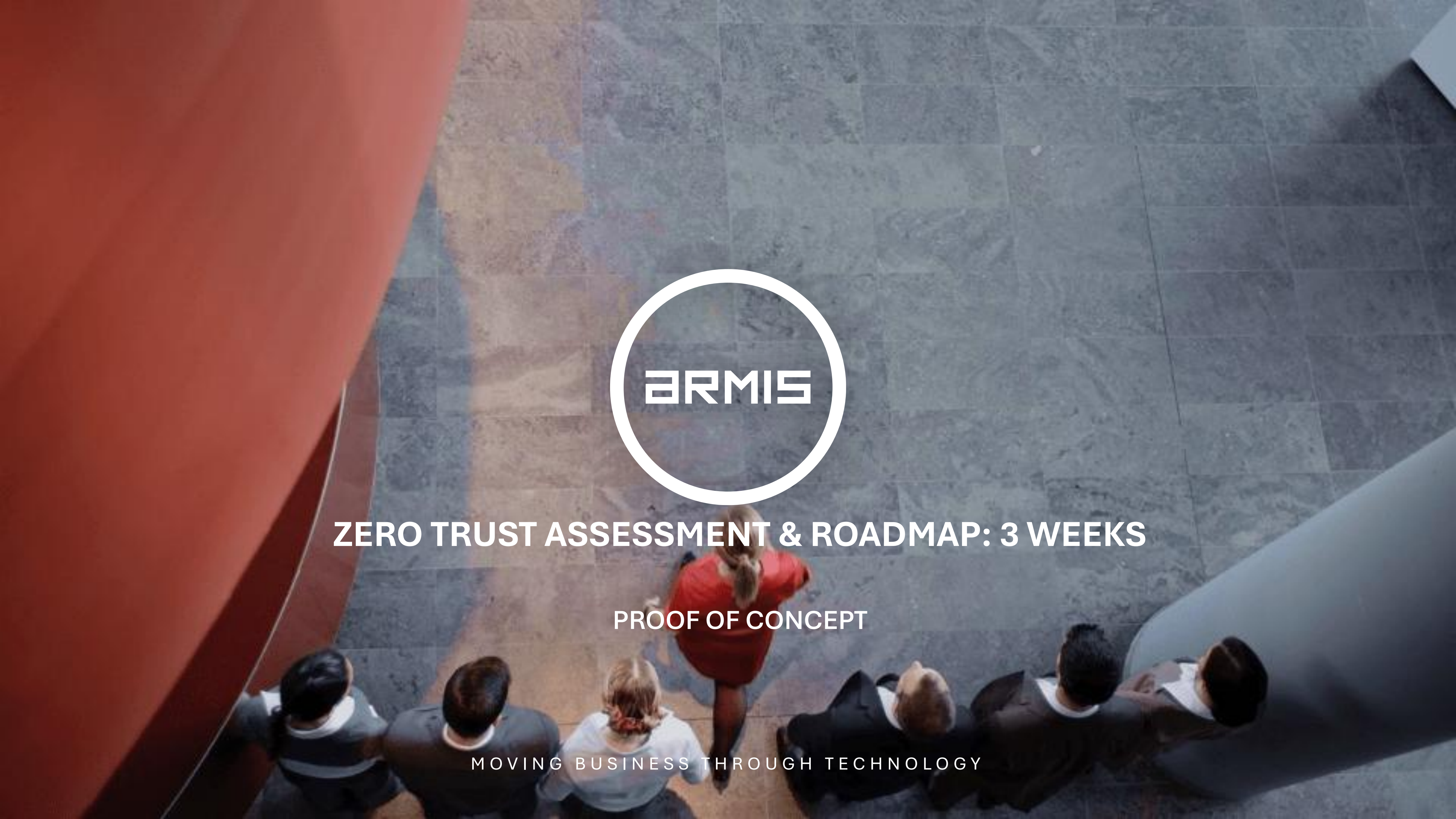


ARMIS

ZERO TRUST ASSESSMENT & ROADMAP: 3 WEEKS

PROOF OF CONCEPT

MOVING BUSINESS THROUGH TECHNOLOGY

PROPOSED SERVICES

WHY ORGANIZATIONS SHOULD DO A ZERO TRUST ASSESSMENT

Today's cyber security landscape is constantly evolving, with increasingly sophisticated threats and the move to hybrid and cloud environments complicating access management. Traditional security approaches, which rely on a fixed perimeter, have become insufficient to protect sensitive data and critical assets. In this context, the Zero Trust model has emerged as a key strategy to ensure that all identities, devices and networks are continuously verified, regardless of their location.

Carrying out a Zero Trust Assessment allows organizations to identify vulnerabilities and define a clear path for implementing this model, in line with security best practices. The assessment provides a detailed analysis of the current state of the IT infrastructure, helping the organization to strengthen its defenses against internal and external threats.

