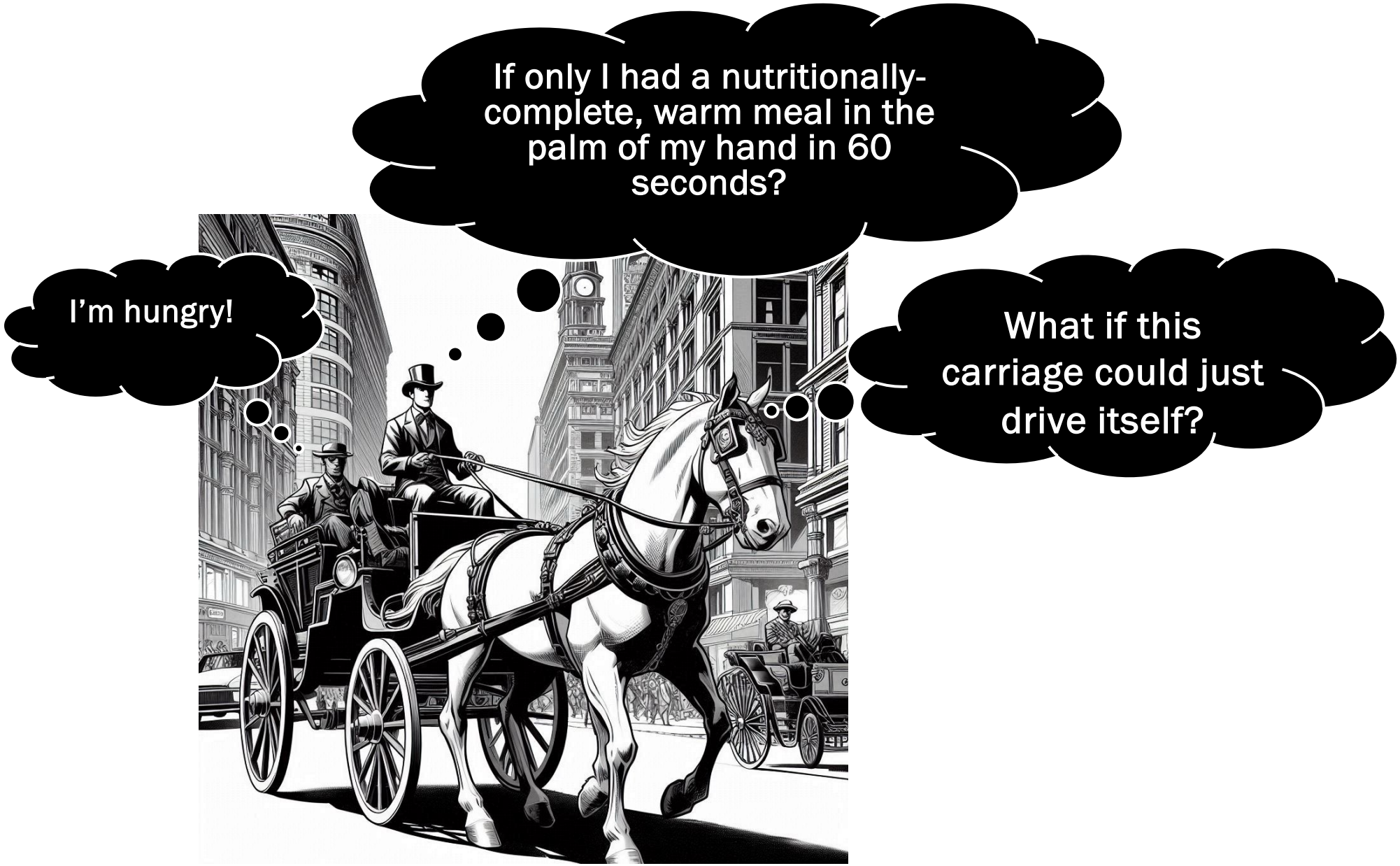
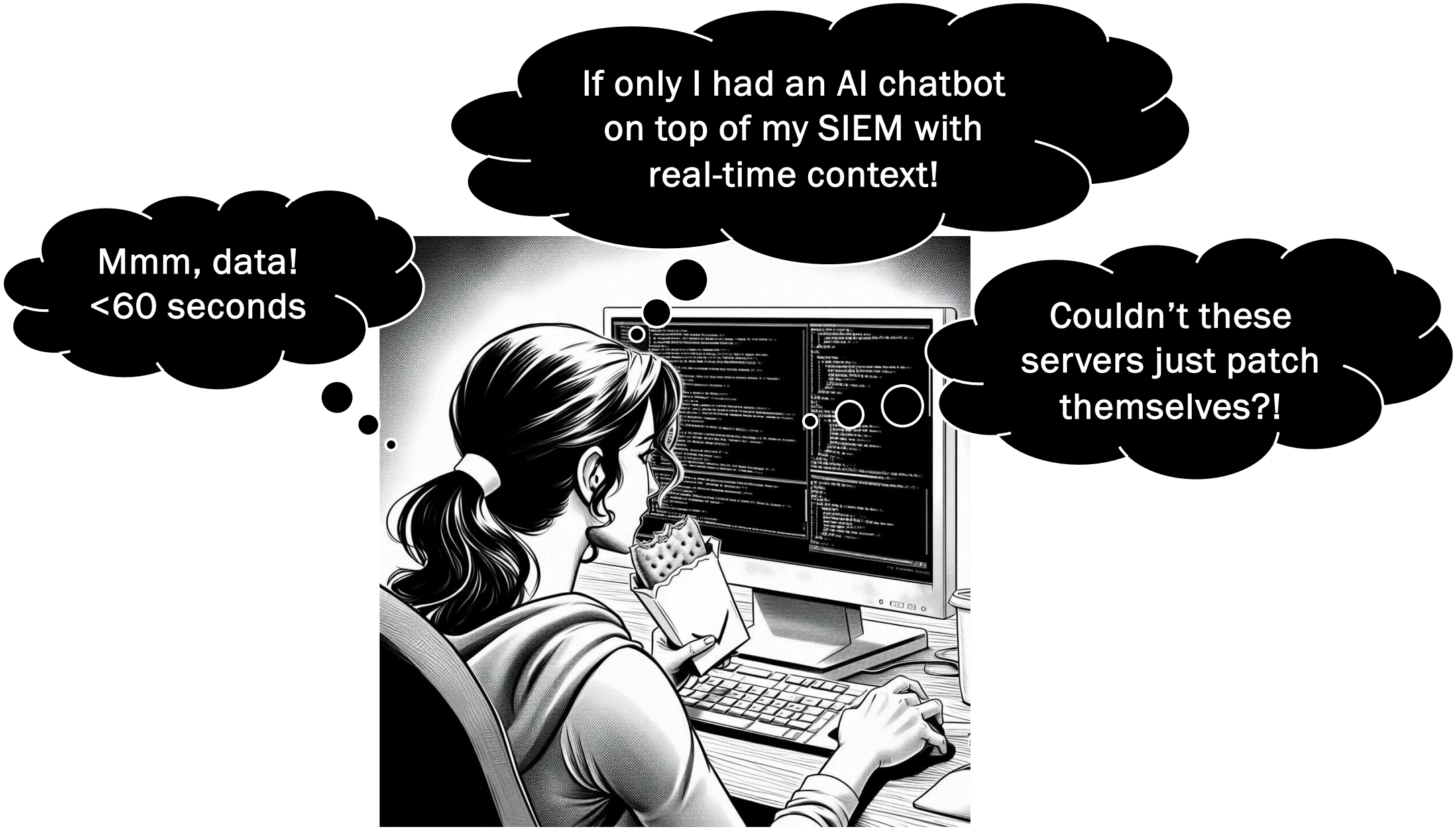

