CISCO Connect

Anticipate. Navigate. Adapt: Advancing Cyber Strategy in a Complex Threat Era

Kimberly Osmond, Splunk Security Advisor

November 19, 2025

Cybersecurity Has Outgrown Its Own Definition

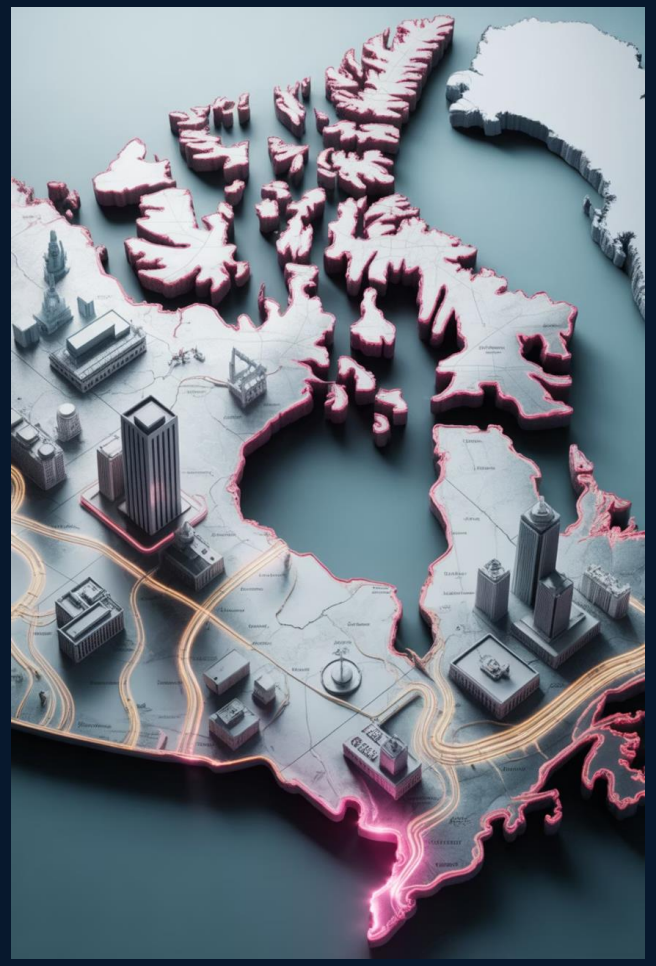
From walls to foresight.

From defense to resilience.

Security isn’t compliance — it’s strategy.

cisco

Why Canada Is at a Turning Point



Nation-State Threats

Rising attacks targeting Canadian critical infrastructure, government systems, and supply chains from sophisticated adversaries

Regulatory Pressure

Data residency, sovereignty requirements, and privacy regulations are tightening across federal and provincial jurisdictions.

Workforce Gap

Significant constraints in cybersecurity talent and emerging AI skills gap creating operational vulnerabilities.

Digital Dependency

Increased reliance on operational technology (OT), cloud-native environments, and interconnected systems expanding the attack surface.

Why Traditional Security Models Are Breaking Down

Yesterday's Model

- Perimeter-based defense
- Static security controls
- Reactive SOC operations
- Compliance-led decision making
- Tool-centric approach
- Siloed security teams

Tomorrow's Posture

- Visibility-based architecture
- Adaptive analytics and automation
- Predictive defense capabilities
- Resilience-led strategy
- Outcome-focused integration
- Unified security operations

Why Transformations Fail

Tool Sprawl

Excessive security tools create fragmentation and complexity.

Alert Fatigue

Teams overwhelmed by constant notifications lose focus on real threats.

Misaligned Priorities

Disconnected objectives prevent coordinated response.

Transformation fails due to a lack of clarity and ownership. Leaders succeed by making visibility and accountability cultural imperatives, not just technical checkboxes.

From Reactive Response to Predicative Posture

Visibility

Unified observability across cloud infrastructure, network traffic, endpoints, and applications—creating a single source of truth.

Insight

AI and ML-driven analytics to surface actionable context, reduce false positives, and identify patterns humans might miss.

