CIONET

Oktober Cyber Fest 2024

How AI and Evolving Architectures are Shaping Predictive Threat Detection and Compliance-Driven Response Systems

Shaun Cooney
| Field CTO
| Principal Strategic Advisor
| Director Innovation

splunk>
a CISCO company

Forward-looking statements

This presentation may contain forward-looking statements that are subject to the safe harbors created under the Securities Act of 1933, as amended, and the Securities Exchange Act of 1934, as amended. All statements other than statements of historical facts are statements that could be deemed forward-looking statements. These statements are based on current expectations, estimates, forecasts, and projections about the industries in which we operate and the beliefs and assumptions of our management based on the information currently available to us. Words such as “expects,” “anticipates,” “targets,” “goals,” “projects,” “intends,” “plans,” “believes,” “momentum,” “seeks,” “estimates,” “continues,” “endeavors,” “strives,” “may,” variations of such words, and similar expressions are intended to identify such forward-looking statements. In addition, any statements that refer to (1) our goals, commitments, and programs; (2) our business plans, initiatives, and objectives; and (3) our assumptions and expectations, including our expectations regarding our financial performance, products, technology, strategy, customers, markets, acquisitions and investments are forward-looking statements. These forward-looking statements are not guarantees of future performance and involve significant risks, uncertainties and other factors that may cause our actual results, performance or achievements to be materially different from results, performance or achievements expressed or implied by the forward-looking statements contained in this presentation. Readers are cautioned that these forward-looking statements are only predictions and are subject to risks, uncertainties, and assumptions that are difficult to predict, including those identified in the “Risk Factors” section of Cisco’s most recent report on Form 10-Q filed on February 20, 2024 and its most recent report on Form 10-K filed on September 7, 2023, as well as the “Risk Factors” section of Splunk’s most recent report on Form 10-Q filed with the SEC on November 28, 2023. The forward-looking statements made in this presentation are made as of the time and date of this presentation. If reviewed after the initial presentation, even if made available by Cisco or Splunk, on Cisco or Splunk’s website or otherwise, it may not contain current or accurate information. Cisco and Splunk undertake no obligation to revise or update any forward-looking statements for any reason, except as required by law.

In addition, any information about new products, features, functionality or our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not be incorporated into any contract or other commitment or be relied upon in making a purchasing decision. We undertake no commitment, promise or obligation either to develop the features or functionalities described, in beta or in preview (used interchangeably), or to include any such feature or functionality in a future release. The development, release, and timing of any features or functionality described for our products remains at our sole discretion.

splunk> a CISCO company

Data & Architecture

Data

Volume, Credibility, Movement
Costs, Value

Hosting

Hybrid: On-prem, Public Cloud,
WebApps, Mobile, IOT, Machine,
Long-lasting vs ephemeral

Convergence

Because the issue's source
matters less than the resolution.
Withstand and recover from
disruption
to digital systems

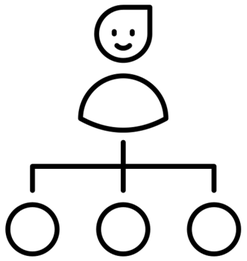
Regulation

Regulated resilience, use of AI,
data and cloud sovereignty, RAG

splunk>
a CISCO company

So what?

Vendor consortiums

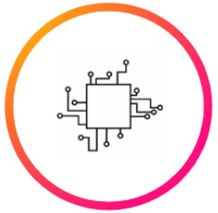


Federated Architectures

Standards (Composable Architectures)

Keep data where it belongs.

Not all data is equal. Treat it appropriately.



Use the most effective technology

Open & Extensible

splunk> a CISCO company

Generative AI is increasing the sophistication and effectiveness of spear phishing attacks

Generative AI is being used to deliver end-to-end capabilities to our adversaries