If only I had a nutritionally-complete, warm meal in the palm of my hand in 60 seconds?
I’m hungry!
What if this carriage could just drive itself?


If only I had an AI chatbot on top of my SIEM with real-time context!
Mmm, data! <60 seconds
Couldn’t these servers just patch themselves?!

AI SecOps: Autonomous Endpoint Management

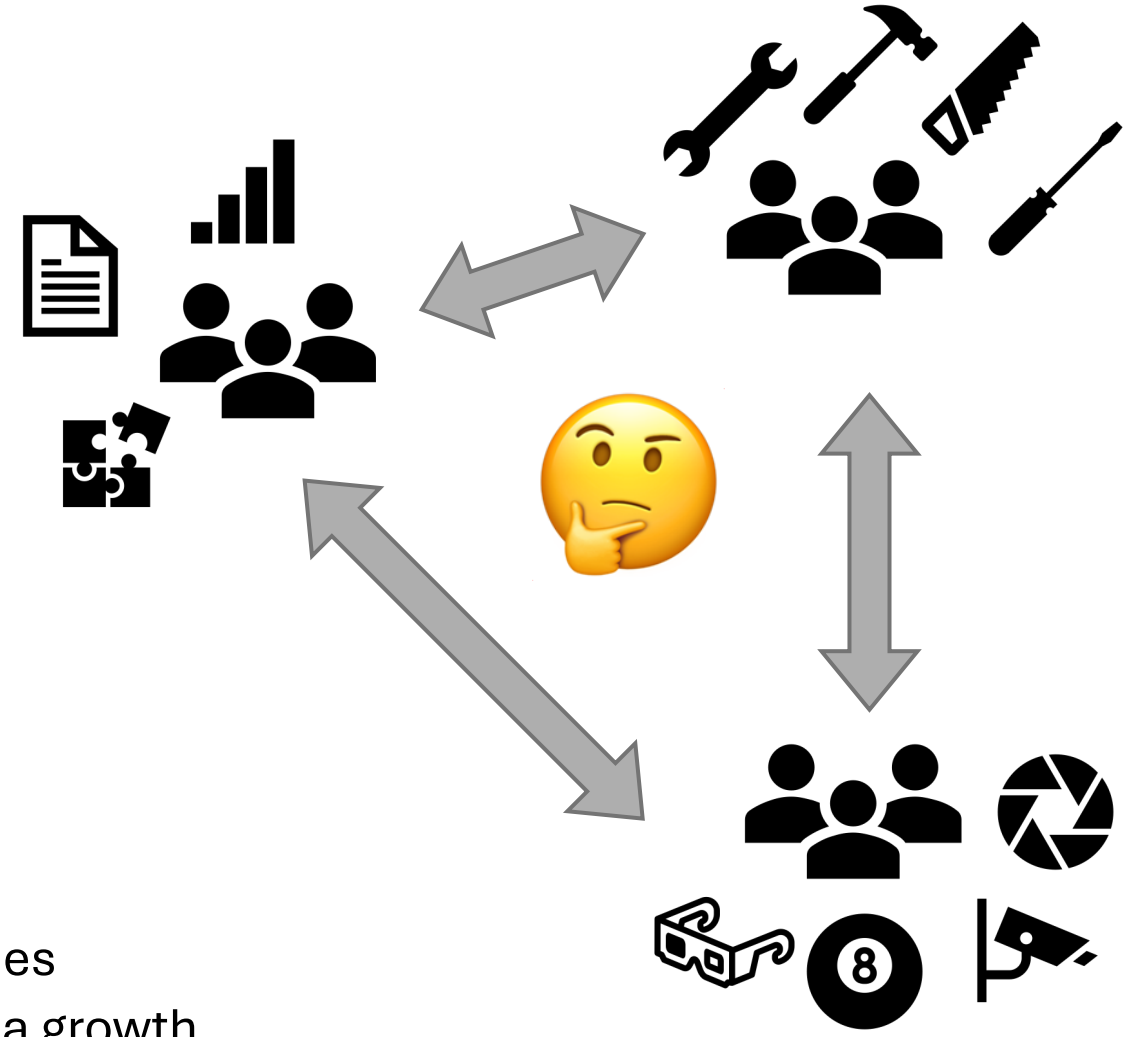
COISSA 2024
Ashley McGlone
Technology Strategist
Tanium

