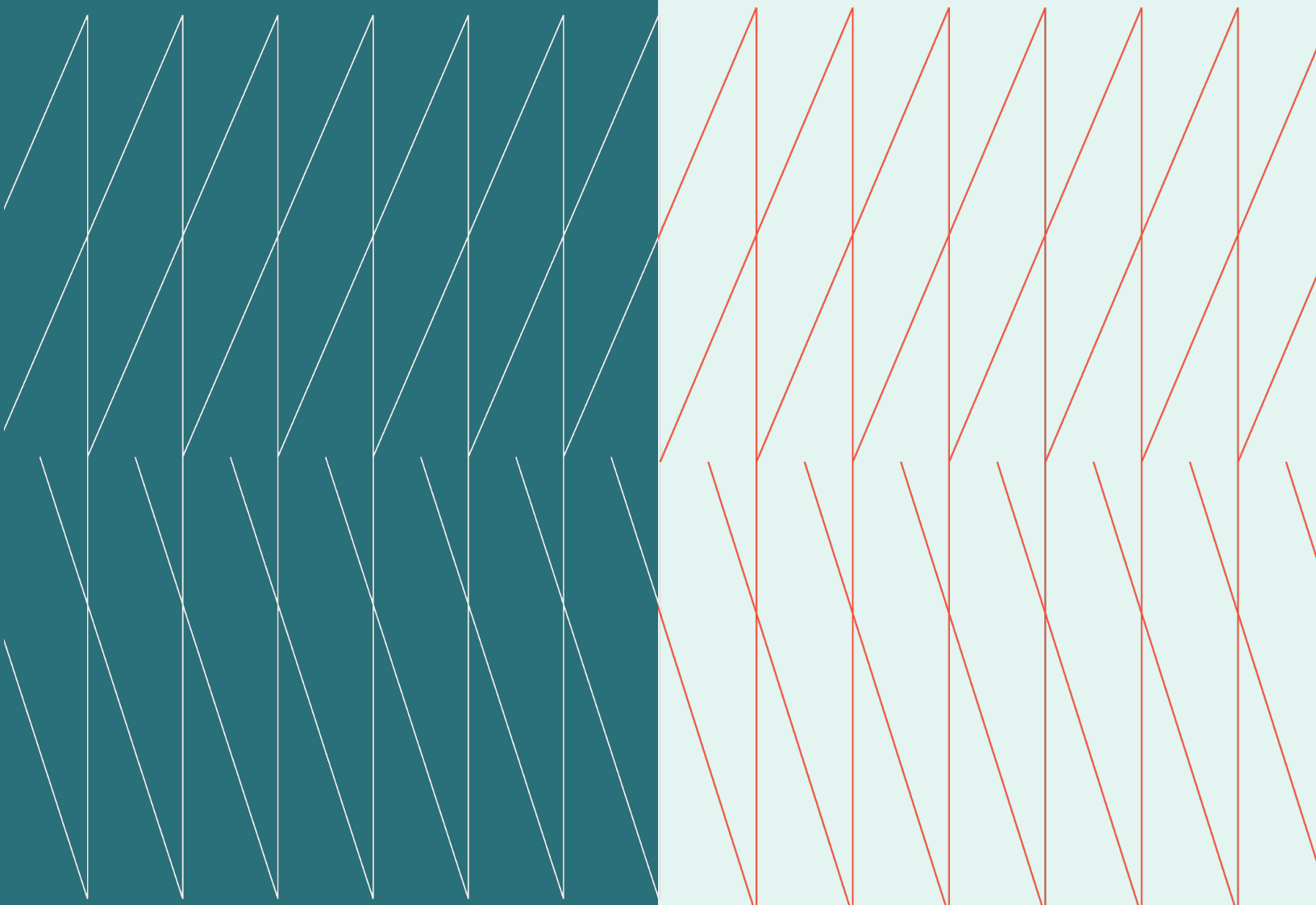
CISO

Expert Exchange

September 16, 2025

kyndryl

Executive Summary



Hosts:

Denis Villeneuve
Cybersecurity and Resilience Practice Leader, Kyndryl Canada

Jimmy Nilsson
Vice President, Zero Trust, Kyndryl

Overview

In this CISO peer exchange, security leaders from various Canadian organizations convened to discuss critical challenges and strategies in cybersecurity, focusing on identity and zero-trust principles within an increasingly complex ecosystem. The conversation highlighted the profound impact of evolving technologies, particularly artificial intelligence (AI), on security operations and risk management. Key themes emerging from the discussion include the foundational role of identity in zero trust, the unique complexities of managing non-human and AI identities, and the operational and incident response challenges introduced by AI's rapid proliferation.

