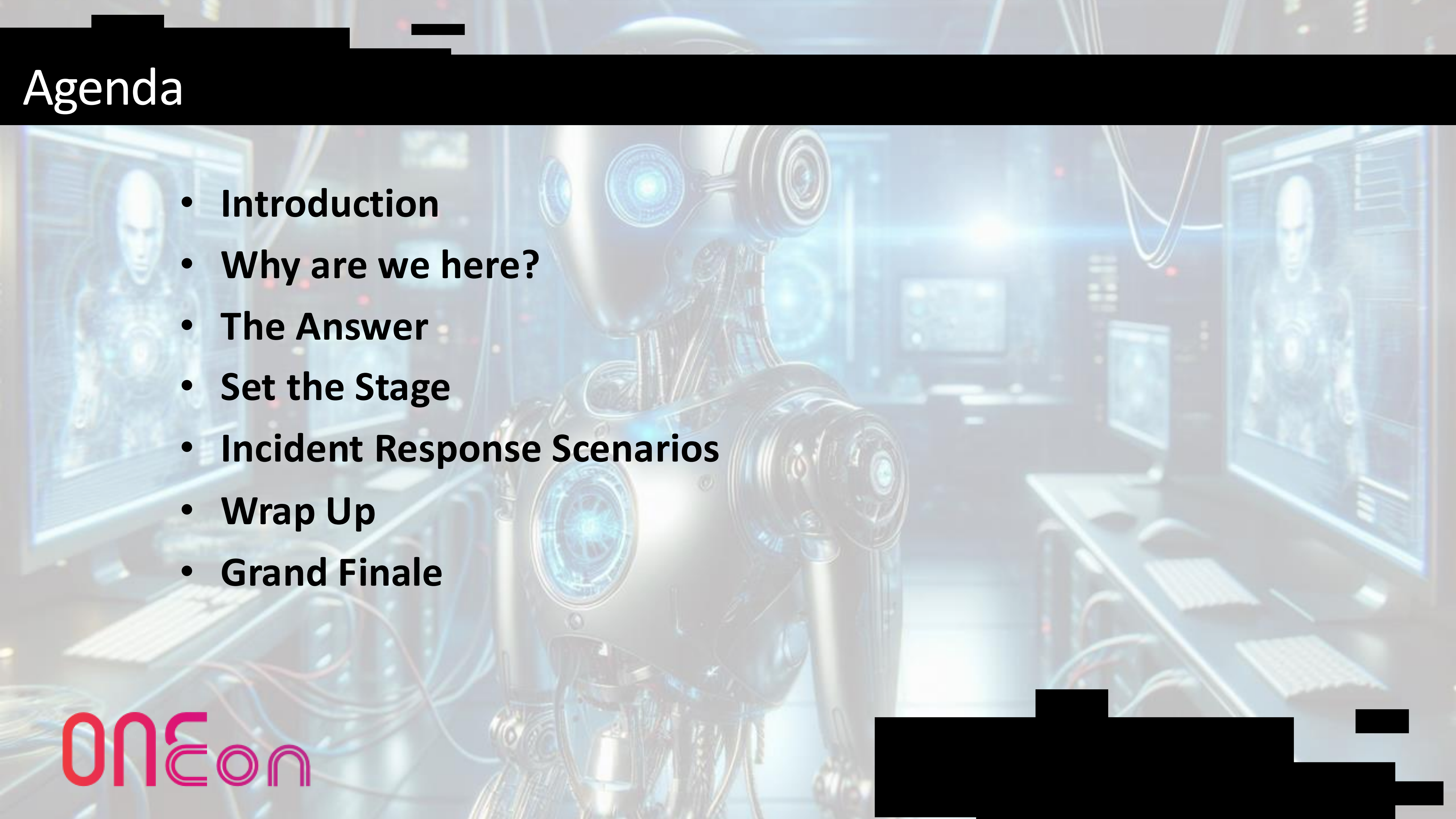
Incident Response Workshop

ONEcon

Agenda



- Introduction
- Why are we here?
- The Answer
- Set the Stage
- Incident Response Scenarios
- Wrap Up
- Grand Finale