LinkedIn

Challenges Today

People

- Skills gap
- Art vs science
- Smaller teams
- Unethical AI adversaries



Process

- Friction
- Manual
- Slow

Technology

- Too many tools
- Complexity
- Sprawling devices
- Exponential data growth
- Expanding attack surface

Possible Today

- Fully automated patching rings of OS and apps
- See under-performing workstations and prompt the user proactively for service or replacement
- Compare your security posture to peer companies using real data
- Scan SBOM components for vulns
- Automatic reporting & recommendations on CVE exposure and remediation
- Vulnerability management lifecycle automation
- Immediate, local remediation of endpoint CVEs without a trip to the SOAR

Dream Questions

AI SecOps: Autonomous Endpoint Management

- How can AI help me prioritize risks?
- How can AEM scale my team?
- How can I reduce manual work at scale?
- How can I speed IR?
- How can I train new security peers faster with immediate productivity?
- What if I had an AI chatbot on top of my SIEM?
- What if I could see what is happening on my endpoints right now?

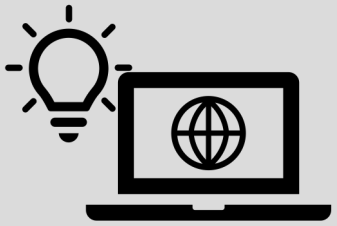
Dream Questions

AI SecOps: Autonomous Endpoint Management

- What if my ops tooling was aware of patching success rates across the industry and automatically progressed through my rings when as certain confidence scores and success rates were met?
  - Isn’t that what we do manually?
  - How much time would we save across how many teams?
- What if AI could sort through the mountain of SOC alerts, find the patterns, collect the artifacts, remediate the exploits, and close the tickets?

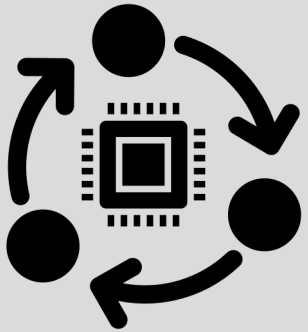
AI

DATA



Autonomous
Endpoint
Management

GLOBAL
DATA
REAL-TIME



AI
SecOps

LOCAL
DATA
REAL-TIME

Autonomous Endpoint Management

Make it easier, faster, and safer to
manage and secure your enterprise

Why AEM, Why Now?

To give teams the ultimate confidence to take
the right action at the right time in their IT environment

1.

Real-Time Endpoint Visibility

achieve decision-making superiority

2.

Control and Remediation

contextualize data into real action

3.

