STRATEGY +
TRANSFORMATION

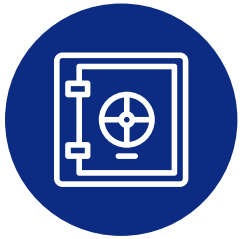
CYBER PROGRAM

November 2024

PEPSICO
LABS

Cyber Security Focus Areas

STRATEGY + TRANSFORMATION

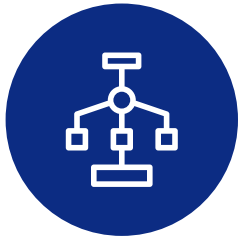


Data Loss Prevention and Data Protection

Tools to help safeguard sensitive information by monitoring, detecting and preventing unauthorized data access and transfer

Zero Trust

Tools that provide continuous, real-time verification and monitoring of users and devices accessing network resources



Incidents Automation

Tools that remove manual work needed to triage security incidents

Risk Quantification and Reporting

Technologies that quantify and report on risks, enabling to take data-driven, proactive decisions using dynamic dashboards

Security Awareness Training for Employees and Developers

Empowering employees and developers to identify, mitigate, and prevent security risks through tailored training solutions

PEPSICO LABS

Cyber Security Focus Areas

STRATEGY + TRANSFORMATION

1. Data Loss Prevention and Data Protection

Tools to help safeguard sensitive information by monitoring, detecting and preventing unauthorized data access and transfer

- **Comprehensive Data Coverage** for both structured and unstructured data across multiple environments
- **Real-time Monitoring and Alerts** on any suspicious activities, potential breaches, policy violations, and contextual awareness
- **Discovery usage of AI models, API calls to public AI models** (i.e., track shadow AI and enforce DLP policies)
- **Robust Encryption, Data Masking and Anonymization** to protect sensitive information in non-production environments and during data sharing
- **User and Entity Behavior Analytics** to identify abnormal behavior patterns
- **Policy Flexibility and Granular Control** to tailor security measures to PEP needs and compliance requirements
- **Real Time Threat detection and Automated response** mechanisms to mitigate risks and contain breaches
- **Ransomware quick recovery and data exfiltration protection** to have near zero downtime to restore data after ransomware attacks and to prevent data leaving PepsiCo

2. Zero Trust

Tools that provide continuous, real-time verification and monitoring of users and devices accessing network resources

- **Continuous monitoring of risk/Identity Verification:** multi-factor authentication and adaptive authentication to ensure that users and devices are continuously verified, dynamically change access of risk scoring, allowing granular access until reconciled.
- **Granular Access controls:** role-based access controls and attribute-based access controls
- **Micro Segmentation:** Segment networks and applications to limit lateral movement and contain potential breaches for pre-Kubernetes and post-Kubernetes workloads on a single platform
- **Real-time Monitoring and Analytics:** logging, and analytics to detect and respond to suspicious activities and potential threats promptly
- **Advanced biometric authentication methods:** Reduce the risk of stolen identity and reduce consumers friction with enhanced user experience (e.g., use of passkeys)
- **Complete zero trust coverage of SBOMs and software supply chain security:** Software Composition Analysis with context and reachability analysis with minimal impact to developers

3. Incidents Automation

Tools that remove manual work needed to triage security incidents

- **Real-time Risk Scoring:** A system that continuously calculates the risk of each incident, only escalating those that require human attention or decision-making
- **Autonomous Alert Investigations:** AI systems that automatically investigates alerts across multiple domains (e.g., phishing, endpoint, cloud, network, insider threats)
- **Autonomous Incident Handling:** AI systems that can automatically handle incidents up to remediation (e.g., stopping malware spread, mitigating attacks, neutralizing ransomware before data is impacted)
- **Self-healing Security:** Automating network infrastructure, allowing systems to reconfigure themselves, patch vulnerabilities, or roll back compromised components without human intervention
- **Predictive AI** to prevent incidents before they materialize
- **Context Knowledge Base:** Tool that maintains a knowledge base that offers contextual information during incident investigation, ensuring analysts have the necessary background to make informed decisions

Cyber Security Focus Areas

STRATEGY + TRANSFORMATION

4. Risk Quantification and Reporting

Technologies that quantify and report on risks, enabling to take data-driven, proactive decisions using dynamic dashboards