Speaker Intro

Natalie Suarez

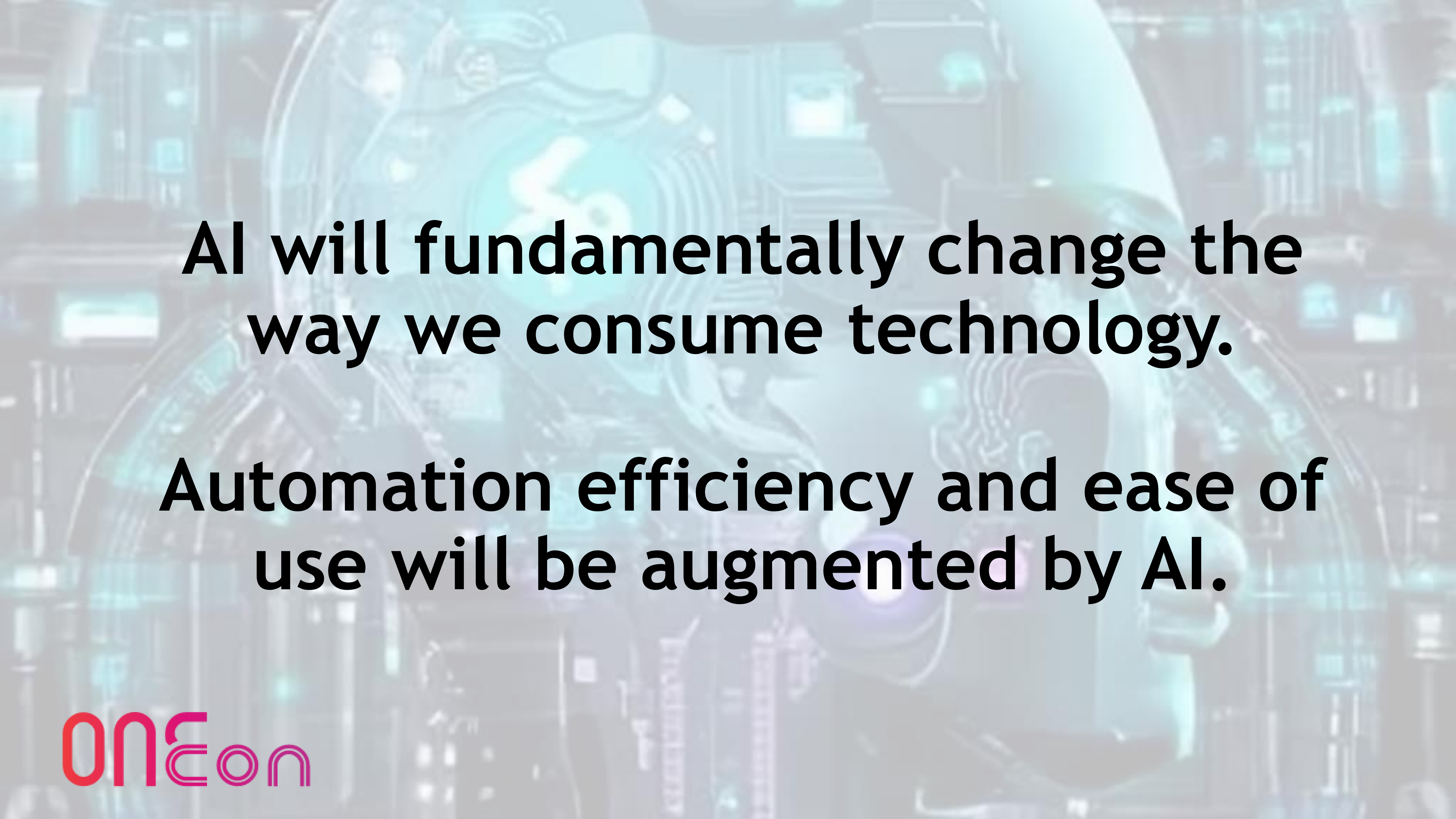
Principal Solutions Advisor

- 2023 CRN® Channel Chief
- 25+ years in IT and Cybersecurity
- Began career as a software developer
- Supported Department of Defense Intelligence analysts
- ConnectWise Certify Instructor
- Speaker at Industry Events
- Co-chair, CompTIA ISAO Executive Steering Committee
- Launched the IT Nation Evolve™ Cybersecurity Peer Groups
- Passionate about my family, threat intelligence, and LEGO™
- Bachelor of Science, Computer Engineering, magna cum laude