- **Identifying Security Gaps:** The assessment helps to map the current IT infrastructure, identifying security gaps and risk areas that need to be addressed before implementing Zero Trust. This includes analyzing access control, authentication and network segmentation policies.
- **Strict Access Control:** One of the pillars of Zero Trust is to ensure that only authenticated and authorized users and devices can access the organization's critical resources. This includes implementing multi-factor authentication and applying least privilege policies to minimize the risk of unauthorized access.
- **Increased Compliance and Auditing:** Implementing Zero Trust helps ensure that the organization complies with regulations such as GDPR, HIPAA or ISO 27001 by providing granular access control and complete audit logs.
- **Reduced Attack Surface:** With Zero Trust, each access request is treated as a potential risk, which significantly reduces the attack surface. Network segmentation and constant verification of devices and identities prevent attackers from moving laterally within the network.

PROPOSED SERVICES

ZERO TRUST BENEFITS

Implementing a Zero Trust model offers a robust and modern approach to cyber security, helping organizations to meet the challenges of today's digital landscape. By adopting this model, companies can not only better protect their critical assets and sensitive data but also ensure greater resilience against external and internal threats. Zero Trust provides a range of benefits, from improved security to increased regulatory compliance.

Secure Access: Only authenticated users and devices can access, with multi-factor authentication and continuous verification.

Less Unauthorized Access: Least privilege and segmentation policies limit risk, even in the event of an intrusion.

Reduction of Internal Threats: Monitoring and control to restrict access and activities of privileged users.

Scalable security: The model adapts to the organization's growth and new needs, such as the cloud.

Data Protection: Strict controls restrict access to and movement of sensitive information.

Quick Response: Enables faster mitigation and containment of security incidents.

Compliance Guaranteed: Ensures rigorous auditing of accesses, facilitating compliance with GDPR and ISO 27001.

Greater Visibility: Continuous monitoring of networks, devices and users makes it easier to detect risks.

PROPOSED SERVICES

ZERO TRUST ASSESSMENT - WHAT WE WILL COVER

The assessment we will be carrying out will focus on three fundamental pillars that guarantee a comprehensive and effective approach to security:

IDENTITIES:

Identity assessment is crucial to ensure that each access is robustly verified and authenticated. Implementing MFA and conditional access policies helps prevent unauthorized access, while monitoring behavior allows for early detection of anomalous activity, reducing the risk of compromise.

- **Multifactor Authentication (MFA):** Check that multi-factor authentication is implemented for all users.
- **Conditional Access Policies:** Evaluate the effectiveness of conditional access policies to ensure that only authorized users can access specific resources.
- **Behavior monitoring:** Analyze the continuous monitoring of identity behavior to detect suspicious activity.

PROPOSED SERVICES

ZERO TRUST ASSESSMENT - WHAT WE WILL COVER

DEVICES:

Device evaluation is essential to ensure that all devices accessing the network are secure and compliant. The use of MDM and compliance policies help maintain visibility and control over devices, while integrity checks ensure that only trusted devices can access critical resources.

- **Mobile Device Management (MDM and MAM):** Verify the use of MDM and MAM solutions to monitor and manage devices.
- **Compliance policies:** Evaluate the compliance policies applied to devices accessing the network.
- **Integrity checks:** Analyzing the integrity checks carried out to ensure that only secure devices can access the network.

DATA:

Data evaluation is key to protecting sensitive information from inappropriate sharing and internal risks. Classification and labelling help identify and protect critical data, while encryption ensures that data is secure both in transit and at rest. Access and usage monitoring enables detection and rapid response to possible threats.

- **Data Classification and Labelling:** Verify the implementation of solutions to classify and label data based on its sensitivity..
- **Encryption:** Evaluate the application of encryption to protect data in transit and at rest.
- **Access and Usage Monitoring:** Analyzing continuous monitoring of data access and usage to detect and respond to suspicious activity.

PROPOSED SERVICES

DEFINIÇÃO DO ROADMAP

In this phase, based on the conclusions of the previous stages, the future vision of **Zero Trust security** at the client will be defined, resulting in a structured roadmap geared towards practical implementation. This roadmap will detail the **priority actions, recommended technologies and security controls** needed to strengthen the organization's security posture.

With a focus on centralizing the infrastructure, we will present the tools and processes to adopt to ensure a phased and sustained implementation of the **Zero Trust model**.

This approach will enable the client to **mitigate risks, optimize access management and ensure continuous protection of its critical assets**.

The roadmap will include the definition of the technological architecture, as well as a governance and compliance plan, ensuring that the transition to this model is made in a structured way.

To support this process, our team will hold technical and functional workshops, ensuring that the client's decision-makers have the necessary knowledge to drive this transformation successfully.

APPROACH TO ASSESSMENT

DEFINING THE ROADMAP - APPROACH

The **Zero Trust Assessment and Roadmap** will be conducted over several weeks, following a structured methodology orientated towards phased implementation.

WEEK 1

INITIAL ANALYSIS

- **Initial meetings** with stakeholders to define objectives and requirements.
- **Mapping** of IT infrastructure and workflows.
- **Analysing** current security.
- **Identification** and assessment of risk exposure.

WEEK 2

IDENTIFYING RISKS AND PRIORITISING

- **Assessment** of compliance with Zero Trust principles.
- **Identification** of vulnerabilities and risks.
- **Prioritization** of risk mitigation.

