TIAA

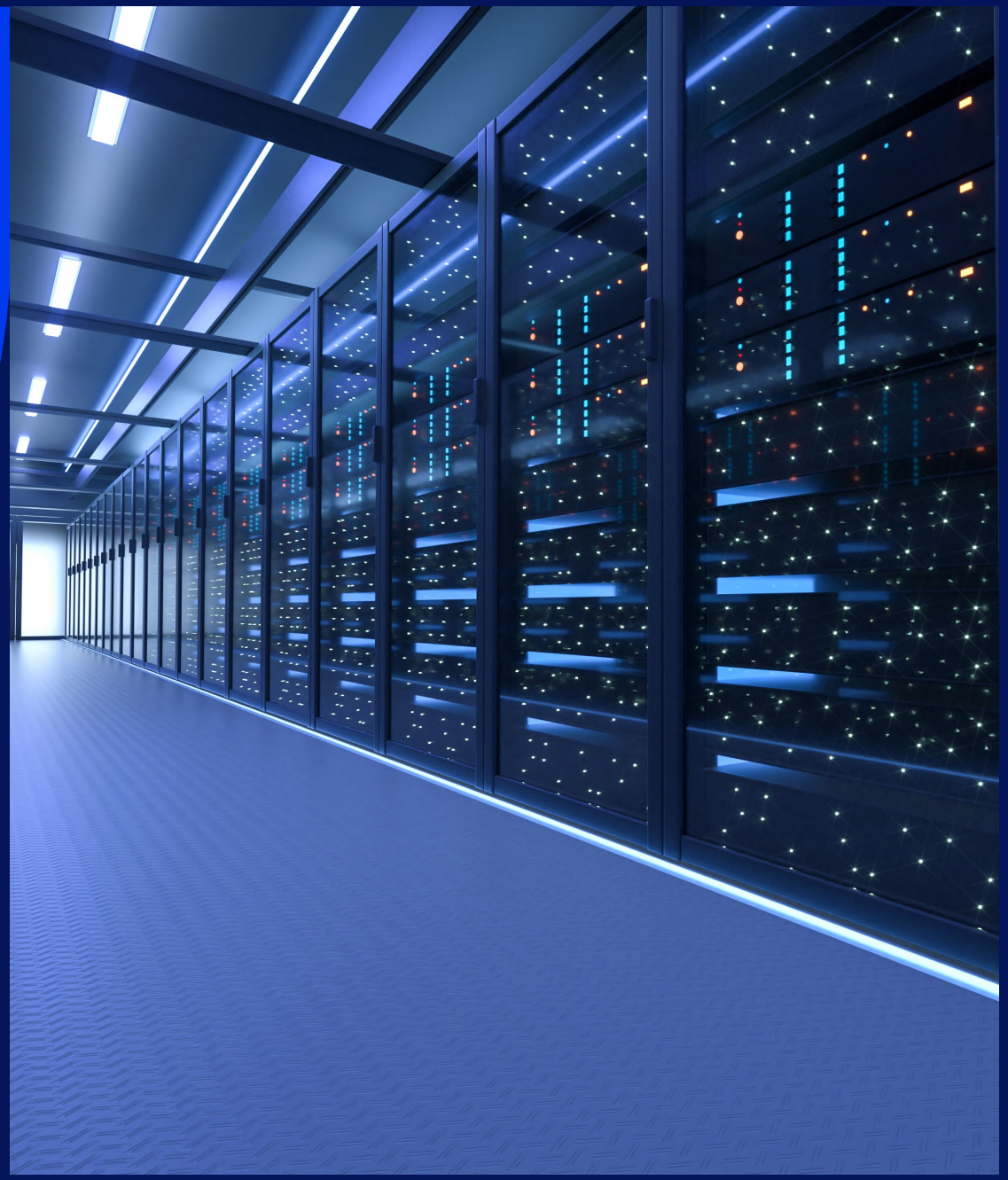
Balancing the Good and Bad of Agentic AI In Cybersecurity

American CIO and Cybersecurity Summit
San Francisco, California

Kapil Pruthi

Managing Director, Sr. Executive
Cybersecurity Engineer, TIAA

June 2, 2025 – 1:45 pm to 2:15 pm



Why is this topic important now?