Autonomous Systems

intelligently automate visibility and control

Millions of Actions Every Day
Billions of Points of Real-time Data
Petabytes of Data Every Week

Scale IT and Security Execution

AI-enabled experiences enable teams to achieve maximum cyber hygiene and compliance

Quicker high-confidence decisions

Intelligent high resilience automation

High fidelity governance

Autonomous Capabilities Dashboard

Insights

Confidence scores from actions globally
Prioritized recommendations

Actions

Orchestrate actions & remediations
Ring-based phased rollout

Oversight

Centralized tracking
Automation controls

Foundational Elements

Orchestration engine | Real-time global data | Multi-vector intelligence

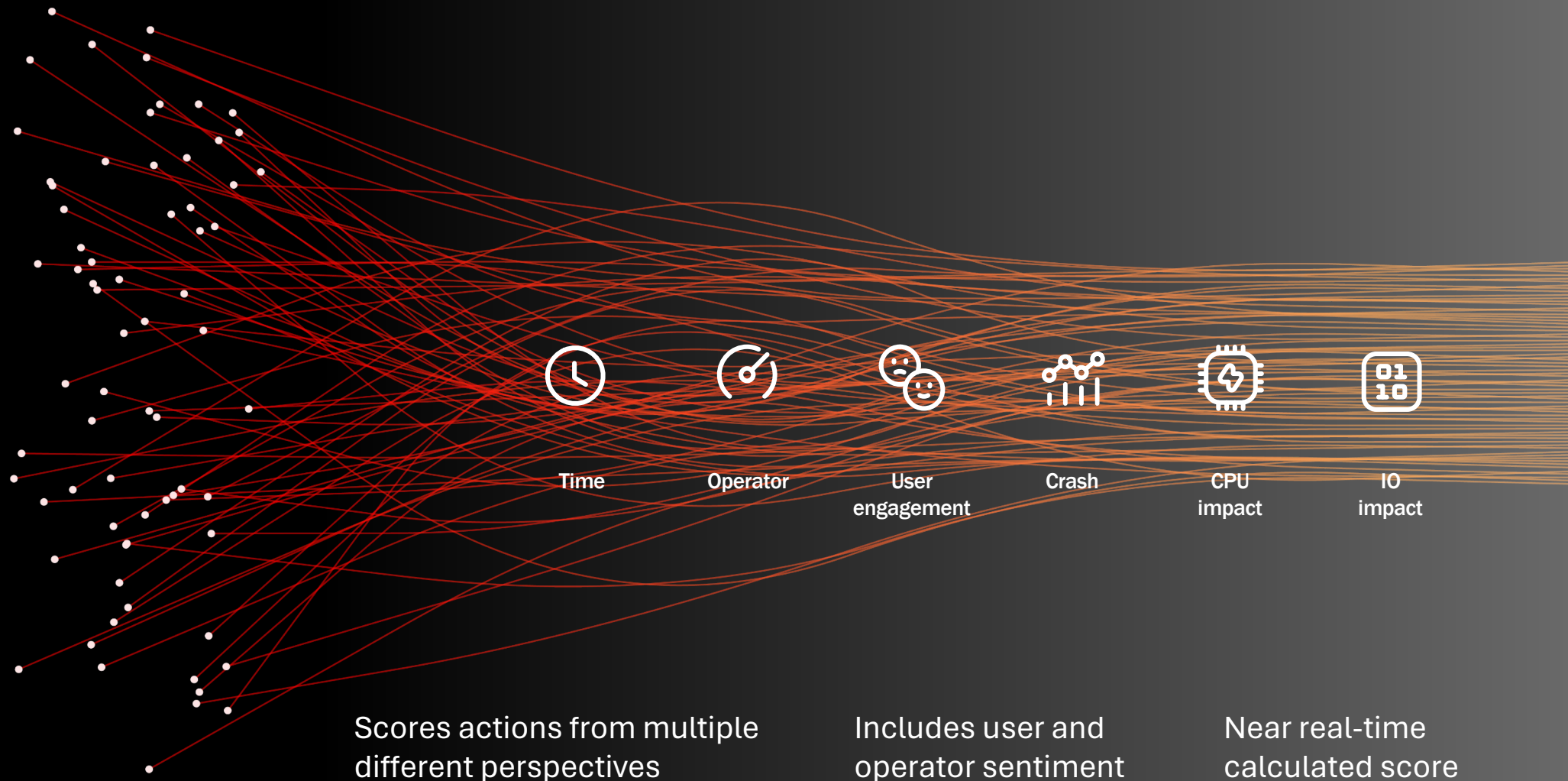
You remain in control.

Trust Considerations

The user is always in control.

- How do you build trust with an autonomous vehicle? At what point do you take your hands off the wheel? Or do you at all? (*real-time data is essential*)
- We are overwhelmed and under-staffed. At what point do we let the machines run the place? Or at least assist?
- How do you build trust with autonomous infrastructure and security management?
- How can I avoid disruption and ensure success?
- Recommendations > Confidence Score > *Human Review & Approval* > Autonomous Remediation

