Securing the Enterprise's Software and Data Supply Chain

- **A Unified BISO & CISO Strategy with Risk and Vulnerability Management and AI Labor Agents**

Contact:

bronackt@dcag.com, or bronackt@gmail.com

(917) 673-6992

Executive Summary

- **Digital enterprises must secure their software and data supply chains.**
- **Risk & Vulnerability Management, combined with AI Labor Agents, empowers BISOs and CISOs to safeguard data, reduce costs, and drive compliance.**
- **Post Quantum Cryptography (PQC) protects software and data after quantum computers defeat current encryption.**
- **Audience:** CEO, CIO, CISO, BISO, COO, CFO, DevSecOps, Legal, and Audit.

How the CISO and BISO work together to safeguard and optimize Enterprise Operations

Areas of Organizational Resilience

Today's Security Challenge

- **Expanding attack surfaces across digital supply chains (i.e., Volt & Salt Typhoon viruses)**
- **Additional Risk and Vulnerability protections are required**
- **Regulatory pressure and compliance fatigue, also Post Quantum Cryptography (PQC) migration**
- **Talent shortages in cybersecurity, tool overload, burnout, and turnover**
- **Disconnect between business and IT security objectives between BISO and CISO under CIO**
- **“Left of Boom” proactive protection must be integrated (Shift-Left proactive protection)**

Discovery Project to determine current environment and Future needs

1. Adherence to Resilience Guidelines.
2. Compliance built into everyday functions.
3. Supply Chain and Vulnerability Management.
4. Automated Applications Factory with adjustable Quality Control Gates
5. Quantum Readiness and PQC

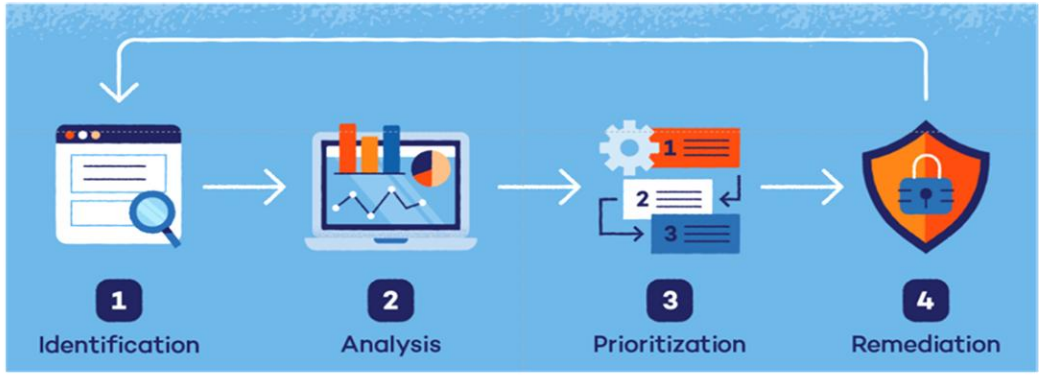
Define Needs

Project Goals:

1. Vulnerability Management Practice understood
2. Tool Assessment and Selection (AoA)
3. Workflow to determine how to use Vulnerability Management Tools
4. Vulnerability-Free Production Environment
5. Compliance to all required laws and regulations
6. Vulnerability Management Maturity Cycle
7. Continuous Threat Exploitation Management
8. Business Continuity Management
9. Awareness and Training.

Create a POA&M

1. Identify your needs and assess your weaknesses, exceptions, and gaps.
2. Define your goals and scope, then conduct an analysis of your environment and workflow.



Define project concept, actions, and deliverables within POA&M

3. Prioritize located weaknesses and develop a Statement of Work (SOW) to resolve issues.
4. Devise a Remediation POA&M, gain approval, formulate team, and commence work.