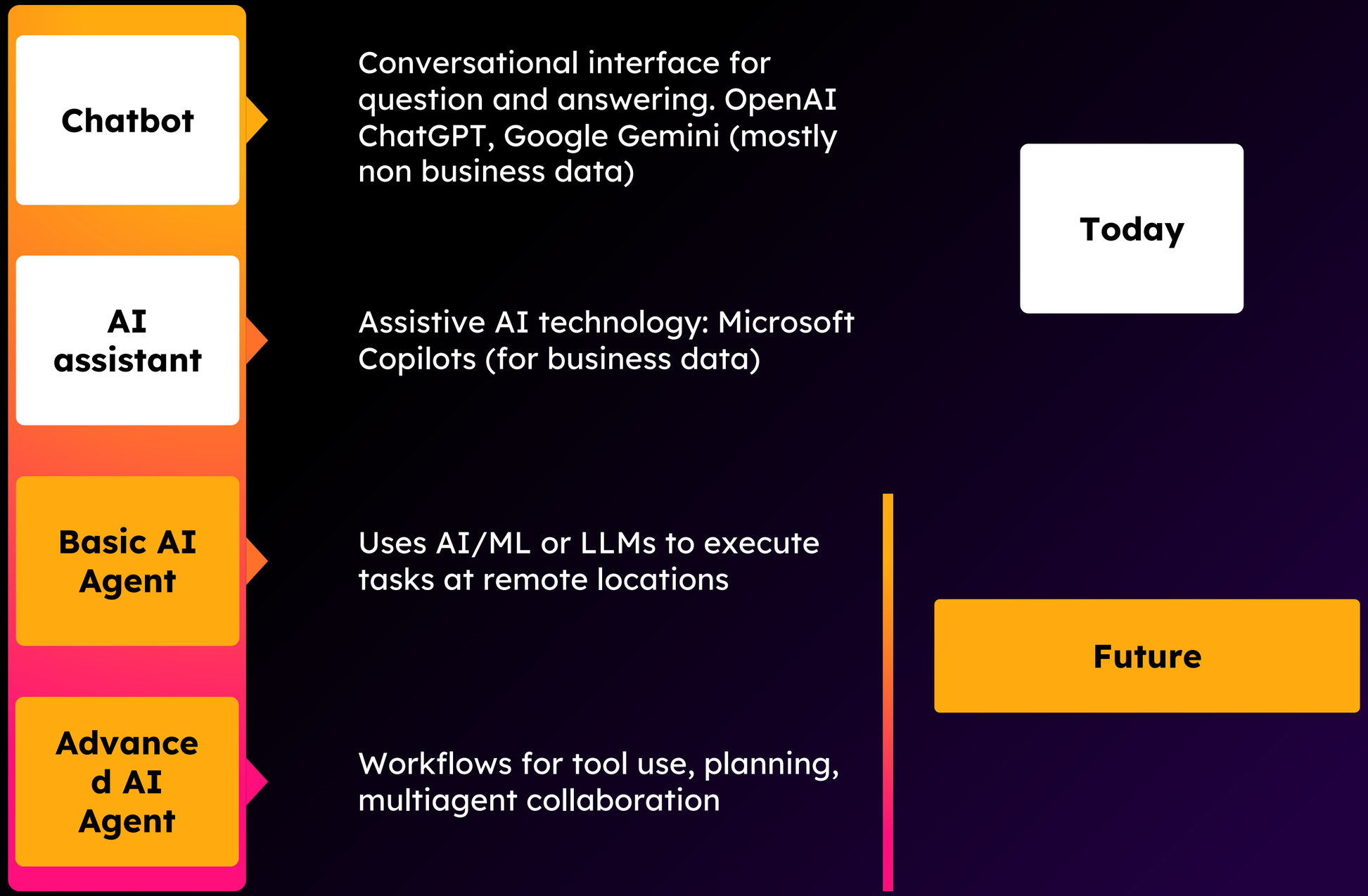
#RSAC

The wonderful world of underground chatbots

Real LLMs	Jailbreaks	Scams or 
• WormGPT	• EscapeGPT • BlackHatGPT • LoopGPT	• XXXGPT • WolfGPT • EvilGPT • DarkBARD • DarkBERT • DarkGPT • FraudGPT

TREND

RSAConference2024



Credits to Dennis Xu, Gartner

AI Futures: Now

AI Enabled Components

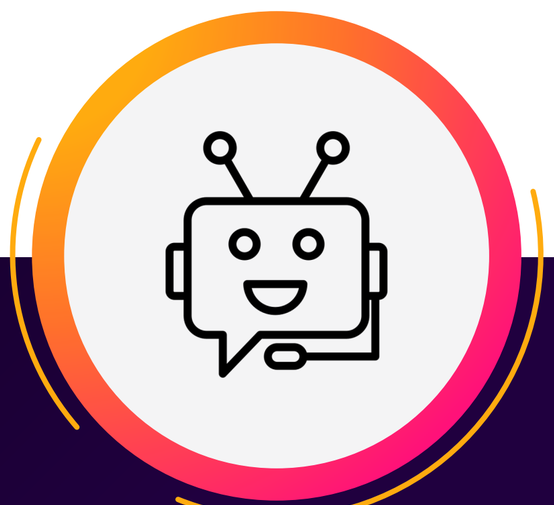
Social media analysis, phishing, AI-driven network reconnaissance to predict which systems are most vulnerable, password guessing

Multimodal Deep Fakes

Safe words, untrusted trusted partners, business email compromise

AI Evasion Techniques

Polymorphic Malware to bypass signature based detection systems



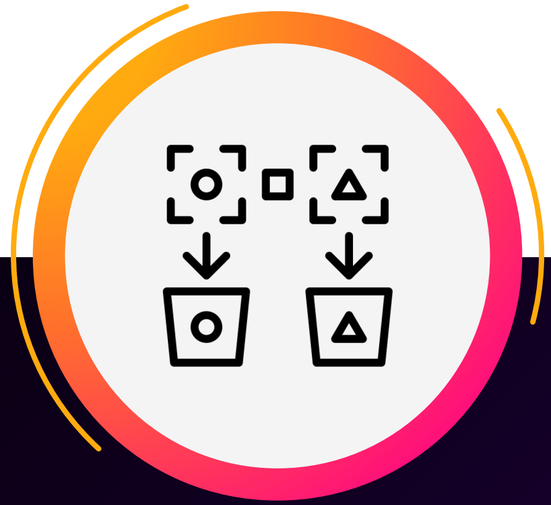
SecOps AI Assistants

NLP, Gen AI, Chat bots, guided/assisted workflows

splunk> a CISCO company

AI Futures: Next

AI enabled End-to-end



Adversarial Attacks on Machine Learning Models

Prompt Engineering!

Exponential Data Volumes

splunk> a CISCO company

So what?

CAUTION:

- **C**onsider your architecture – where is your data?
- **A**I Assistants to upskill staff and boost efficiency
- **U**se protection for your AI software and data
- **T**rain for "no trust," change processes, and introduce safe words
- **I**dentify and aggregate factors to balance risk
- **O**bserve behavioral analytics for abnormalities
- **N**ever forget the basics!

Thank you

splunk> a CISCO company