AEM Confidence Score Dashboard



Scores actions from multiple different perspectives

Includes user and operator sentiment

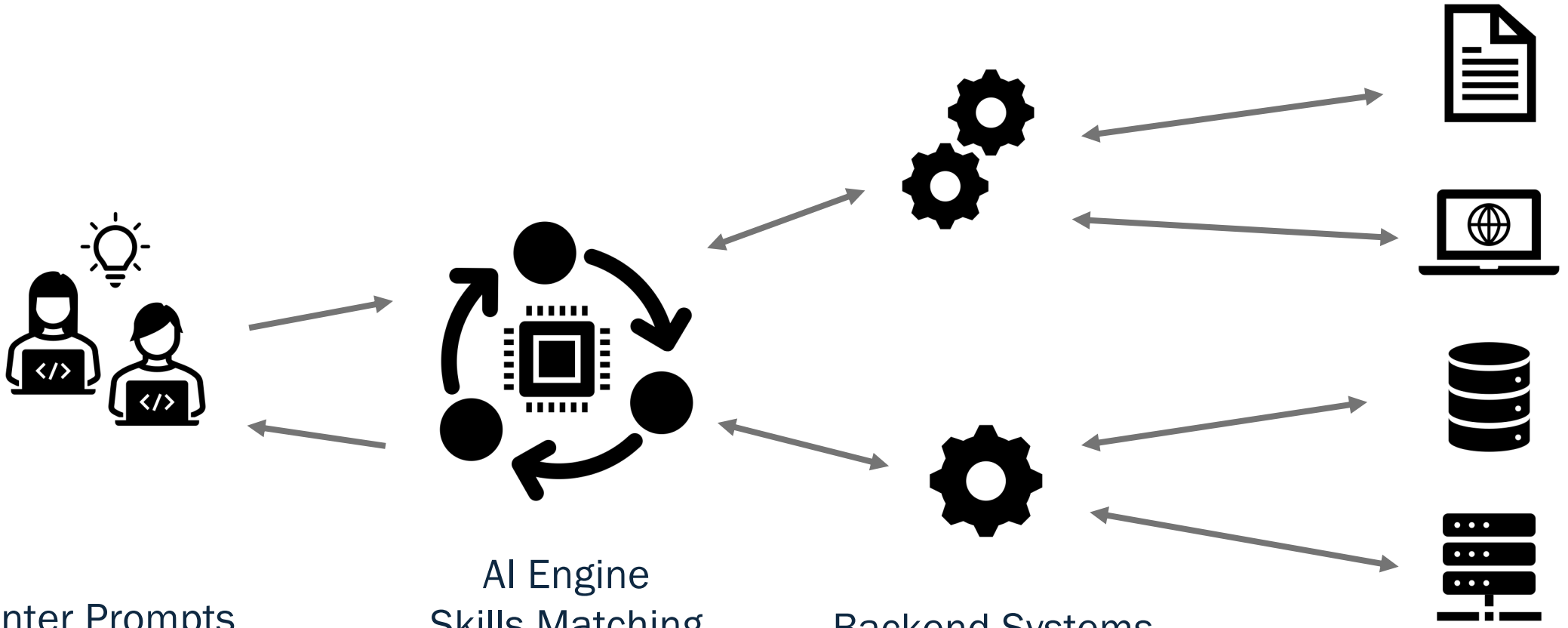
Near real-time calculated score

AI-Powered SecOps

Delivering better outcomes for
Security Analysts & Incident Responders

AI SecOps Architecture

Conversing with your SecOps data sources from a single interface



Enter Prompts

Return Outputs

AI Engine
Skills Matching
Send request
Receive data
Collation AI Magic

Backend Systems
API Integrations
Automated Tooling

Data Sources

AI SecOps

Delivering better outcomes for Security Analysts & Incident Responders

Structured queries

Run complex queries using natural language

Assess security posture of devices

Enrich alerts and incidents

Upskill teams via prompts and recommendations

Analyze malicious scripts / author remediation scripts

Gain access to arbitrary real-time endpoint data & accelerate Threat Hunting and Incident Response

Identify vulnerable OSs, software, & libraries

Identify activities related to a compromised user

Zero-day vulnerability reporting

Real-time remediation in minutes

AI SecOps: Arming defenders with the data you need

- Vulnerability Management focused skills (Zero-day or routine vulnerability scenario):
  - Systems vulnerable to a CVE
  - Versions of software on systems (SBOM)
  - Systems with software version (SBOM)
- Incident Response focused skills (Investigating a Security Breach):
  - Processes (exe hash, app name) that ran as user on computers
  - Process and User associated with network connection to (IP address)
  - Hosts and Users associated with a suspicious process
  - Unique hashes for an application version's process
  - Investigate vulnerable processes, child processes, and network connections

- Surface Suspicious Activities
- Extend Incident Response scenarios:
  - Service Status & Details
  - Active Open ports (listening)
  - Outliers (e.g. <5% endpoints)
  - Correlation of Processes to Network activity
  - File details, handles, open files
  - Registry keys & autoruns
  - User logins / history
  - Process execution trees
- Flexible real-time actions on Endpoints

What if I could ask AI things like…

- Show me all the machines without BitLocker encryption enabled.
- Write a PowerShell script to set this registry value and delete these two files that could be in one of three locations.
- Show me every every laptop connected to an unencrypted WiFi network.
- List every endpoint that has vulnerability CVE-2023-24880, and then show why is it vulnerable.
- Show all processes connected to IP address 104.16.35.39, and then quarantine the endpoint.
- Show me all endpoints with a file create event for C:\Windows\Temp\badware.exe in the last two weeks.
- Write all this up in a report for my manager!