The Evolving Roles of BISO and CISO

- **CISO Focus:** Governance, compliance, enterprise-wide oversight to protect business products and services
- **BISO Focus:** Operational execution, alignment with business unit goals
- **Overlap:** Shared need for visibility, real-time intelligence, and “Secure-by-Design” adoption
- **Enterprise guidelines:** Standards, and procedures must be published, distributed, and Awareness and Training provided
- **Automation Integration:** AI Agentic RAGS and other workflow automation tools must be evaluated to meet the ongoing

Vulnerability Management & BOMs

Components:

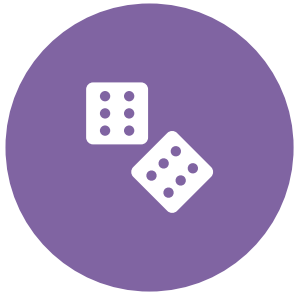
- **SBOM** – Software Bill of Materials
- **RBOM** – Release Bill of Materials
- **CBOM** – Cryptographic analysis for PQC Migration
- **AIBOM** (Ongoing) – AI-generated Behavior Trust Scores
- **Value:** Controls, visibility, and risk insights across development and operations to provide ATO and cATO
- **Knowledge Graph:** Component Relationships and Analysis information

The Role of AI Labor Agents

BOM - Bill of Materials (Software, Release, Crypto. AI, etc.)
CVE – Common Vulnerability Enumeration / Exploitation
CVSS – CVE Security Score (10 is highest)
CWE – Common Weakness Enumeration / Exploitation
VEX – Vulnerability Exploitation eXchange (Context Aware)
EPSS – Exploit Prediction Scoring System (Chance of Exploit)
KVE – Known Vulnerability Exploitation
UEFI – Unified Extensible Firmware Interface exploitation
Secure Boot – Validates System Boot prior to UEFI
Tee – Trusted Execution Environment

Automate SBOM/RBOM analysis and reporting

Monitor CVEs and supply chain activity in real time



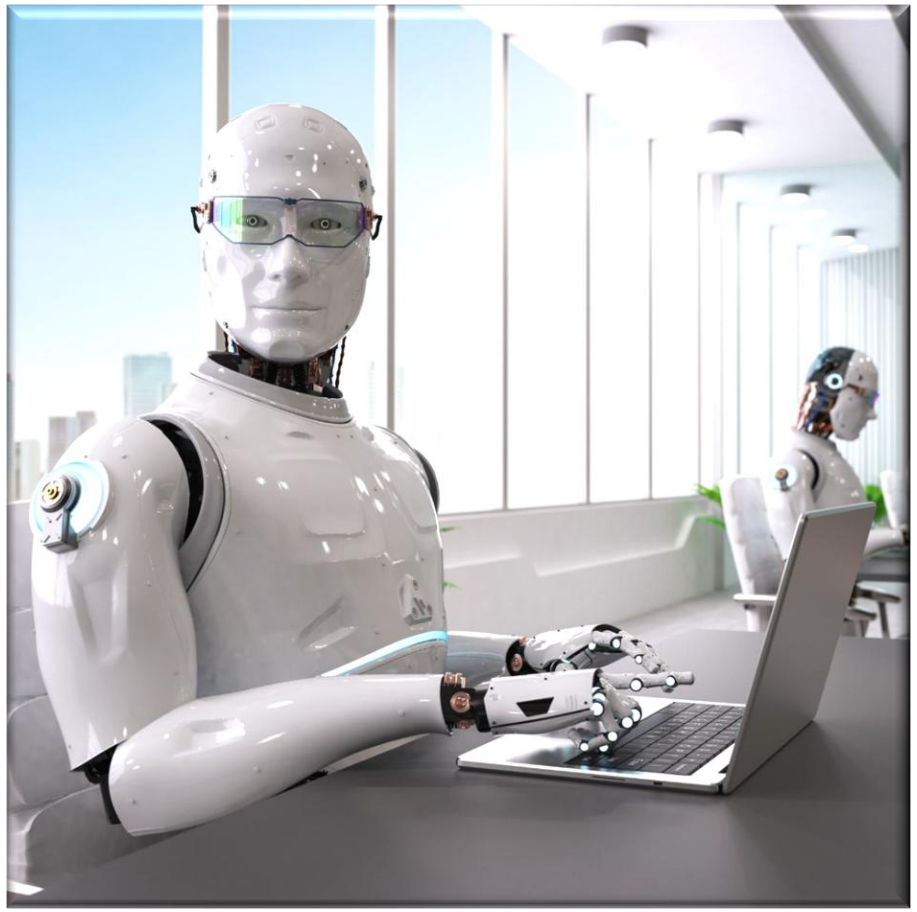
Predict risk using behavioral data (AIBOM)

