Cyber Defense of the Supply Chain

Meghan Good | VP, Director of the Cyber Accelerator

Supply Chain in Action at Leidos

Strategic Approach to Supply Chain Risks

leidos

Threat Vectors

Increasing Regulations	Limited Influence on Manufacturers
Supplier Financial Stability	Globalization of the Supply Chain
Counterfeit and Gray Market	Geopolitical Influences
Cybersecurity Intrusions	Global Pandemic & Natural Disasters
Open Source Solutions	Transportation Network Security

GLOBAL SUPPLY CHAIN

Strategy of Supply Chain Resiliency

**Build a framework for a resilient, flexible supply chain
One that resists disruptions and recovers after disruptions occur**

Approach to Managing Supply Chain Risks

▶ Enterprise & Program Level Supply Chain Risk Management (SCRM) Plans

▶ Supply Base Rationalization

▶ Restricted Supplier List

▶ Supply Chain Incident Database

▶ Pre-Award Cyber & Privacy Assessments

▶ Chain of Custody Audits

▶ CMMC Guidance for Small Business

▶ Robust Report Card Program

▶ Supply Chain Tabletop Exercises

▶ Leadership in Industry Associations

▶ Sponsored University Research

INTEGRITY

PEOPLE
Trained Sourcing Team
Industry Associations
Strong Supplier Relationships

TOOLS
Data Exchanges
Due Diligence, Monitoring
Risk Register
Traceability Audits

SUPPLY CHAIN RISK MANAGEMENT APPROACH

PROCESSES
Continuous Process Improvement
Secure Supply Chain Process
FAR Compliance: Purchasing Manual

RESILIENCE

SECURITY

QUALITY

Accredited Testing and Evaluation (AT&E) Lab

20+ years of Common Criteria, FIPS testing

1,000+ IT security products certified

Our NVLAP Accredited Lab provides:

▶ Common Criteria certifications

▶ Federal Information Processing Standards (FIPS) 140 certifications

▶ Security Content Automation Protocol (SCAP) validations

▶ Personal Identity Verification Middleware validations

▶ Transportation Working Identification Credential validations

▶ Ad-hoc evaluation and consulting

Challenges in Cyber Defense of the Supply Chain

Persistence of advanced threats

Intent, sophistication, opportunities

Engineering Tradeoffs

Functionality, security, resiliency

Continuous Change

Suppliers, dependencies, vulnerabilities

Proactive emphasis given current threat landscape

leidos

Augment cybersecurity capabilities to harden software systems against future supply chain attacks

Supply Chain

Enhancing software review process

Enhancing supplier code scanning

Improving supplier relationship management

Cyber Hygiene

Accelerating adversarial testing

Continuing to limit internet access, privilege

Enhancing our SecDevOps environments

Cyber Defense

Improving behavioral detections

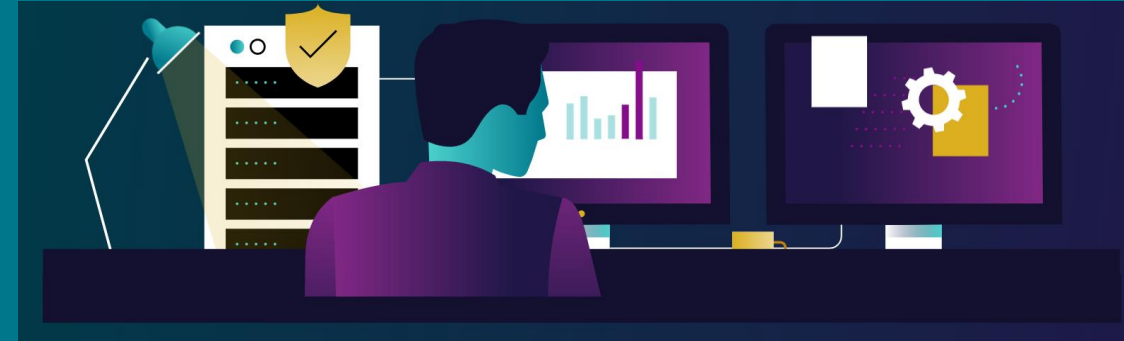Enhancing inspection of user authentication activity
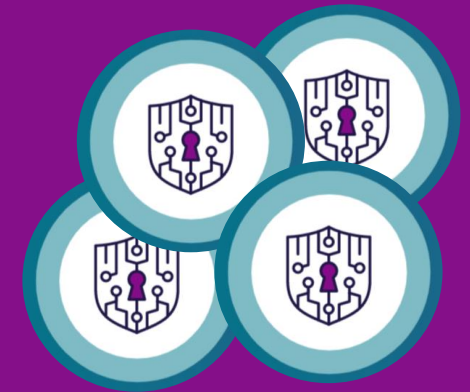
Expanding threat intelligence automation

Expanding Research into Practical Applications

Securing Development Environments

Operationalizing SBOMs

Journey to Zero Trust: Behaviors, Detections, Responses

SBOM: Software Bill of Materials

Supply Chain in Action at Leidos

Integrated Systems | Mission Software Systems | Digital Modernization | Cyber Operations | Logistics