3 Objectives

01 To demystify AI agents and Agentic AI – **To define and provide ways to understand them**

02 To cover how AI agents and Agentic AI **strengthen and weaken cybersecurity**

03 To highlight AI agents and Agentic AI opportunities that TIAA is exploring

What you'll get: knowledge and actionable insights about agentic AI & AI agents in cybersecurity

Part One

Setting context

- Definitions
- Illustrative Example – Higher Education

Part Two

Cybersecurity strengths/ weaknesses

- Good News/Bad News
- Amazing List of Agentic AI Capabilities
- How Agentic AI & AI Agents Strengthen Cybersecurity
- How Agentic AI & AI Agents Weaken Cybersecurity

Part Three

TIAA's cybersecurity Agentic AI opportunities

- Automated Security Policy Enforcement
- Pentesting/Bug Bounty Program
- Actionable Insights

Part One: Setting Context

How industry views AI Agents and Agentic AI

AI Agents & Agentic AI - Defined

AI Agent

- **Follows rules/script & completes a single task**
- **Goal-oriented**
- **Example:** ChatGPT's Deep Research – searches/synthesizes hundreds of online sources and produces comprehensive report – like a research analyst

Agentic AI

- **Multiple AI agents**
- **Write its own script to achieve a goal**
- **Acts independently to achieve broader, multi-step goals**
- **Dynamically reasons**
- **Makes decisions & acts on them**

Major Takeaway…

Agentic AI is more adaptable and autonomous than an AI agent

An example – Higher education

AI Agent

- Sends reminders to students about deadlines of assignments
- **One Task!**

Agentic AI

- Professor teaches class, grades work, spots a student struggling, and schedules office hours to meet with student – all autonomously
- Focuses on success of student throughout college
- Multi-step reasoning
- **Multi-Step Tasks!**

Part Two: Cybersecurity Strengths/Weaknesses

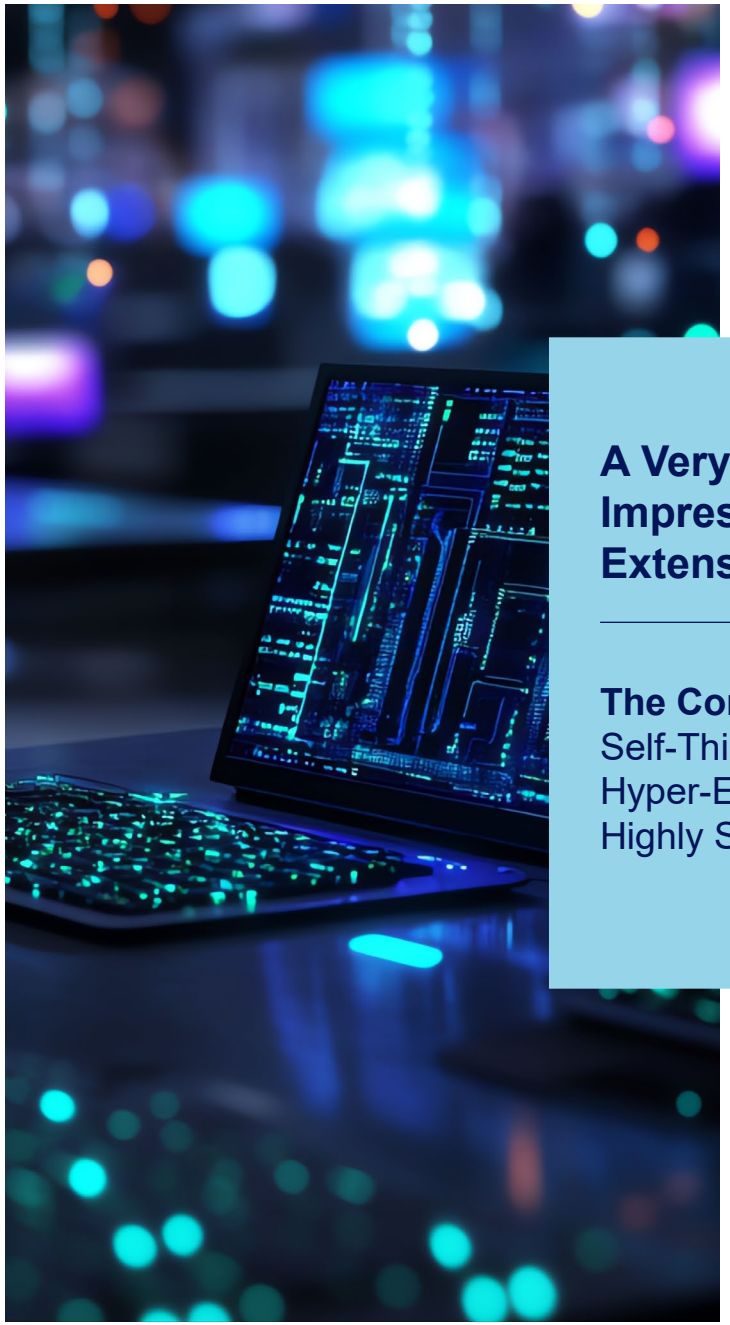
The good & The bad

Good News

- More AI agents/Agentic AI can help strengthen cybersecurity
- **Much faster, more frequent, in high volume, accurate, and economical detection & prevention of cyberattacks – Huge benefits**
- We can measure productivity gains by comparing AI agents or agentic AI to work done/hours expended by employees, while also recognizing that AI agents are not humans

Bad News

- Increase in AI agents/agentic AI can weaken cybersecurity
- Rogue Actions & Sensitive Data exposure
- **Much faster, more frequent, voluminous, accurate, and economical cyberattacks – Huge concerns**
- Productivity gains for bad actors as well.