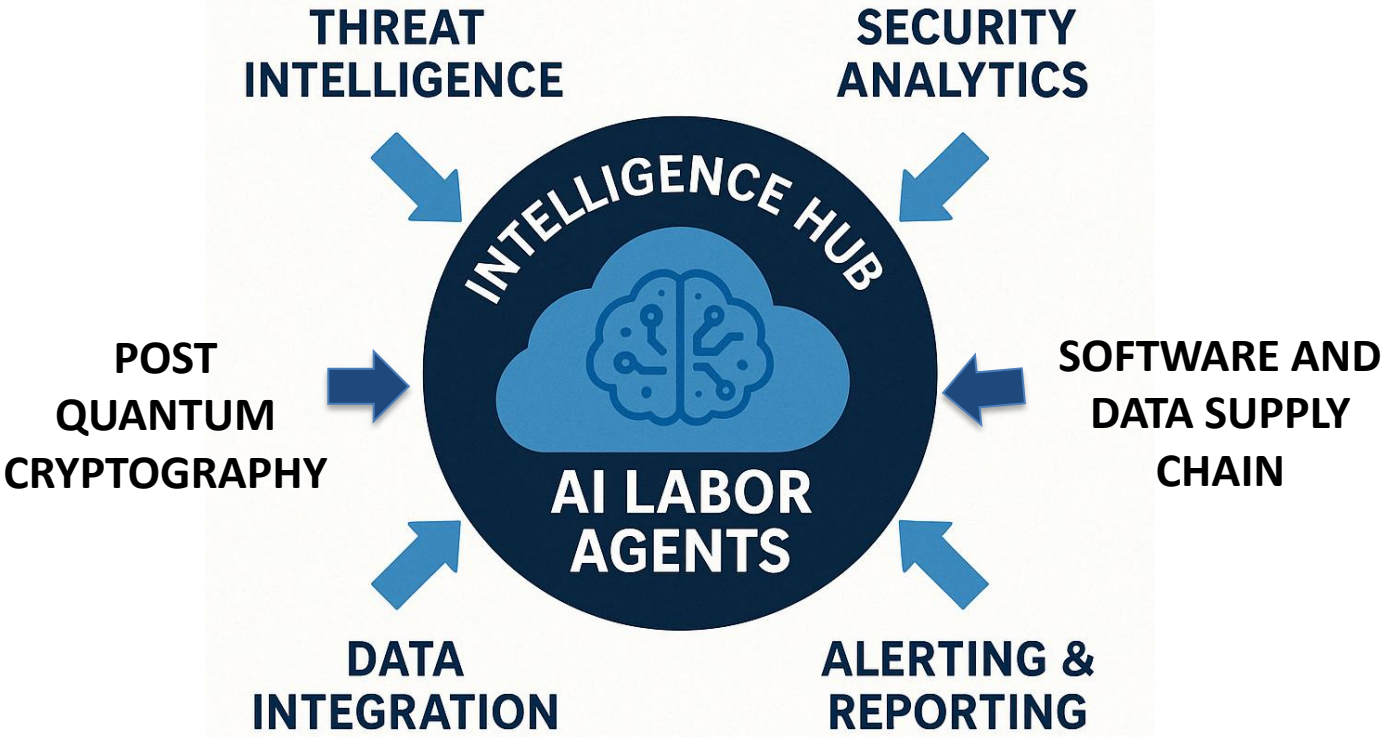
Reduce manual labor and analyst workload