ONEcon

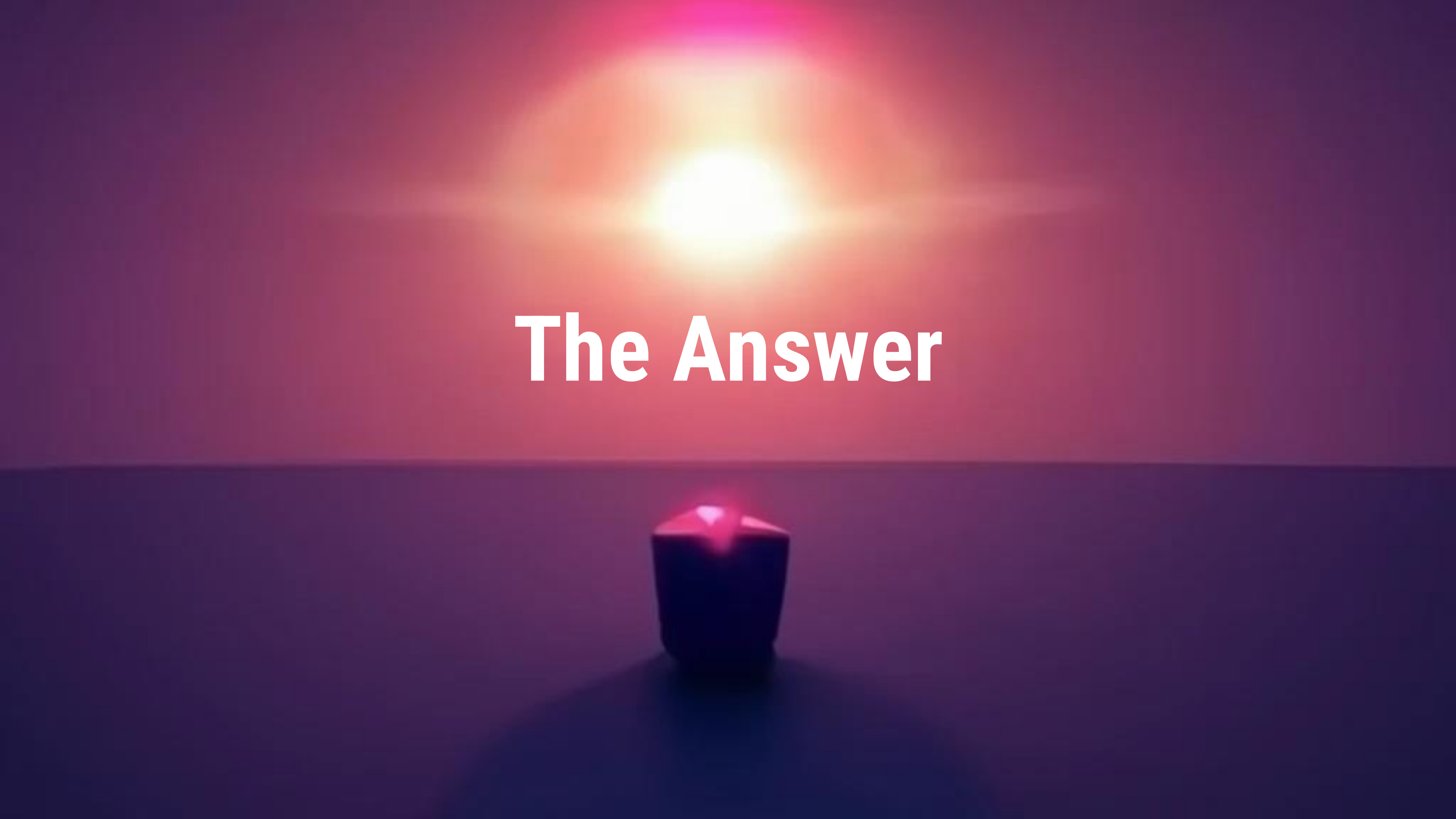
CONNECTWISE

Why Are We Here?



AI will fundamentally change the way we consume technology.

Automation efficiency and ease of use will be augmented by AI.