Protect at the speed and scale of AI

Enable response in minutes,
not hours

Simplify the complex with natural
language prompts and easy reporting

Catch what others miss with deeper
understanding of your enterprise

Strengthen team expertise
with cyber skills and promptbooks

AI-Powered SecOps: elevating your security program

Outpace adversaries

- Less time spent on low-value repetitive tasks
- Accelerated detection and response
- Critical context on incidents at analysts' fingertips

+

Strengthen team expertise

- Junior analysts performing more advanced tasks
- Human expertise redirected to the hardest problems
- Guidance on processes to drive consistency

=

Defend at machine speed and scale

- Reduction in mean time from detection to response
- Shift from reactive to proactive tasks
- Better understanding of risk for strategic improvements

Considerations for security, privacy, and compliance.

Keep your data as your data

Ensure your data is not used to train the foundation AI models

Your data posture should satisfy enterprise compliance and security controls

NIST AI Risk Management Framework

https://www.nist.gov/itl/ai-risk-management-framework

Fig. 2. Lifecycle and Key Dimensions of an AI System. Modified from OECD (2022) OECD Framework for the Classification of AI systems — OECD Digital Economy Papers. The two inner circles show AI systems' key dimensions and the outer circle shows AI lifecycle stages. Ideally, risk management efforts start with the Plan and Design function in the application context and are performed throughout the AI system lifecycle. See Figure 3 for representative AI actors.

5. AI RMF Core

The AI RMF Core provides outcomes and actions that enable dialogue, understanding, and activities to manage AI risks and responsibly develop trustworthy AI systems. As illustrated in Figure 5, the Core is composed of four functions: **GOVERN, MAP, MEASURE,** and **MANAGE**. Each of these high-level functions is broken down into categories and subcategories. Categories and subcategories are subdivided into specific actions and outcomes. Actions do not constitute a checklist, nor are they necessarily an ordered set of steps.

Fig. 5. Functions organize AI risk management activities at their highest level to govern, map, measure, and manage AI risks. Governance is designed to be a cross-cutting function to inform and be infused throughout the other three functions.

Career Impact?

This is an old story. Same song. 47th verse.

"AI won't take your job. It's somebody using AI that will take your job."