Expert exchange themes

- Identity Management as a Zero-Trust Imperative
- Managing Non-Human and AI Identities
- Navigating AI's Operational and Incident Response Complexities

Identity Management as a Zero-Trust Imperative

Effective identity and access management (IAM) forms the critical foundation for successfully implementing a zero-trust security strategy, demanding a strategic, integrated approach across the enterprise.

Organizations widely acknowledge that zero-trust security cannot be effective without robust identity management systems. One participant noted that it is challenging to achieve an effective zero-trust posture without a strong handle on identity. Similarly, another member emphasized that while zero trust is a valuable philosophy, its efficacy hinges on solid identity and vulnerability management practices, which were foundational even decades ago.

- Many organizations invest in industry-leading identity and access management tools, but often fail to fully integrate these investments into their broader IT architecture, resulting in continued manual operations for identity governance. This gap between investment and effective operationalization highlights a common challenge in leveraging advanced security solutions.
- A defined methodology is crucial to address integration challenges, one that convenes cross-functional teams comprising business, IT, and security stakeholders. This collaborative approach ensures a comprehensive understanding of the systems being secured and the specific identity requirements, whether human or non-human, that the system relies upon.
- One participant shared a "back to basics" approach for human identity management, clearly defining specific scopes, such as financial perimeters, crown jewels, or critical applications managing sensitive data. This structured approach helps the organization prevent scope creep and allows for manageable, operationalized implementation of identity practices.

Managing Non-Human and AI Identities

The rapid proliferation of non-human and AI identities presents significant challenges for traditional identity governance and lifecycle management, requiring innovative approaches.

Non-human identities, especially those related to agentic AI, are growing exponentially, creating a more complex management landscape than human identities. These identities often lack traditional multi-factor authentication and rely on certificates, demanding different lifecycle management disciplines. Members noted the difficulty in governing these identities effectively without slowing business innovation.

- A key best practice involves mandating a sponsor or owner for every non-human identity, ensuring accountability within the organization. If an identity lacks a sponsor, it faces deactivation, a process that requires significant effort to trace and revalidate, particularly for AI-generated identities, which are often spun up quickly and without standardized naming conventions.

- Cloud security posture management tools provide critical visibility for discovering and inventorying non-human identities within cloud platforms. This tooling is invaluable for identifying the vast number of cloud assets, many of which are identities, and helps manage vulnerabilities and ensure secure deployments.

- The dynamic nature of microservices and AI, where identities are frequently spun up and down, makes continuous inventory and management a significant challenge. Organizations are learning to manage this sprawl by implementing controls around data egress from cloud environments and continuously monitoring volumes of new identities.

Navigating AI's Operational and Incident Response Complexities

The increasing integration of AI into business processes introduces new operational hurdles and complex incident response scenarios that traditional frameworks may not adequately address.

Development teams often deploy AI solutions on cloud platforms without adequate security considerations, leading to vulnerabilities and potential data exposure. An executive described finding numerous instances exposed to the internet through cloud security posture management solutions, necessitating immediate remediation. The rapid pace of AI development and deployment compounds these operational risks.

- Effective control over AI solutions requires external attack surface management and network lockdown strategies, such as using a secure access service edge (SASE) solution to funnel all traffic, including SaaS applications, for better visibility and identity-based control. This allows organizations to monitor data flows and block unauthorized access to AI services.

- Developing a specific incident management framework for AI-driven processes is critical, as current incident response teams may lack the expertise to handle AI-specific issues like hallucinations. Responding to such incidents in interconnected AI components within business workflows is complex, risking significant business disruption if the only option is to shut down the process.

- Integrating builders' knowledge into the incident response process is essential for AI-related incidents. This involves proactive knowledge transfer to operations teams, including diagrams, potential problem types, and call trees to quickly engage subject matter experts when AI-driven processes encounter issues. This helps bridge the skill gap between AI developers and traditional incident responders.

- Data discovery and classification programs are foundational for managing risks associated with organizational data used by AI services, whether internal or public. Manual classification by users, validated by security controls, is seen as a more effective approach to prevent data exfiltration compared to solely relying on automated tools, which can create excessive noise or liability. However, securing funding for such foundational, non-revenue-generating cleanup efforts remains a common challenge for organizations.

To learn more about the Kyndryl Canada CISO Expert Exchange or to become a member of this community, please visit this website.

kyndryl