From Consumer-Grade to Enterprise-Ready AI

This session explored the transition from individual AI usage to enterprise-scale implementation within corporate security. Most organizations remain stuck at “consumer-grade” AI, achieving personal productivity gains without systemic transformation. The discussion highlighted that successful enterprise AI requires structured process documentation, data readiness, governance, and cross-functional alignment. The session underscored that AI transformation is a multi-year effort centered on operational redesign rather than technology alone.

Speakers

Ankur Arora
VP, Marketing
Ontic

Christopher McDonald
VP, Security Technology
Oracle

Key Themes and Topics

From Individual Productivity to Organizational Transformation

Many security teams use AI tools individually, but enterprise value requires embedding AI into workflows. Without systemic integration, outcomes remain inconsistent and dependent on user skill, limiting measurable impact across security operations and decision-making processes.

Business Process as the Core of AI Success

AI implementation failures are rarely technical. The primary barrier is unclear or undocumented processes. Security leaders must first define how work is performed before applying AI, ensuring consistency, scalability, and alignment with operational objectives.

Data Normalization and Integration as Critical Enablers

Fragmented tools and siloed data limit AI effectiveness. Consolidating and standardizing data across systems enables better insights, automation, and cross-functional visibility. Without clean, connected data, AI outputs remain incomplete or unreliable.

Continued on next page

Key Themes and Topics

Managing Cognitive Debt in High-Velocity Environments

AI accelerates output generation, but review capacity often lags. This creates “cognitive debt,” where teams produce more than they can fully validate. Security leaders must redesign workflows to maintain quality without creating bottlenecks.

Governance and Privacy as Foundational Requirements

Security teams handle sensitive data, making governance essential. Clear guardrails on data usage, access, and AI interaction are necessary to prevent risk exposure. Governance must evolve from policy to practical, operational controls embedded in workflows.

Actionable Takeaways

Document End-to-End Security Processes

Map both formal and informal workflows across security functions, including undocumented practices. This creates a shared knowledge base for humans and AI, enabling consistent execution and forming the foundation for automation and transformation.

Define Process-Level AI Impact Goals

Move beyond generic goals like “increase productivity.” Establish specific outcomes for each process, such as improved risk assessment accuracy or faster incident triage. Clear definitions enable measurable success and stronger business justification.

Consolidate and Normalize Security Data Sources

Inventory all tools and data flows, then reduce fragmentation. Integrate systems where possible and standardize data formats to ensure AI can access complete, high-quality inputs across investigations, operations, and intelligence functions.

Establish Practical AI Governance Guardrails

Create a simple, actionable framework outlining acceptable data use, tool access, and review requirements. Align with existing policies but translate them into operational rules that security teams can apply consistently in daily workflows.

Continued on next page

Actionable Takeaways

Redesign Workflows to Address Cognitive Bottlenecks

Reevaluate review and approval processes to prevent senior-level bottlenecks. Introduce tiered validation, sampling, or automated checks to maintain quality while allowing AI-driven velocity to scale across the organization.

Start with High-Impact, Low-Complexity Use Cases

Select a critical but manageable process to pilot AI transformation. Demonstrate measurable improvements, then scale incrementally. Early wins build credibility, reduce resistance, and create momentum for broader enterprise adoption.

Notable Quote

“What we're working on is fully embedding [AI] into people's processes so it's transparent to the users. It's more than just one user optimizing their workflow, it's an optimization across the board for everyone and surfacing insights that can be consistent and repeatable”

- **Christopher McDonald**
VP, Security Technology
Oracle

Final Message

Enterprise AI in security is not about tools, but about redesigning how work gets done. Leaders who invest in process clarity, data readiness, and governance will move beyond experimentation to real operational impact. Start small, measure precisely, and scale deliberately to build sustainable advantage.