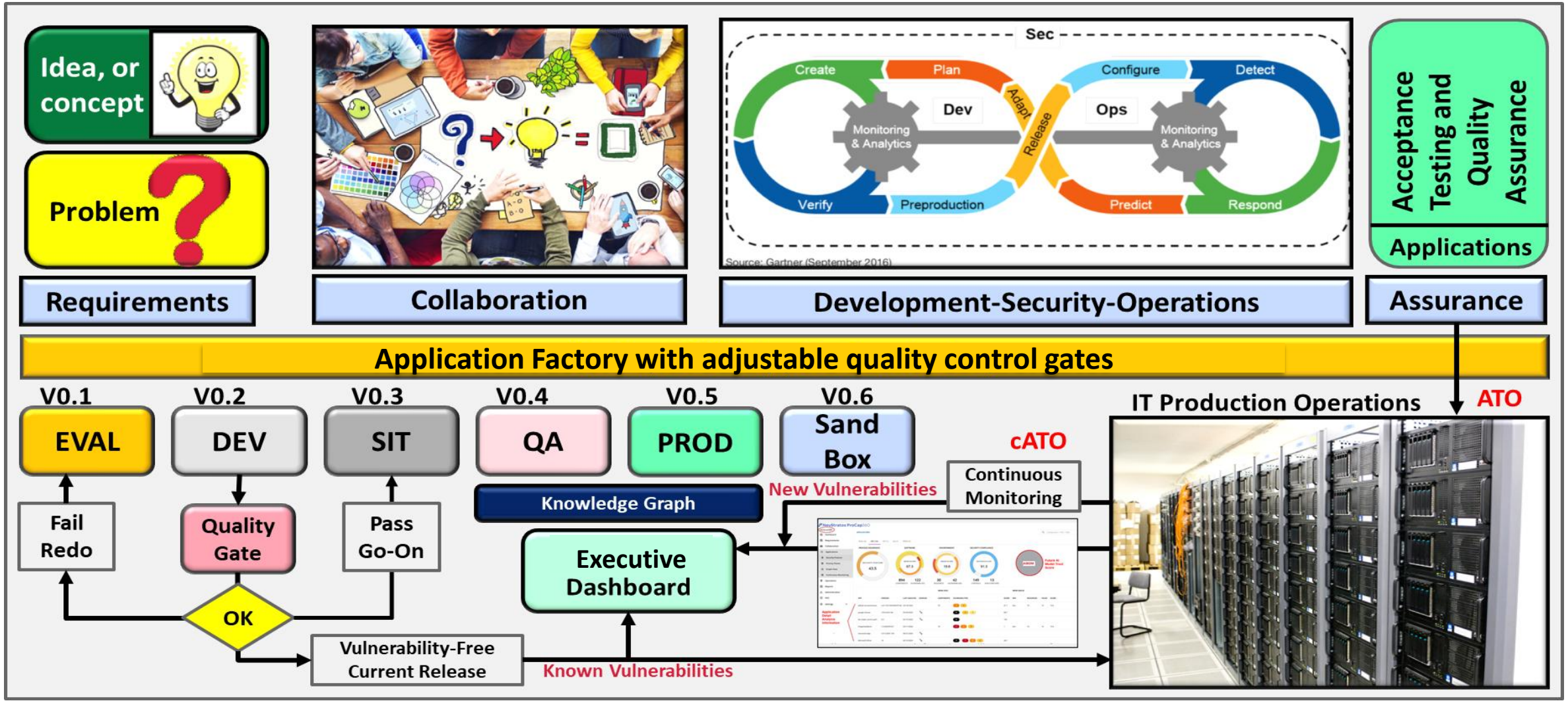
Integration Model = BISO + CISO + AI Agents

1. Identify areas for automation.
2. Obtain agreement and management approval.
3. Create POAM, assemble team, commence work, provide status, mitigate problems, complete on-time and within budget.
4. Monitor efficiency and ROI.

