ARMIS®

Armis and Cal-Secure Alignment

Introduction

California's status as a global technology hub and the largest U.S. economy underscores the importance of a robust cybersecurity strategy. The increasing reliance on digital infrastructure and the interconnected nature of government and private sector operations necessitated a roadmap that not only addressed current risks but also anticipated future challenges including:

1. **Rising Cyber Threats**
   California, as the largest state economy in the U.S., faces escalating cyber risks targeting its critical infrastructure, public services, and private sector organizations.

2. **Regulatory Compliance**
   Evolving state and federal mandates with focus on reducing legal and operational risks.

3. **Enhanced Resilience**
   Mitigating risks, recover from incidents more effectively, and protect citizens' data and trust.

4. **Cross-Sector Collaboration**
   Fostering partnerships between government, private enterprises, and critical infrastructure sectors to share intelligence and build collective defenses.

Cal-Secure was officially launched in October 2021. It marked California's first comprehensive, multi-year cybersecurity strategy, designed to enhance the state's defenses against evolving cyber threats and establish a framework for proactive risk management and collaboration across public and private sectors. The process began with collaborative efforts among state agencies, private sector experts, and academic institutions to assess vulnerabilities and identify priorities. Insights from these stakeholders, coupled with guidelines from the National Institute of Standards and Technology (NIST) Cybersecurity Framework, shaped the foundational structure of Cal-Secure.

ARMIS®

People, Process, and Technology

It takes people, agencies, and vendor community collaboration with the government to deliver critical services to Californians in the most efficient and equitable method possible. This is why People, Process, and Technology comprise the three strategic categories CDT outlines in the Cal-Secure roadmap.

People – CDT Defined Initiatives

Cybersecurity is a shared responsibility, and having skilled professionals is crucial to defending against sophisticated threats. Cal-Secure emphasizes workforce development, cybersecurity awareness, and fostering a culture of vigilance to mitigate risks stemming from human error.

- Develop pipelines for cybersecurity professionals
- Align cybersecurity roles with the National Initiative for Cybersecurity Education (NICE) framework
- Create a cybersecurity career path toolkit
- Expand tailored workshops for the state cybersecurity workforce
- Promote innovative programs for cybersecurity skills and leadership development

Armis Alignment to People Defined Initiatives

- Armis provides a platform for security professionals to develop knowledge, capability, and experience within the cyber-security industry
- Armis can supplement top cybersecurity talent while CDT builds out a security workforce
- Armis can assist with workshops for expanding cybersecurity and network skills

Process – CDT Defined Initiatives

Standardized, repeatable processes are essential for managing risks, ensuring regulatory compliance, and responding effectively to incidents. Cal-Secure prioritizes governance, risk management, and incident response planning to create a robust cybersecurity framework.

- Create tools for cybersecurity strategy and roadmap development at state agencies and entities
- Formalize the cybersecurity governance structure
- Transform state information, privacy, and cybersecurity policies and standards
- Modernize cybersecurity procurement
- Create multi-tiered cybersecurity governance bodies

Armis Alignment to Process Defined Initiatives

- Armis Centrix™ supports multi-tiered governance bodies

- Armis Centrix™ can assist CDT in auditing and enforcing policies across different level agencies and entities

- Armis helps agencies transform cybersecurity standards by addressing the extended attack surface from IoT, OT, BOYD assets

Technology – CDT Defined Initiatives

Advanced tools are necessary to defend against today's evolving cyber threats. Cal-Secure stresses the deployment of modern technologies to secure critical assets, detect vulnerabilities, and respond to incidents in real-time

- Create a portfolio of cybersecurity-as-a-service offerings

- Implement the Unified Integrated Risk Management Platform

- Provide all state entities with security operations services

- Define cybersecurity technology requirements through community-led groups

- Integrate cybersecurity platform into the IT modernization roadmap

Armis Alignment to Technology Initiatives

- Armis Centrix™ is a cloud-first platform and a Software as a Service (SaaS) offering

- Armis Centrix™ provides risk scoring for every device with adaptive risk scoring

- Armis Centrix™ is an integrated single source of truth for all assets and risks associated with these assets

- Armis Centrix™ can easily be integrated into CDT's SOC environment and services

Cybersecurity Capabilities

Priority 1	Armis Support Level
Anti-Malware Protection	Supportive
Anti-Phishing Program	Supportive
Multi-Factor Authentication	Not Applicable
Continuous Vulnerability Management	Complete
Priority 2	
Asset Management	Complete
Incident Response	Complete
Continuous Patch Management	Supportive
Privileged Access Management	Supportive
Security and Privacy Awareness Training	Not Applicable
Security Continuous Monitoring 24x7	Complete
Cloud Security Monitoring	Supportive
Priority 3	
Data Loss Prevention	Supportive
Log Management	Supportive
Network Threat Detection	Complete
Network Threat Protection	Supportive
Threat Intelligence Platform	Complete
Application Security	Supportive
Operational Technology Security	Complete
Priority 4	
Disaster Recovery	Supportive
Enterprise Sign-On	Not Applicable
Mobile Device Management	Supportive
Application Development Security	Not Applicable
Application Whitelisting	Supportive
Software Supply Chain Management	Supportive
Priority 5	
Identity Lifecycle Management	Supportive
Insider Threat Detection	Complete
Network Access Control	Supportive
Enterprise Encryption	Not Applicable
Mobile Threat Defense	Not Applicable

Armis supports CDT Required and Recommended capabilities throughout the priority levels 1-5. Armis delivers critical business value that helps agencies achieve CDT's recommended cybersecurity maturity levels with a single, easy-to-deploy, and agentless platform.

Business value includes:

Discover all assets, managed or unmanaged.

Alert on security incidents with SIEM Integrations.

Create and track tickets for completion.

Trigger vulnerability scans automatically.

Enrich existing CMDB, SIEM and SOAR solutions with accurate, rich, and contextual insight.

Enable remediation through existing FW and NAC solutions.

Label devices for a multi-dimensional and logical segmentation.

Prioiritize remediation of vulnerabilities with real-time insight to vulnerabilities, risk, and business impact.

By addressing the **People, Process, and Technology** pillars, Cal-Secure provides a holistic approach to building cyber resilience. Armis aligns with this framework by equipping organizations with the tools, insights, and capabilities to empower teams, streamline processes, and modernize technology, ensuring compliance and strengthening defenses against cyber exposure and threats.
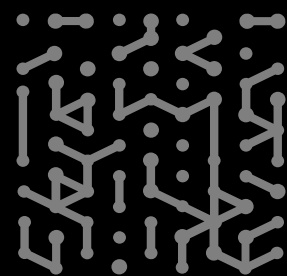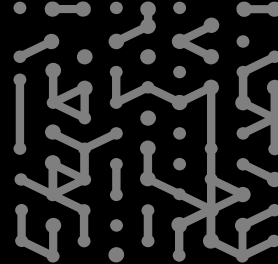
ARMIS.

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