WEEK 3

DEFINING THE ROADMAP

- **Creation** of an implementation plan for the Zero Trust model.
- **Definition** of KPIs to monitor progress.
- **Presenting** the roadmap to stakeholders and collecting feedback.

APPROACH TO ASSESSMENT

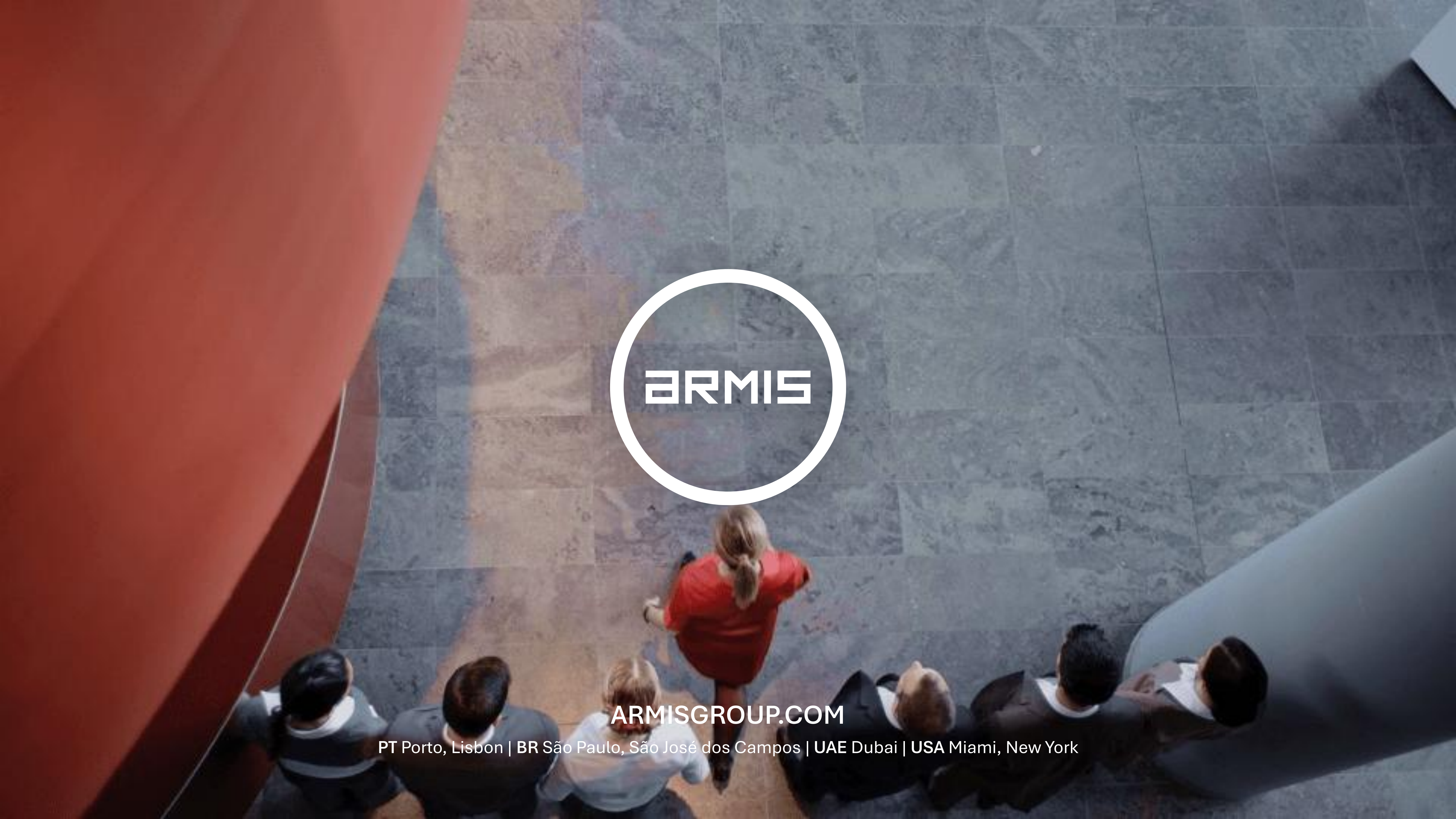
DEFINITION OF THE ROADMAP - DELIVERABLES

The **Zero Trust Assessment and Roadmap** will be conducted over several weeks, following a structured methodology orientated towards phased implementation.

- **Diagnostic report** with an initial assessment of the organization's security posture.
- **Vulnerability List** with potential weak points and areas for improvement in security.

- **Security Assessment Report** analyzing compliance with Zero Trust principles.
- **Risk Matrix** with categorization of threats and impact on the organization.
- **Mitigation Plan** with recommendations for correcting the gaps identified.

- **Implementation roadmap** with phases, priorities and dependencies.
- **Definition of Key Performance Indicators (KPIs)** to monitor the adoption of the Zero Trust model.
- **Detailed Action Plan** with next steps, responsible parties and deadlines.



ARMISGROUP.COM

PT Porto, Lisbon | **BR** São Paulo, São José dos Campos | **UAE** Dubai | **USA** Miami, New York