Trial