List of Potential Agentic AI Capabilities

A Very Impressive and Extensive List

The Concept
Self-Thinking, Hyper-Efficient, Highly Skilled

01 **Reason** and plan

02 **Break tasks into sub-tasks**

03 **Self-correct based on new information**

04 **Autonomously ponder problems and solve them through a coherent series of logical deductions**

05 **Focus on longer term and more broad goals and make decisions**

06 Complete entire workflows

07 Perform research

08 Think at every step

09 Recognize patterns

10 Make inferences

11 Complete entire workflows

12 Write new software code

How Agentic AI & AI Agents Strengthen Cybersecurity

- Provide a framework for **risk reduction** and **efficiency** within cybersecurity
- More **autonomous, continuous, and faster** strengthening of cybersecurity controls, incident investigations
- Analysis of patterns to predict potential future attacks
- Intelligent Security Operations

How Insecure deployment of Agentic AI & AI Agents Weaken Cybersecurity

The Overall Problem – **Agentic AI opens more "doors"** for cyberattacks to enter – faster, easier, and more deceptively

01 **Rogue Actions**

02 **Data Exfiltration**

03 **Agentic AI & AI agents is not always accurate**

Part Three: Cybersecurity Agentic AI Opportunities TIAA is Exploring

Cybersecurity Agentic AI Use Case Opportunities

01 Continuous Network Monitoring & Automated Incident Response

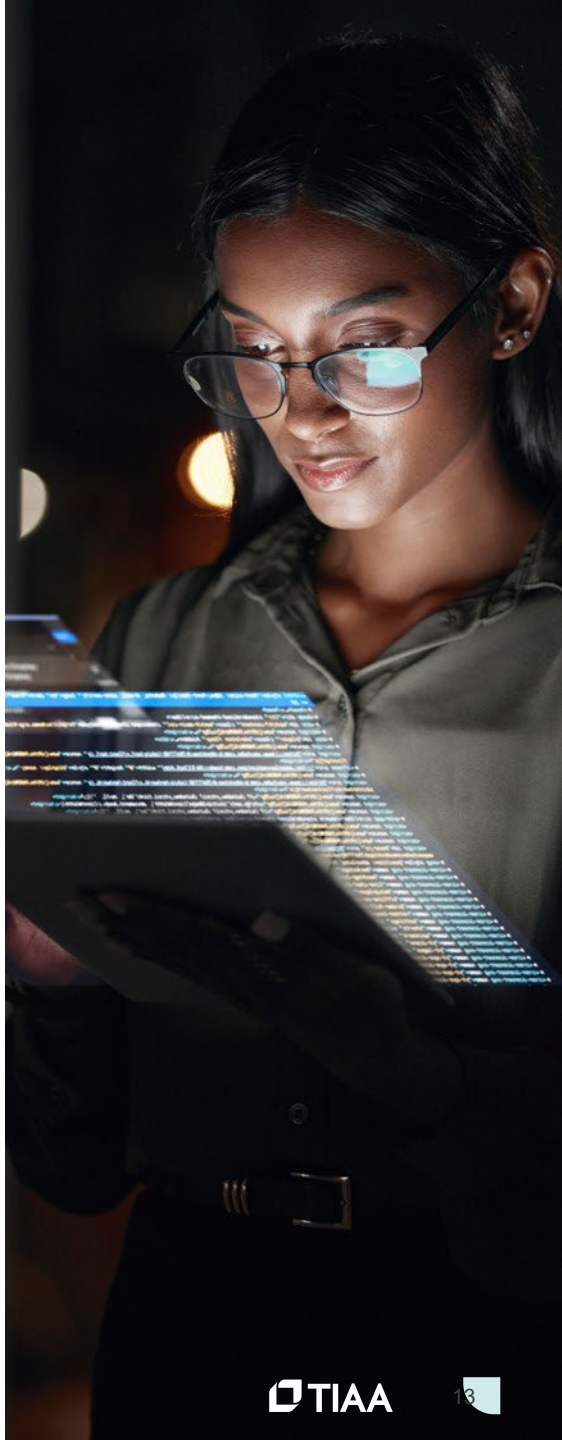
- Analyzes vast amounts of network traffic & system activity to **detect malicious behavior**
- **Identifies anomalies** based on historical data and behavioral baselines.
- **Inspects lateral movements** of cyberattackers if they penetrate inside a company's network
- **Disable/Isolate** host or traffic.

