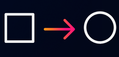
splunk> a CISCO company

The Evolution of AI in Cybersecurity

1970



Early Expert Systems and Rule-based IDS

In its earliest days, "artificial intelligence" in cybersecurity meant expert systems, rule-based programs using "if–then" instructions created by humans to make decisions automatically.

1986 "An Intrusion-Detection Model" is published.

1990s AI Winter reduces research funding.

1998 DARPA creates benchmarks to test rule- and learning-base prototypes.

2000

Behavioral Analytics and Machine Learning

By the 2000s, machine learning (ML) broke free from static rules — learning "normal" behavior for users, devices, and applications, and then detecting behavior anomalies.

2010s Adversarial machine learning leads to sharper attack tactics. In response, new proactive countermeasure methods emerge (e.g., adversarial training).

These concepts and safeguards still form the foundation of AI security conversations today.

2016

Breakthrough Events and Emerging Threats

By the late 2010s, AI moved from research promise to operational reality. Meanwhile, foundational research makes revolution strides, and threat actors adapt to AI's expanded capabilities.

2016 DARPA Cyber Grand Challenge sees AI systems tackle security tasks without human help.

2019 Deepfakes and voice cloning move from novelty to serious business risk.

2022

A New Era of Generative AI

By the early 2020s, generative models transform cybersecurity. As ChatGPT becomes publicly accessible, organizations look to prevent misuse.

2022 OpenAI releases ChatGPT.

2023 Black Mamba shows how LLMs could generate polymorphic malware.

2025

Rise of Agentic AI

Unlike traditional systems, agentic AI can perceive its environment, make decisions, and adapt strategies in real time with limited or no human intervention.

Early 2025 Rapid advances in generative AI open the door for Agentic AI.

Learn more about pivotal moments in the evolution of AI in cybersecurity and key takeaways for defenders as we enter the agentic AI era.

Read the blog

splunk> a CISCO company

26_CMP_Infographic_The-evolution-of-AI-in-cybersecurity