HUNTERS

AI IN THE SOC:

The Revolution Is An Evolution

AI HYPE IS REAL

AI ▶

The 20 Hottest AI Cybersecurity Companies: The 2024 CRN AI 100

BY KYLE ALSPACH ▶

APRIL 8, 2024, 2:00 PM EDT

The coolest AI cybersecurity companies in 2024 include Crowdstrike, Fortinet, Netskope and Trend Micro.

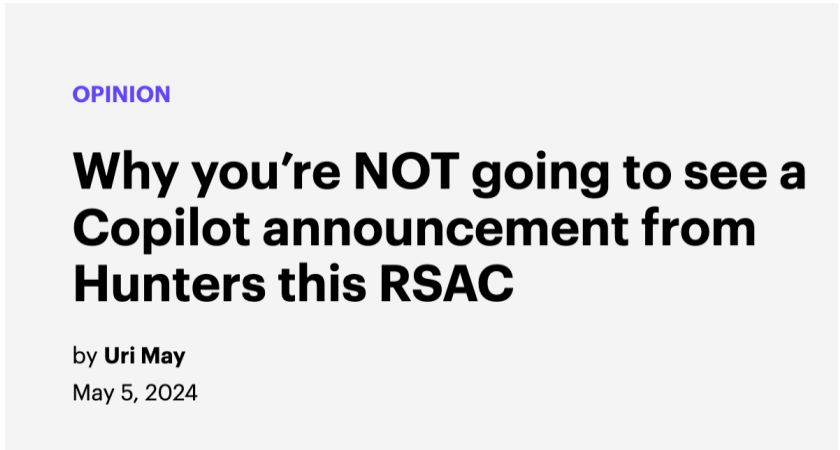
RSA Resources / Videos

Cyber Resilience in the Age of AI

EMERGING TECHNOLOGIES

Cybersecurity is on the frontline of our AI future. Here's why

Jan 15, 2024



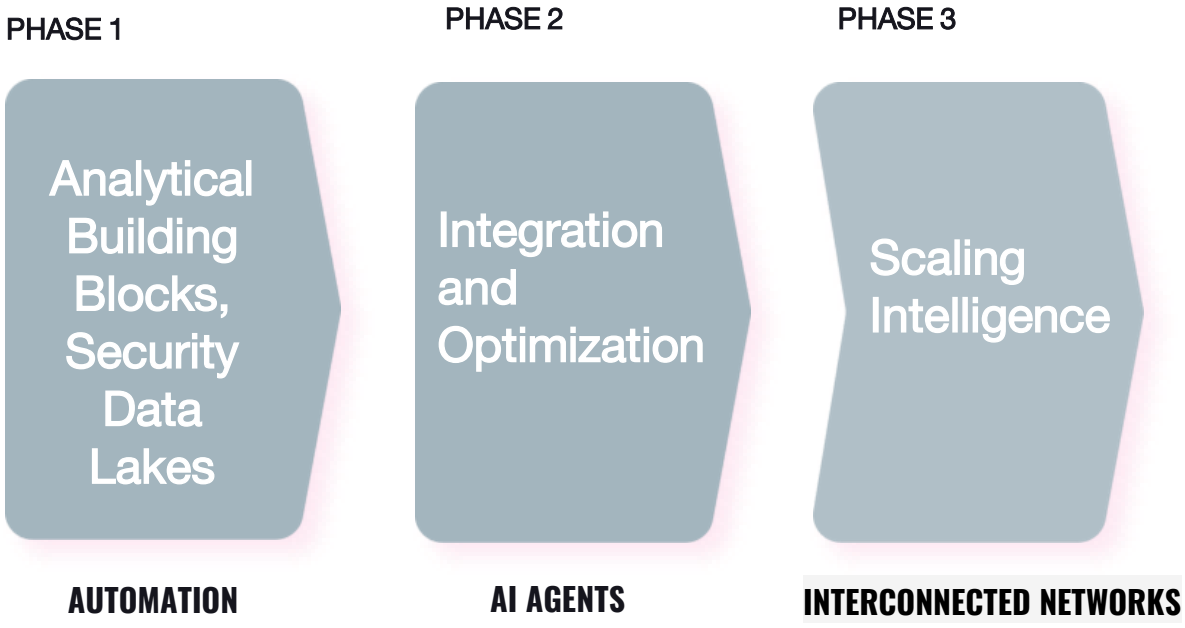
OPINION

Why you're NOT going to see a Copilot announcement from Hunters this RSAC

by **Uri May**

May 5, 2024

THE AI REVOLUTION IS AN EVOLUTION



HUNTERS

PHASE 1

Automation

ADVANCED CLUSTERING

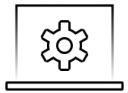
Clustering related threats based on their type and context cuts down on background noise, sharpens detection capabilities, leads to quicker triaging and more effective investigation.

ANOMALY DETECTION & MULTI CONTEXT UEBA

Proprietary ML-based anomaly detection algorithms detect anomalous events based on historical data.Multi-context UEBA techniques help reduce noise, find events that matter.

MULTI STAGE SCORING LAYERS

Deploy several dynamic layers on vast amounts of alerts and threat clusters based on multiple confidence and severity models, providing an accurate threat score.



GRAPH BASED CORRELATION AND ATTACK STORIES

Graphs are used to narrate attacks, drawing together all of the separate strands into a single story instead of multiple separate, isolated events.

PHASE 2

Integration and Optimization

AGENT BASED ARCHITECTURE

AI agents form a multiagent network and will be used for distinct tasks (i.e. triage), with access to skills and actions sufficient to do their work.

REINFORCEMENT LEARNING FROM HUMAN FEEDBACK

AI agents utilize various ML techniques, such as reinforcement learning, to optimize task execution based on past experiences embedded.

FROM BRUTE FORCE TO PRECISION

Move from a brute force approach (processing every alert in a linear, exhaustive manner) to an intelligent approach with the agent determining the most effective path for investigation.

PHASE 3

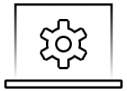
Scaling Intelligence

MULTIPLE FEEDBACK LOOPS

Agents share outcomes and insights, allowing the system to adapt collectively to new threats efficiently. The system learns from other agents, human analysts, and ecosystem knowledge.

DYNAMIC, RAPID RESPONSE MECHANISMS

The system's capability to react to threats can evolve, leveraging collective intelligence and automated adjustments to strategies in real-time.



OPTIMIZED RESOURCES

The system detects, responds to threats more efficiently and prioritizes actions based on the likelihood of success and the impact of the threat.

ULTIMATE VISION: AI-POWERED, HUMAN-DRIVEN SECURITY OPERATIONS

AI IS A MEANS TO AN END

Stopping threats ultimate goal

AI will help reach that goal more effectively

AI one component in security

SECURITY IS HUMAN ENDEAVOR

AI makes analysts work easier

AI doesn't replace analysts

Both have a role in security

MULTI-STAGE JOURNEY

In phase one now

Each phase builds off successes in previous one

Long journey (think self-driving cars)