02 Automated Security Policy Enforcement

- **Analyzes sensitive elements in the unstructured data or documents**
- Detects and labels the document with sensitive information
- Monitors its movement
- Blocks unauthorized transfers

03 AI Powered Security Orchestration and Automation (SOAR)

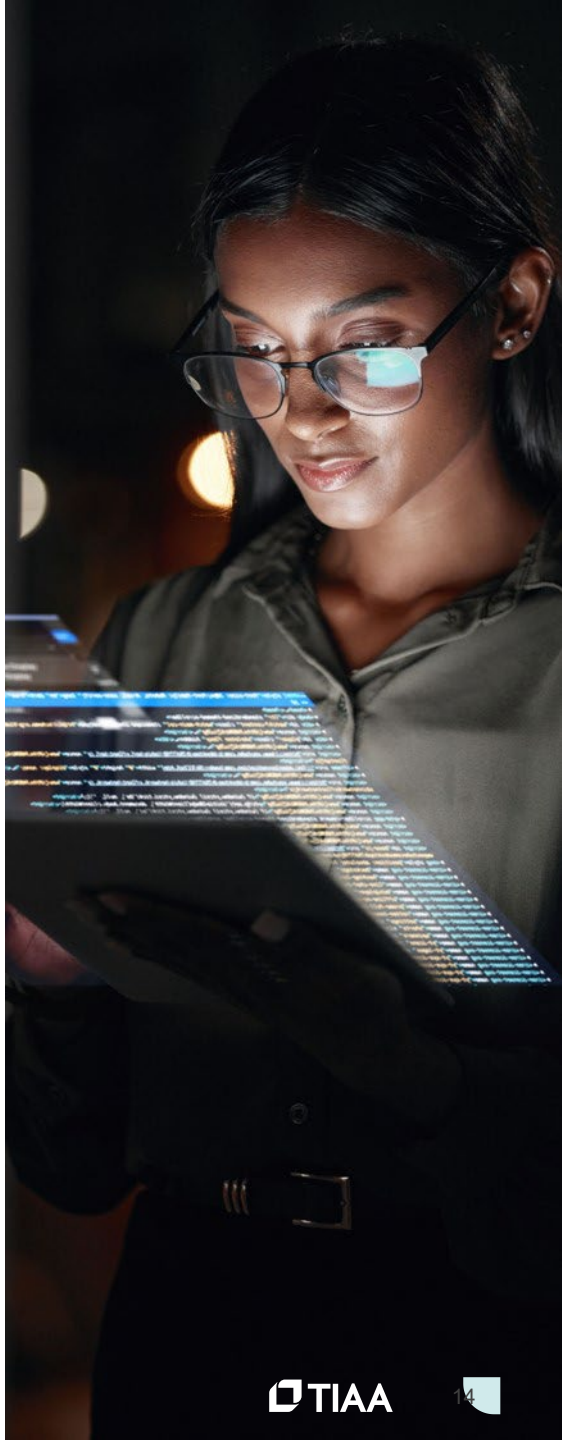
- **Automates cybersecurity playbooks** for faster threat containments and responses



Cybersecurity Agentic AI Use Case Opportunities

04 Pentesting/Bug Bounty Program

- Program depends on crowdsourcing initiatives (input from different people) that financially incentivizes **ethical hackers to find and report valid vulnerabilities in our company's software and systems** before real cyberattacks do
- **Uses autonomous security researcher technology** powered by AI agents
- **Scans our Internet-facing attack surface** to identify security vulnerabilities before bad actors do
- Leverages Gen AI to **rewrite and proofread pentesting and bug bounty reports**



7 Actionable Takeaways

01 **Train agentic AI & AI agents as if they're employees – give clear instructions and structure**

02 **Control access of agentic AI and AI agents**

03 Make sure they're consistent with business goals

04 Prepare for, and guard against, **variability in reasoning, planning, and actions agentic AI will perform**

05 **Ensure validation of source data before processing within Agentic frameworks.**

06 **Embrace a zero-trust architecture to contain agentic AI risks**. Zero trust means verify first and continuously, then trust second

07 **Focus on agentic AI and AI agent malicious activities;** keeping cyber teams updated regularly on these new threats and how to detect and prevent them

Open Q&A

Thank You