AI Agentic RAG





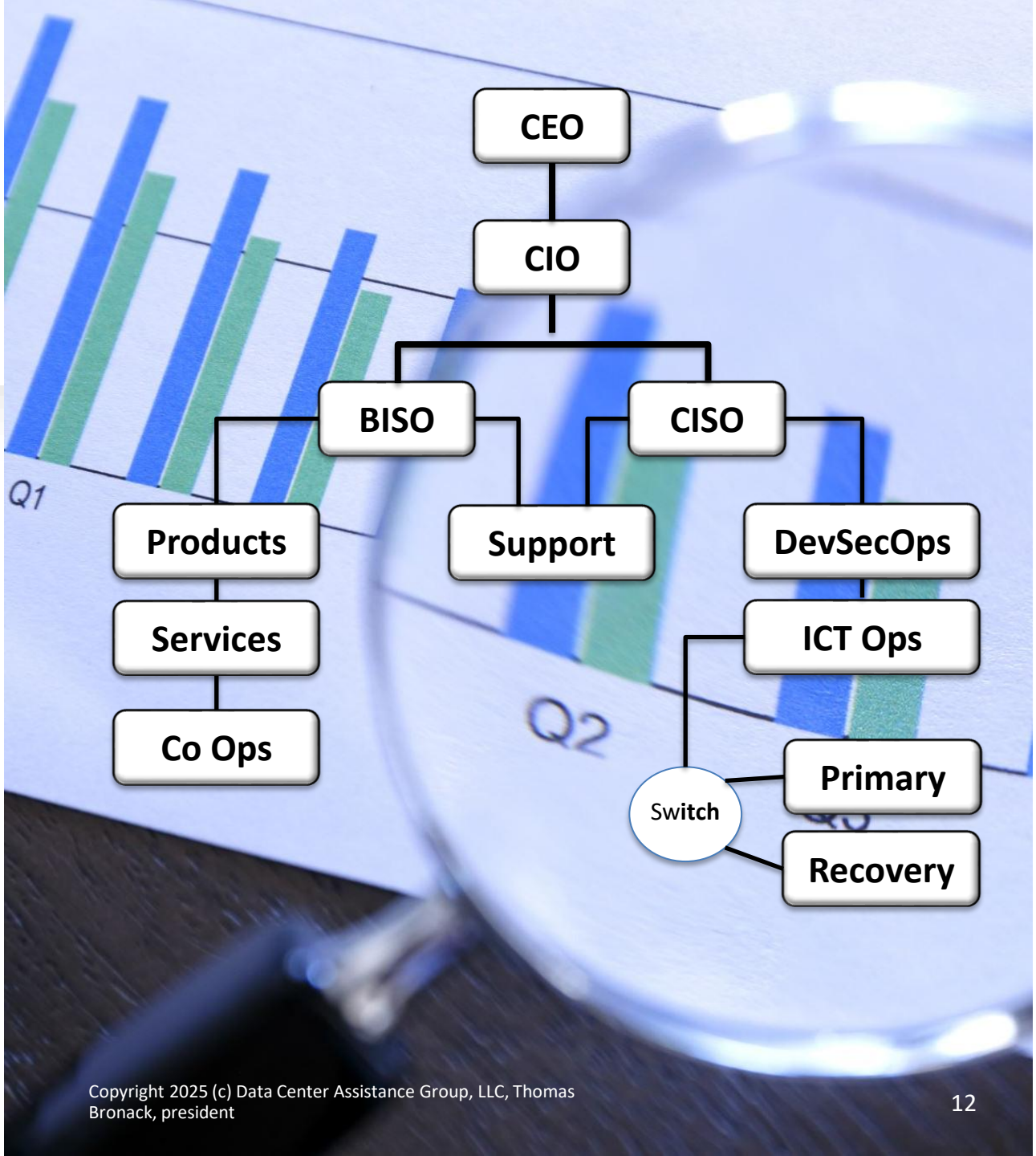


From initial Idea to Final Delivery and Support of Business Applications

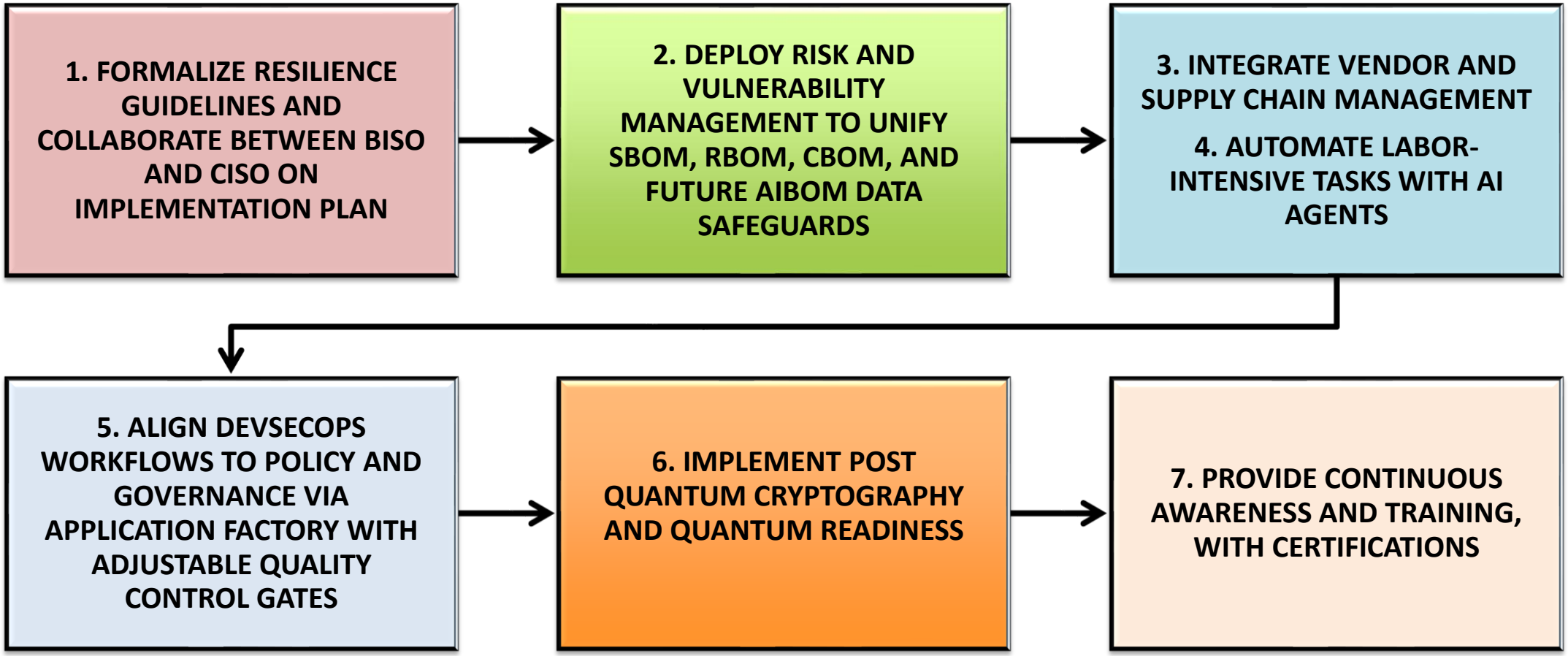
Application Factory with Adjustable Quality Control Gates to ensure components are at current release levels and free of vulnerabilities.

Value by Role

- **CEO:** Brand protection, reduced risk cost, due diligence accomplished.
- **CIO**: Integrated IT & security operations.
- **CISO:** Holistic visibility, faster threat response.
- **BISO:** Secure product development, business unit reporting.
- **DevSecOps:** Frictionless CI/CD integration.