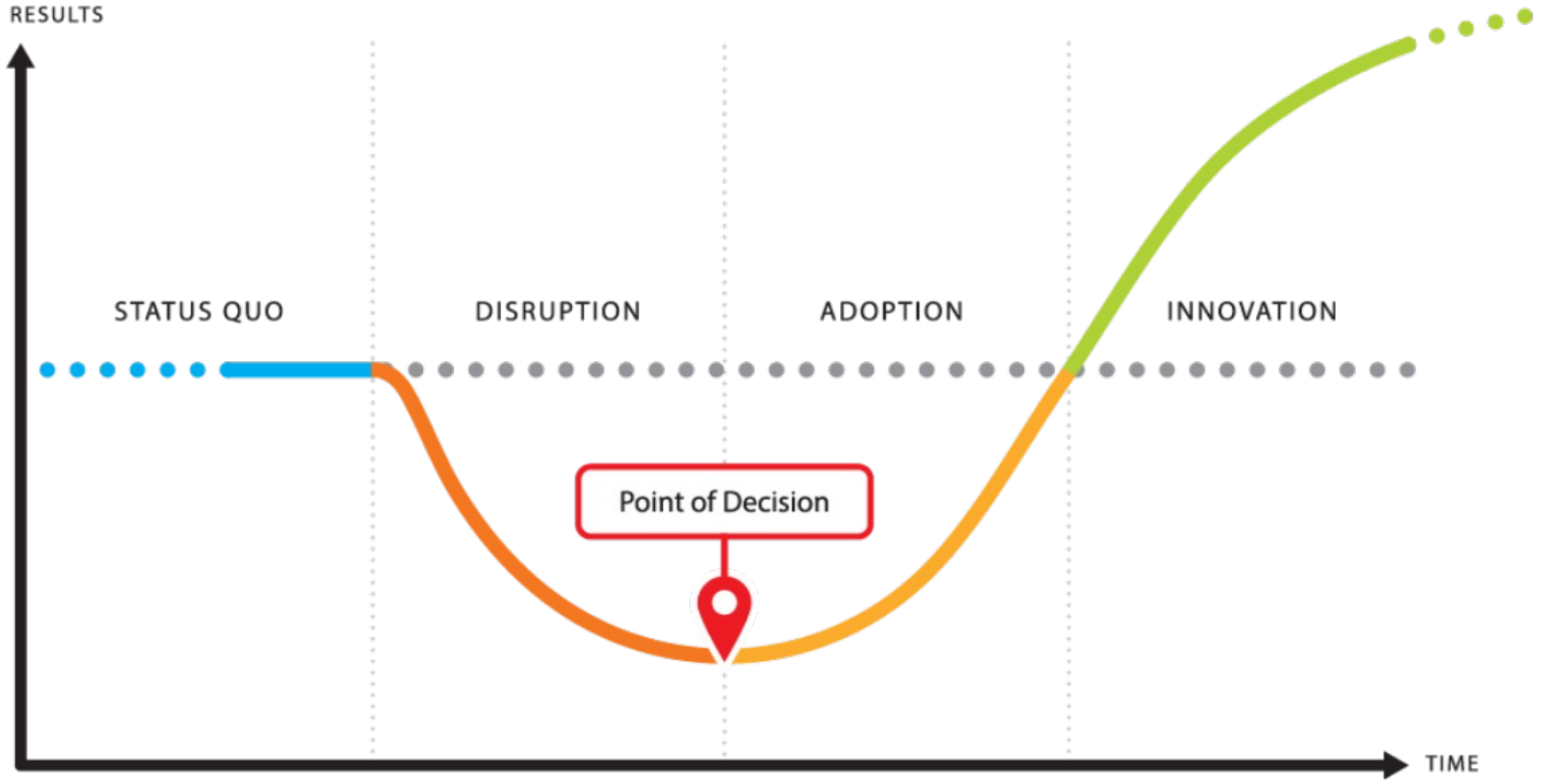
Richard Baldwin

Economist and professor, Geneva Graduate Institute, Switzerland

2023 World Economic Forum - Growth Summit

Franklin Covey Change Model

My company. My career.



What can I do?

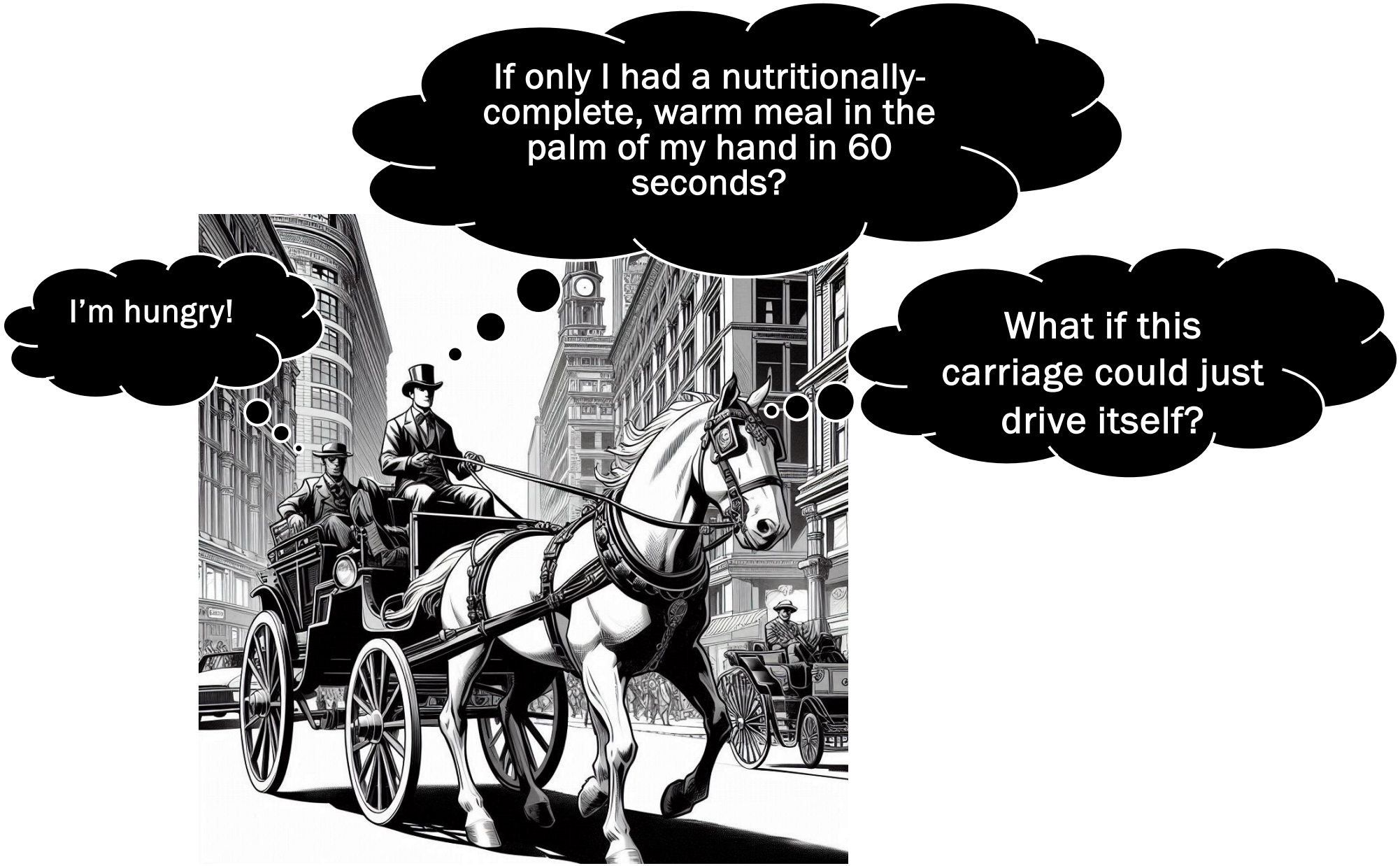
- Building detection rules for new threats
- Building visualizations for reporting capabilities
- Upskilling threat hunting skills for major incidents
- Building automations for incident response and remediation
- Identifying alert tuning opportunities and resolving them via automation
- Performing configuration reviews for security platforms
- Investing in engineering skills to build integrations