- **Comprehensive Risk Landscape Mapping**: Identify and analyze potential risks across various dimensions, providing a clear understanding of PEP's exposures
- **Quantifying and Prioritization of Risks:** evaluate risks across multiple domains (e.g., reputation damage, IP, vulnerabilities, operational disruptions etc.)
- **Simplification of Complex Risk Data:** Transform intricate risk datasets into actionable insights, enabling stakeholders to make informed decisions
- **Interactive and Customizable Dashboards:** real-time monitoring and reporting, dynamic dashboards tailored to specific needs, facilitating real-time monitoring, reporting, and scenario analysis

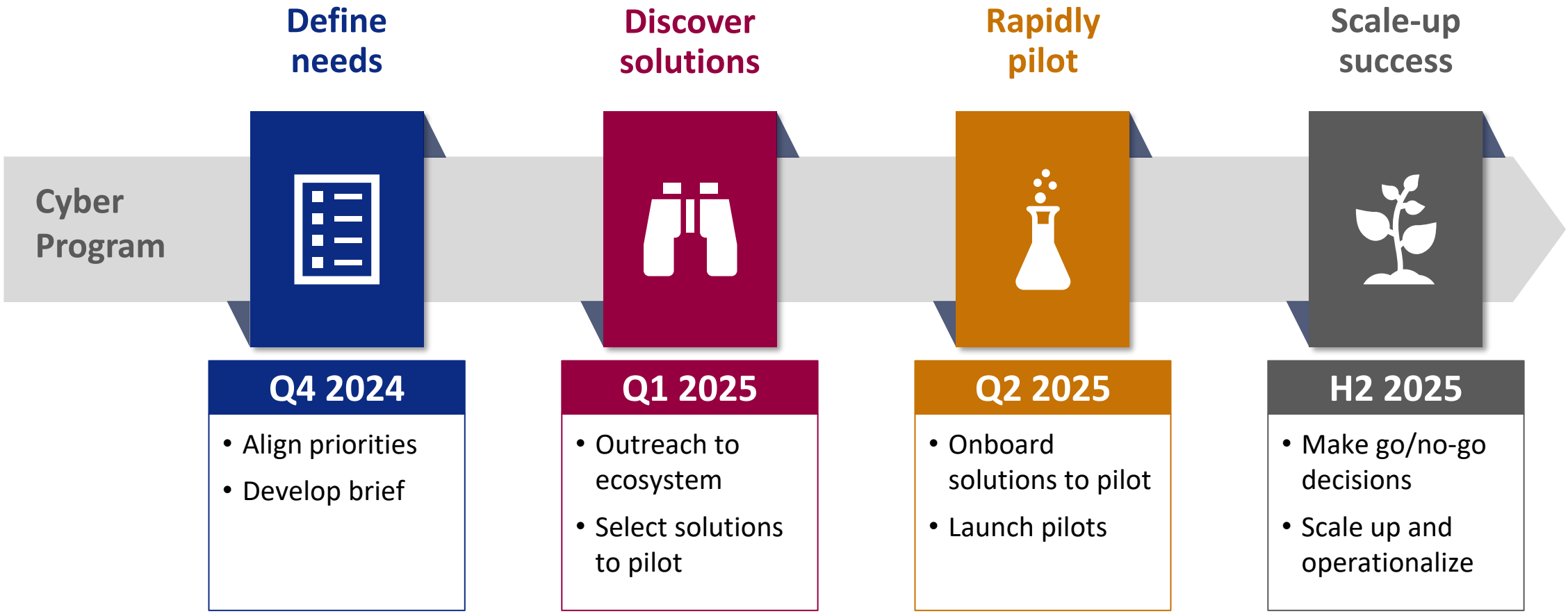
5. Security Awareness Training for Employees and Developers

Empowering employees and developers to identify, mitigate, and prevent security risks through tailored training solutions

- **Customized Security Training Programs and Gamification**: Develop engaging, role-specific training modules designed to address the unique challenges faced by employees and developers in safeguarding organizational assets, by leveraging enjoyable and impactful techniques
- **Hands-On, Scenario-Based Learning**: Utilize real-world simulations and interactive exercises to enhance awareness and practical understanding of security threats.
- **Threat Detection and Mitigation Skills**: Equip employees and developers with the ability to recognize and respond to phishing attempts, social engineering tactics, and potential vulnerabilities in applications
- **Developer-Focused Security Practices**: Tools that can ensure secure coding principles into the software development lifecycle to prevent vulnerabilities and ensure compliance with security standards

Key Phases for Cyber Security Program

STRATEGY + TRANSFORMATION



PEPSICO LABS