Response

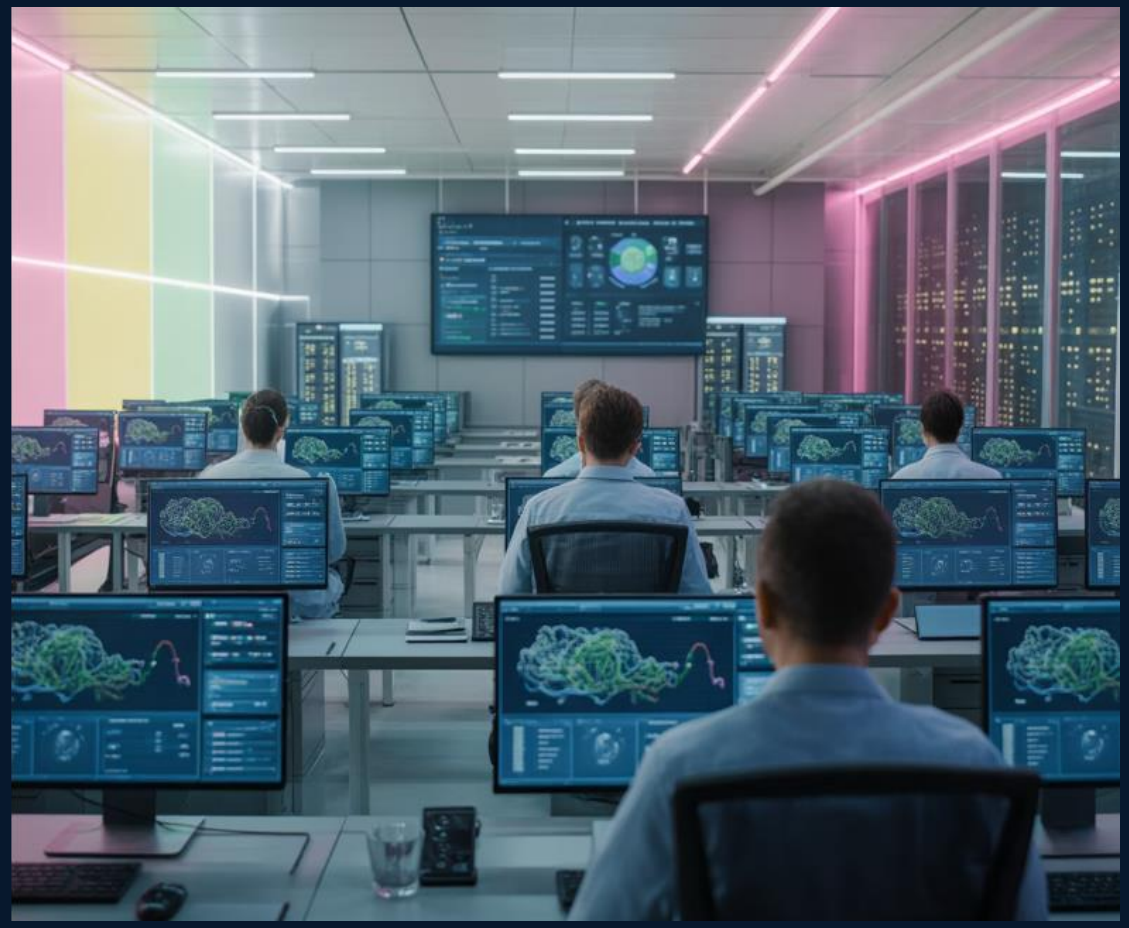
Intelligent automation with human oversight for rapid containment, orchestrated remediation, and coordinated defense.

Adaptation

Continuous posture improvement based on threat intelligence, incident learnings, and evolving risk landscape.

Real-World Transformation: Healthcare Resilience

- Unified data. Predictive defense. Automated response.
- 68% faster detection without adding headcount.
- Proved that clarity, not complexity, drives resilience.



The Playbook for Continuous Cyber Evolution

01

From Projects to Programs

Treat security as a living, breathing system that evolves with your business, not a series of disconnected initiatives with arbitrary end dates.

02

From Tools to Telemetry

Measure what matters—focus on meaningful signals that drive decisions, not vanity metrics that generate noise and alert fatigue.

03

From Compliance to Confidence

Build metrics around genuine resilience and recovery capabilities, not just audit checkboxes that satisfy minimum regulatory requirements.

04

From Detection to Anticipation

Leverage advanced analytics and threat intelligence as predictors of future risk, enabling proactive defense before incidents occur.

05

From Silos to Synergy

Connect IT security, OT environments, cloud architecture, and business risk perspectives into a cohesive enterprise view.

cisco

Operationalize Resilience – From Concept to Practice

People

Build operational muscle memory

- Conduct regular tabletop exercises
- Run realistic threat simulations

Process

Standardize response frameworks

- Create unified incident response playbooks
- Define clear escalation paths and authority