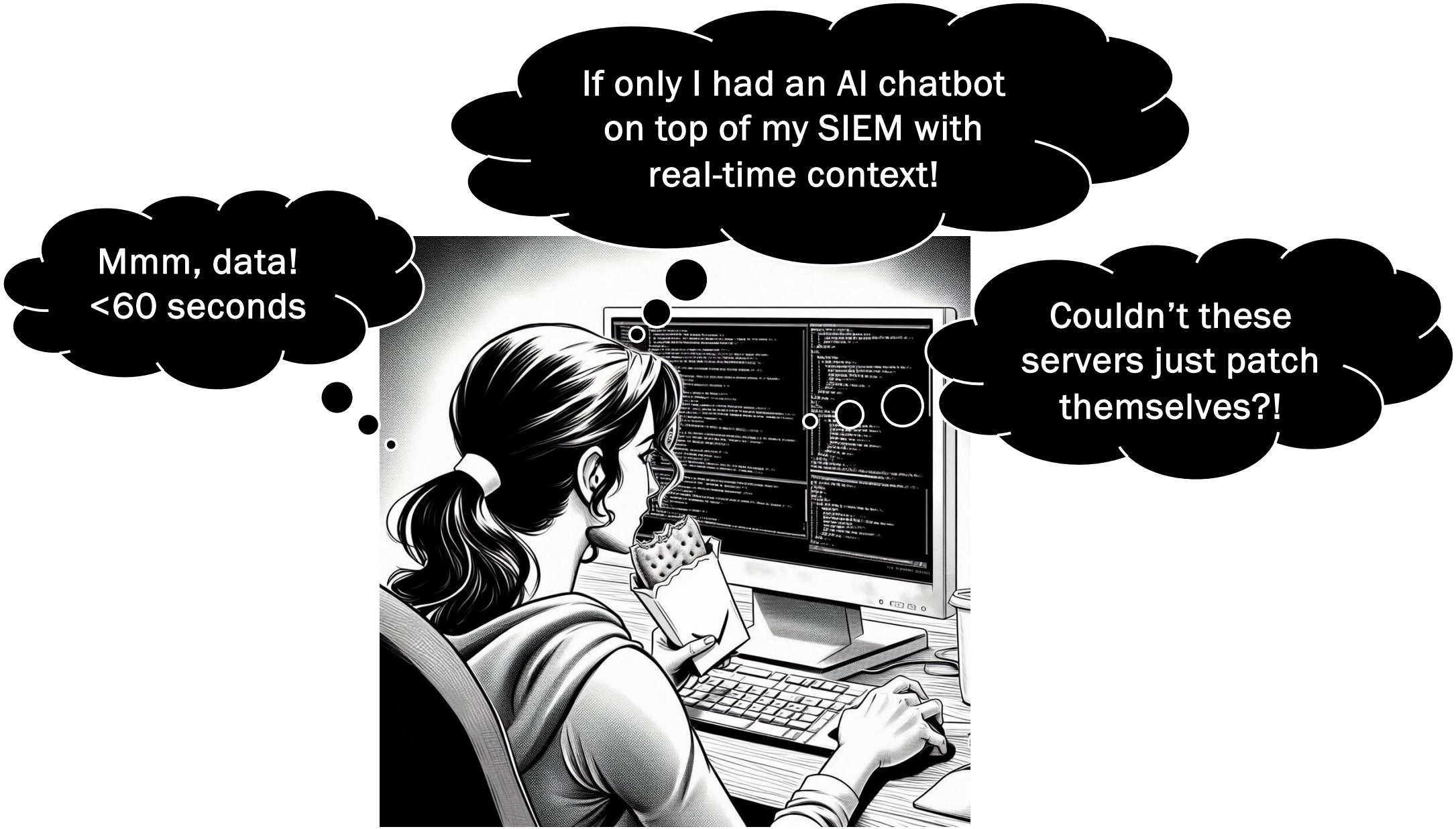
Debac Manikandan
Senior Cybersecurity Engineer
Will it replace a SOC Analyst?

Call To Action

AI SecOps: Autonomous Endpoint Management

- What flavor Hot Pocket do you want?
- Career Opportunity: What did the horseshoe blacksmith do? Ride the wave of this new tech to build your brand and become the answer person for how to build prompts, write skills for matching on the backend, and leverage your SecOps knowledge into the model.
- What can you automate today? (ex. automatic quarantine of risky endpoints)
- How can you leverage the LLM of your endpoint data for insights into SecOps?
- What is the low-hanging fruit for autonomous endpoint management and security in your environment and team?
- What entry-level autonomous actions would you begin with to build trust?
- What factors would you consider in creating a confidence score for patching or remediation based on industry telemetry?
- Form an AI SecOps dream team to start working through governance decisions and charting a roadmap for exploring these capabilities.


If only I had a nutritionally-complete, warm meal in the palm of my hand in 60 seconds?
I’m hungry!
What if this carriage could just drive itself?


If only I had an AI chatbot on top of my SIEM with real-time context!
Mmm, data! <60 seconds
Couldn’t these servers just patch themselves?!

Optional Resources

https://github.com/GoateePFE/TaniumResources

https://www.linkedin.com/in/ashleymcglone