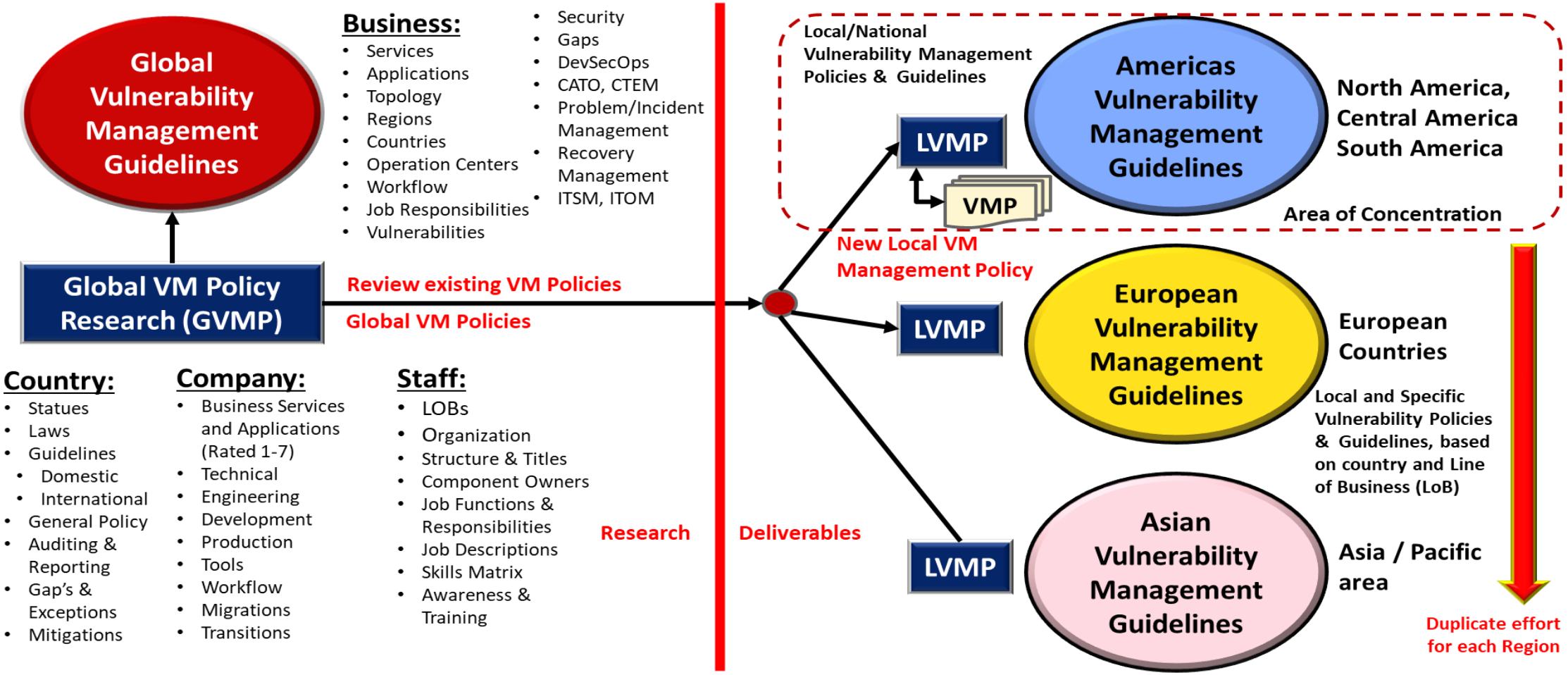


Strategic Recommendations



Enterprise Resilience and Corporate Certification Guidelines

1. Determine Enterprise Resiliency and Corporate Compliance Certification.
2. Standardize Enterprise Guidelines via CISO and have BISO implement in LOB.
3. Coordinate Domestic and International adherence to guidelines.