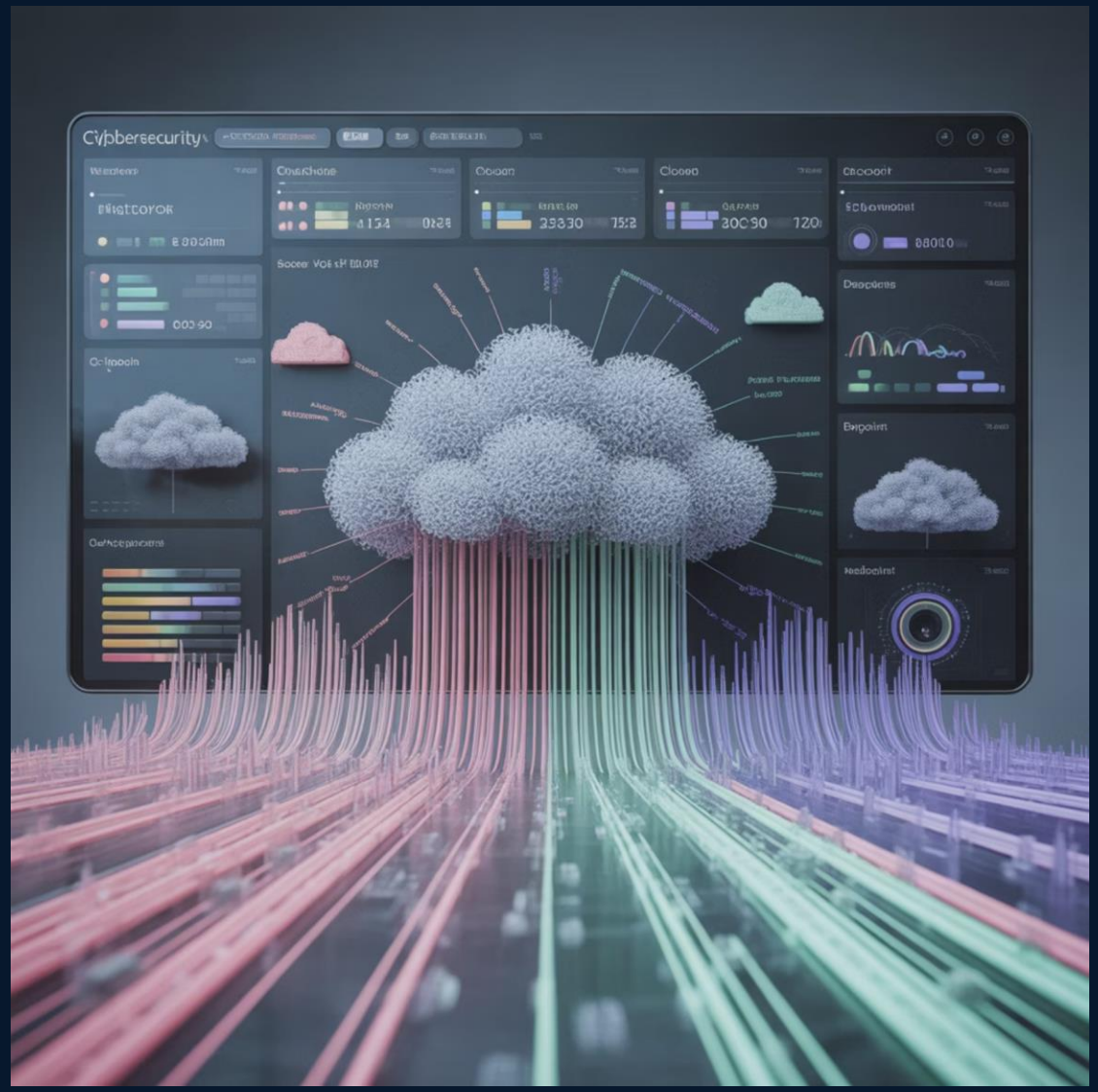
Platform

Unify visibility and control

- Consolidate telemetry data into a single source
- Integrate security tooling for seamless data flow

Cisco + Splunk: Unified Security Intelligence

- Transforms data into actionable insight across your digital real estate
- Eliminates blind spots and reduces complexity
- Accelerates response and boosts analyst effectiveness



Where the Next Wave of Risk Will Emerge

Short-Term Horizon

AI-Generated Attacks: Sophisticated phishing, deepfakes, and automated vulnerability exploitation using generative AI.

Supply Chain Risks: Third-party compromises and software supply chain attacks increasing in frequency and sophistication.

1

Mid-Term Horizon

Quantum Preparedness: Crypto-agility and post-quantum cryptography migration becoming critical for long-term data protection.

Cloud-Native Challenges: Container security, serverless vulnerabilities, and edge computing expanding the attack surface exponentially.

2

Long-Term Horizon

Regulatory Harmonization: Evolving privacy laws, critical infrastructure requirements, and cross-border data governance creating complexity.

Human Factors: Cognitive load, analyst fatigue, and the need for augmented decision-making in security operations centers.

