AI as a Force Multiplier — Without Compromising Trust

This panel explored how AI is being applied as a force multiplier in corporate security operations, with a strong emphasis on practical use cases, limitations, and governance. Speakers highlighted AI's role in accelerating intelligence analysis, improving threat detection, and enhancing consistency across workflows. At the same time, they stressed the importance of human-in-the-loop validation, data protection and governance, and cross-functional collaboration to mitigate risks such as hallucinations, data leakage, and misuse.

Speakers

Michael Civitano
Sr. Security Manager, GSOC & Intelligence
ServiceNow

Jesse Leads
VP, Global Security & Intelligence
Vast Space

Erik Jones
Senior Director, Data and AI Operations
Ontic

Farhad Tajali
SVP, Global Head of Safety & Security
Creative Artists Agency

Key Themes and Topics

AI as a Consistency and Efficiency Engine

AI is most effective when used to process large volumes of intelligence and standardize outputs across teams. It reduces variability caused by human fatigue or shift changes, enabling analysts to focus on higher-value judgment and decision-making rather than manual data triage.

Human-in-the-Loop Remains Critical

Across all security use cases, AI should be treated more like a junior analyst rather than a decision-maker. Human validation is required to ensure accuracy, prevent overreliance, and mitigate risks such as hallucinated or outdated information influencing security decisions.

Data Governance and Risk Management Are Foundational

Effective AI deployment requires early involvement from legal, privacy, compliance, and InfoSec teams. Without clear guardrails, organizations risk exposing sensitive data, violating regulations, or creating discoverable records that could introduce legal and operational vulnerabilities.

Continued on next page

Key Themes and Topics

AI Enhances Threat Detection and Intelligence Prioritization

AI significantly improves the ability to identify high-risk signals within large datasets, such as workplace violence and insider risk signals or open-source intelligence. By filtering noise and surfacing critical threats, teams can respond faster and allocate resources more effectively.

Trust in AI Requires Validation, Training, and Iteration

Trust is built over time through continuous training of models, validation of outputs, and alignment with internal data. Organizations must actively refine AI systems and challenge outputs rather than treating them as authoritative sources of truth.

Actionable Takeaways

Define Clear Use Cases Before Deploying AI

Identify specific operational pain points such as slow intelligence processing or inconsistent reporting. Deploy AI in targeted areas where it can deliver measurable improvements in speed, accuracy, or scalability rather than adopting tools broadly without clear purpose.

Establish Strong Data Governance Frameworks

Engage legal, privacy, and compliance teams early to define acceptable data inputs, usage policies, and guardrails. Ensure sensitive information is excluded or properly controlled to prevent regulatory exposure and unintended data leakage.

Implement Human Validation Workflows

Design processes where AI outputs are reviewed and validated by trained analysts before action is taken. This ensures accuracy, builds trust in the system, and reduces the risk of false positives or misleading intelligence.

Leverage Internal Data to Train AI Models

Use historical incident data, threat patterns, and internal workflows to train AI systems, in accordance with your company's policies. This improves relevance and predictive capability, enabling more accurate forecasting of risks such as workplace violence or regional threats.

Continued on next page

Actionable takeaways

Pilot and Test AI Solutions Before Scaling

Run controlled pilot programs to evaluate vendor claims and system performance in real-world environments. Validate accuracy rates, identify failure points, and refine configurations before deploying AI tools across the organization.

Develop AI Literacy Across Security Teams

Train team members on how to effectively use AI tools, including prompt design, validation techniques, and risk awareness. Encourage knowledge sharing and identify internal champions to drive adoption and innovation across the function.

Notable Quote

"We treat AI as a junior analyst. It can propose things, but it can't really determine everything, so there needs to be a lot of validation."

- Farhad Tajali
SVP, Global Head of Safety & Security
Creative Artists Agency

Final Message

AI is already reshaping security operations, but its value depends on disciplined implementation. Leaders who pair strong governance with practical use cases and human oversight will gain meaningful advantages in speed, insight, and scalability. The goal is not automation for its own sake, but smarter, more resilient decision-making in the high-stakes world of corporate security.