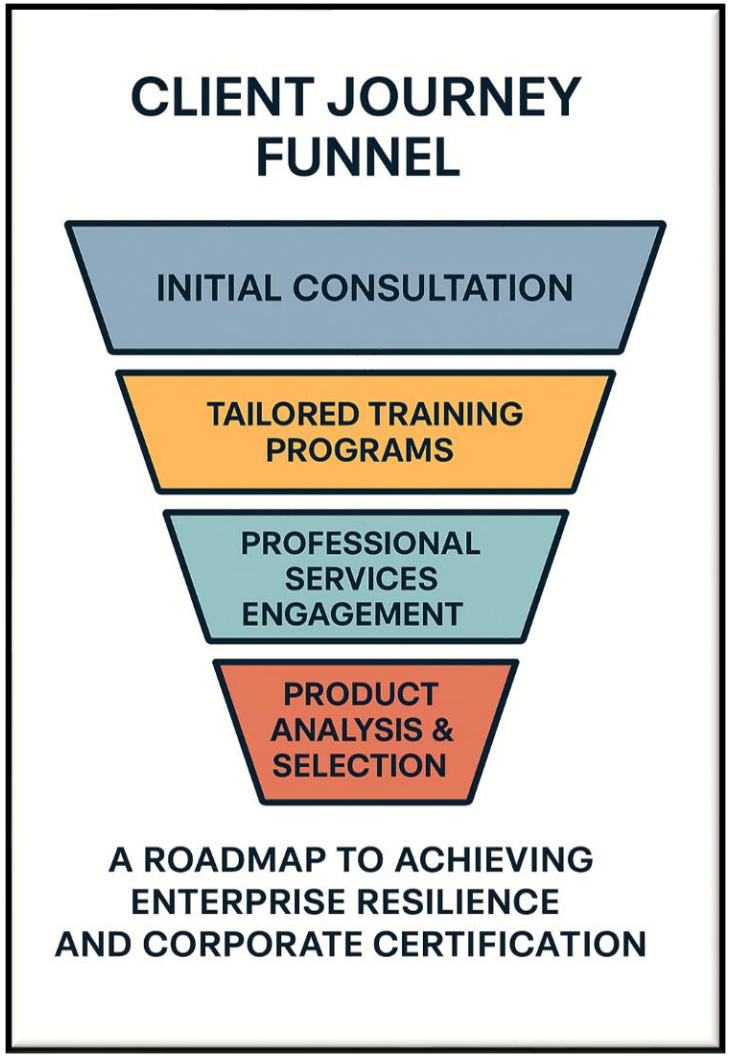


Conclusion & Call to Action

TO STAY AHEAD OF EVOLVING THREATS, ENTERPRISES MUST UNIFY BUSINESS AND CYBERSECURITY LEADERSHIP AROUND A SHARED PLATFORM. VULNERABILITY MANAGEMENT TOOLS WITH AI LABOR AGENTS MAKES THAT FUTURE POSSIBLE—TODAY.

CONTACT US FOR AN EXECUTIVE STRATEGY SESSION.

Services provided by the Data Center Assistance Group



DCAG SERVICES

Business Continuity Management
Ensuring readiness for disruptions to sustain critical operations

Disaster Recovery
Planning for the restoration of IT systems an I data following an incident

Risk Management
Identifying, assessing, and mitigating potential threats

Vulnerability Management
Detecting and addressing weaknessees in systems and software

Operations Management
Optimizing processes for effective and efficient through a structured approach

Systems Development Life Cycle (SDLC)
Guiding the cration and maintenances systems through a structured approach

Production Operations Support (ATO, CATO)
Enabling secure and compliant systems deployment and operation

Software Supply Chain Management (SBOM)
Managing the integrity of software components. and their dependencies

Corporate Certification
Achieving standards and certifications for organizational excellence

Helping organizations enhance resilience, manage risk, and maintain compliance

Additional Services

Protecting against the Volt and Salt Typhoon Cyber Attacks

Providing Post Quantum Cryptography Migration

Integrating Business Information Security Officer (BISO) function within CIO structure

Providing Enterprise-wide Risk and Vulnerability Guidelines and Procedures Documentation, Awareness, and Training

Contact Information

Data Center Assistance Group, LLC

- bronackt@dcag.com
- bronackt@gmail.com
- (917) 673-6992