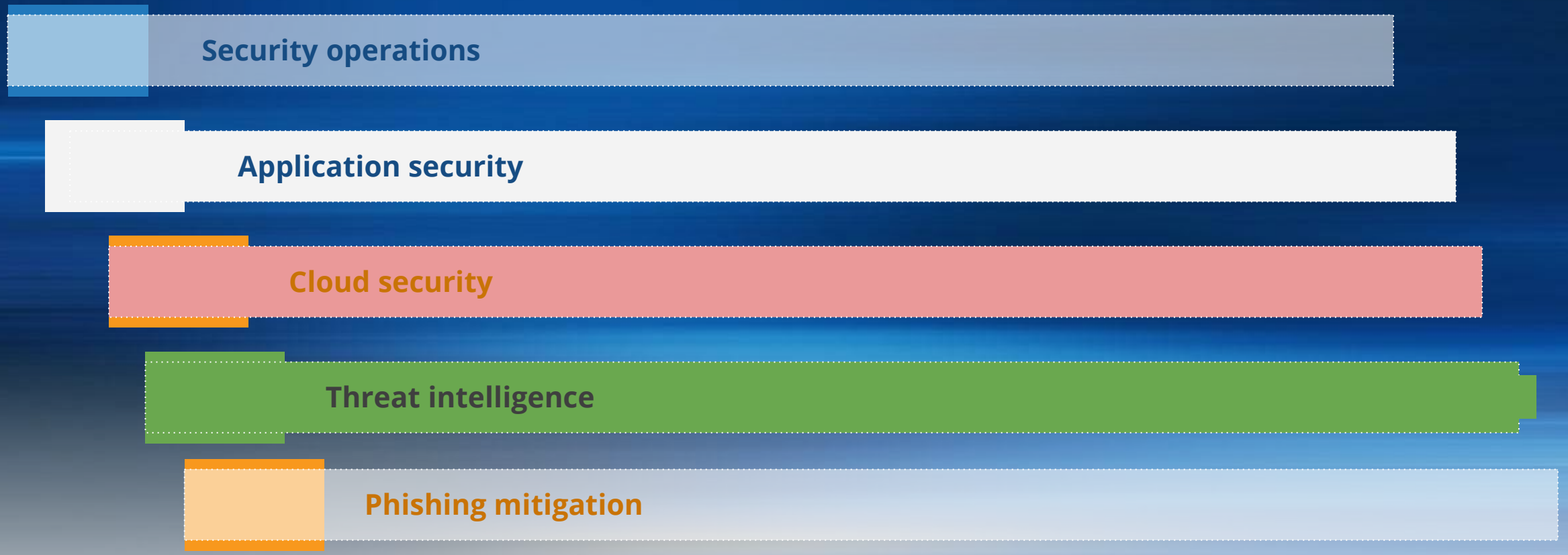
IDC IT Executive Programs

The Promises and Limitations of AI Transformation

Examples from the cybersecurity ecosystem

Christopher Tozzi
Adjunct Research Advisor, IDC
2024 - Q1

Key topics: The state of AI transformation in…



Background: The state of AI

The AI (spending) hype is real

40% of core IT spending will focus on AI by 2025

Worldwide spending on AI solutions will reach $500B by 2027

60% of enterprises are actively investing in genAI as of November 2023

100% increase in spending on genAI in 2024

Sources: IDC FutureScape: Worldwide IT Industry 2024 Predictions; IDC EMEA FutureScape 2024; GenAI Implementation Market Outlook: Worldwide Core IT Spending for GenAI Forecast, 2023–2027

But how real is AI transformation?

AI in cybersecurity: A brief history

What's old is new again (kind of)

Interpretive and predictive analytics

- snort (1998)
- OSSEC (2003)

VS.

Generative AI

- Tabnine (2013)
- Copilot (2021)
- ChatGPT-3.5 (2022)

The state of AI-powered cybersecurity

Security operations

Using generative AI to detect, investigate and respond to threats

Capabilities

- Query cybersecurity data using natural language (Splunk, CrowdStrike)
- Summarize or consolidate alerts (Google Cloud AI Workbench, Elastic)
- Reverse-engineer malware (Trend Micro, Microsoft Security Copilot)

Benefits:

- Speed and streamline operations
- Increase effectiveness of inexperienced analysts
- Increase ability to handle high volumes of threats

Limitations:

- Limited accuracy
- Less valuable for experienced analysts

Source: Generative AI in Cybersecurity Tools: Distinguishing Hype from Value (2023)

Application security

Improving application security across the software development lifecycle (SDLC)

Capabilities

- Detect vulnerable source code during development (Copilot)
- Suggest remediations for vulnerable code (Veracode, Snyk)
- Write queries to scan code for risks (Checkmarx)

Benefits:

- Increased ability to detect vulnerabilities early in the SDLC
- Faster vulnerability remediation

Limitations:

- May not detect vulnerabilities in complex codebases
- Suggested remediations may not be ideal

Source: Generative AI in Cybersecurity Tools: Distinguishing Hype from Value (2023)

Cloud security

Generate and validate cloud security configurations

Capabilities

- Evaluate IAM policies for security flaws (Tenable)
- Generate secure cloud security configurations (Cisco)

Benefits:

- Quick detection of risky settings in cloud environments
- Reduced risk of introducing insecure settings

Limitations:

- Support limited to certain clouds (such as AWS)
- Little clear advantage compared to rule-based IAM scanning

Source: Generative AI in Cybersecurity Tools: Distinguishing Hype from Value (2023)

Threat Intelligence

Accelerating threat assessment and response

Capabilities

- Synthesize threat data from multiple sources (Microsoft Security Copilot)
- Use natural language to explore threats (Sentinel One)
- Summarize threats (Recorded Future)

Benefits:

- Faster analysis of vast quantities of threat data
- Increased ability to detect threats before breaches occur
- Reduced burden on cybersecurity analysts

Limitations:

- Risk of inaccurate threat synthesis or summarization
- Limited tool support
- Less beneficial for experienced analysts

Source: Generative AI in Cybersecurity Tools: Distinguishing Hype from Value (2023)

Phishing mitigation

Enhancing phishing education and training

Capabilities

- Generate content for mock-phishing campaigns (IronScales)

Limitations:

- Generative AI may help threat actors execute phishing attacks more than it helps businesses stop them

Benefits:

- Ability to run more phishing simulations with less effort

Source: Generative AI in Cybersecurity Tools: Distinguishing Hype from Value (2023)

Guidance

Separating hype from reality

Do...

- Distinguish between different types of AI-based solutions
- Recognize that AI's value varies across domains
- Align AI adoption strategy with team experience and needs
- Erect safeguards to control for inaccuracy risks

Don't...

- Assume that anything labeled "AI" is actually novel
- Expect AI to supplant human teams fully
- Overestimate the speed and efficiency gains provided by AI
- Entrust key functions to AI alone

Christopher Tozzi

Adjunct Research Advisor, IDC

ctozzi@idc.com

IDC.com twitter.com/idc blogs.idc.com