3

Cybersecurity: From Cost Centre to Confidence Engine

- Enables innovation and drives competitive advantage
- Builds trust and strengthens market position
- Resilience -> Trust -> Loyalty -> Growth

Cyber Resilience Blueprint

Start with visibility:

The foundation of every decision.

Build adaptability:

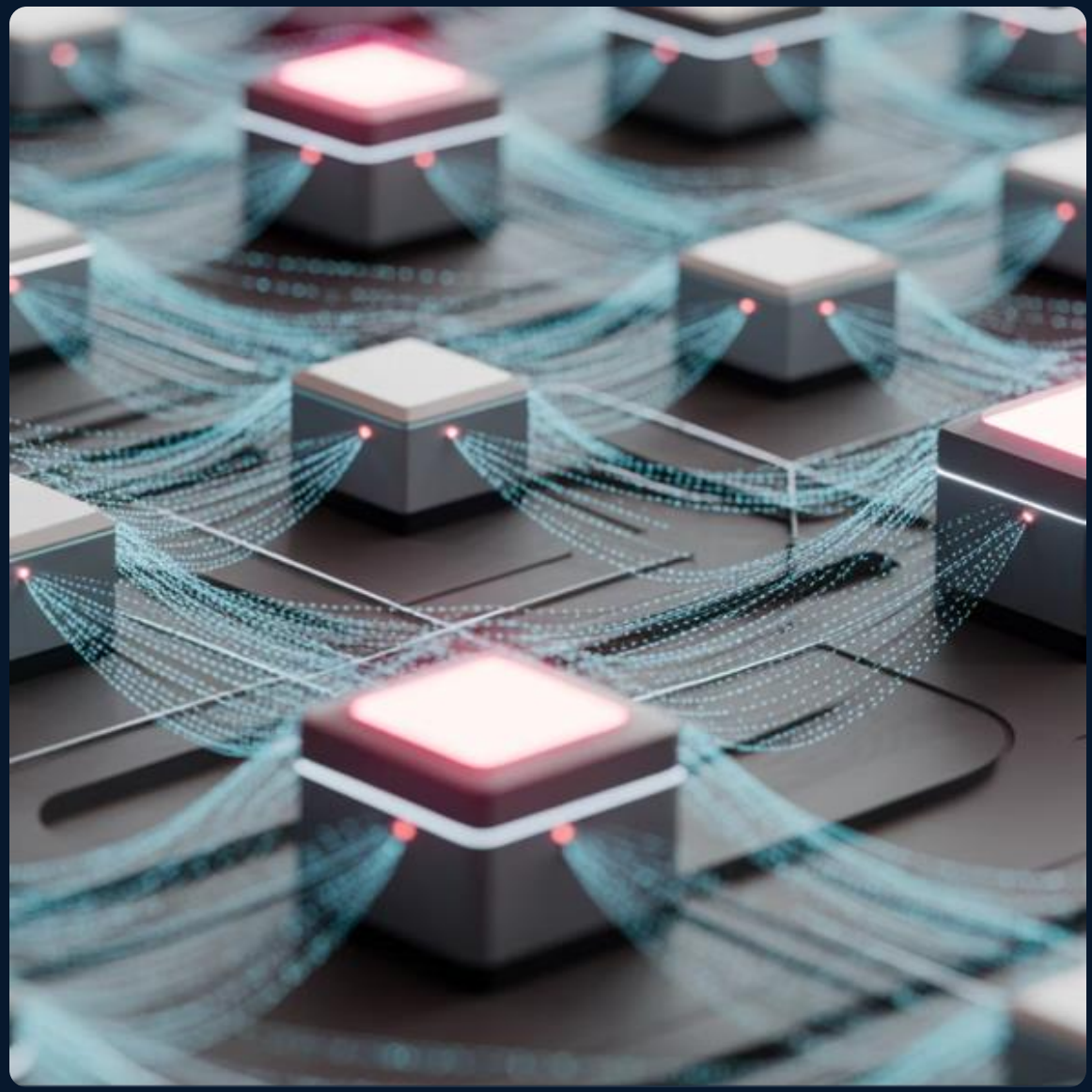
Design resilience into your architecture.

Partner across ecosystems:

Collaboration multiplies defense.

Design for resilience, not perfection:

Expect breaches. Recover fast.



Cyber Leadership in 2026: Proactive Resilience

Quantify Cyber Risk

CISOs use FAIR methodologies to translate cyber risk into business impact, enabling data-driven investment and clear ROI.

Advanced Analytics in SOC

SOC leaders use machine learning, custom rules, and data visualization (Python, SIEM) to detect subtle indicators and complex attack patterns.

AI as Force Multiplier

AI augments human judgment for vulnerability prioritization, incident triage, and secure code reviews, freeing experts for strategic challenges.

Thank you