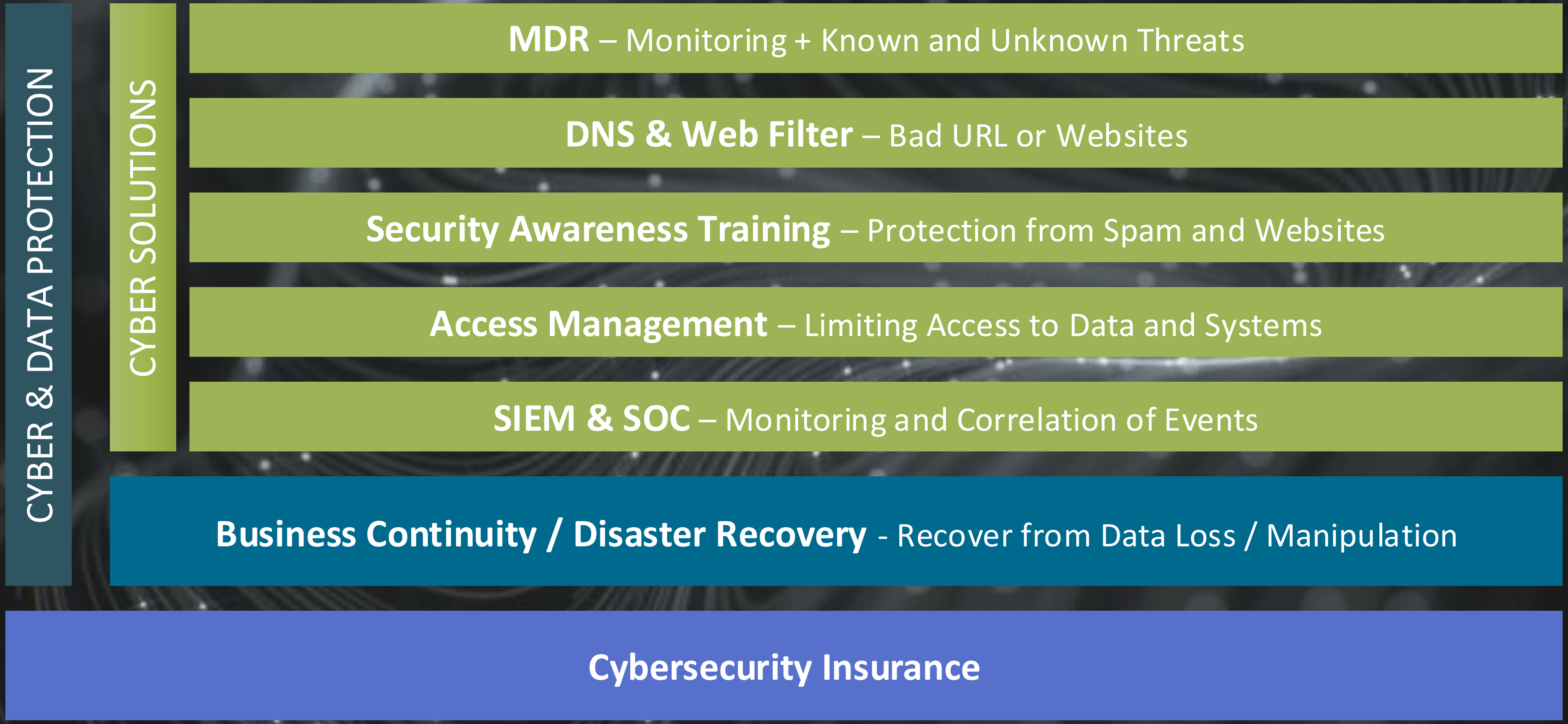


The Answer

PEOPLE	PROCESS	TECHNOLOGY		CAPACITY OUTCOMES
○	○	○	→	No Defense
●	○	○	→	No ability to execute
○	●	○	→	Wasted effort
○	○	●	→	Shelf-ware
●	●	○	→	Burden to scale
●	○	●	→	Inconsistent operation
○	●	●	→	Poor adoption
●	●	●	→	**Success**

ONEcon

Building a Layered Defense



CYBER & DATA PROTECTION

CYBER SOLUTIONS

MDR – Monitoring + Known and Unknown Threats

DNS & Web Filter – Bad URL or Websites

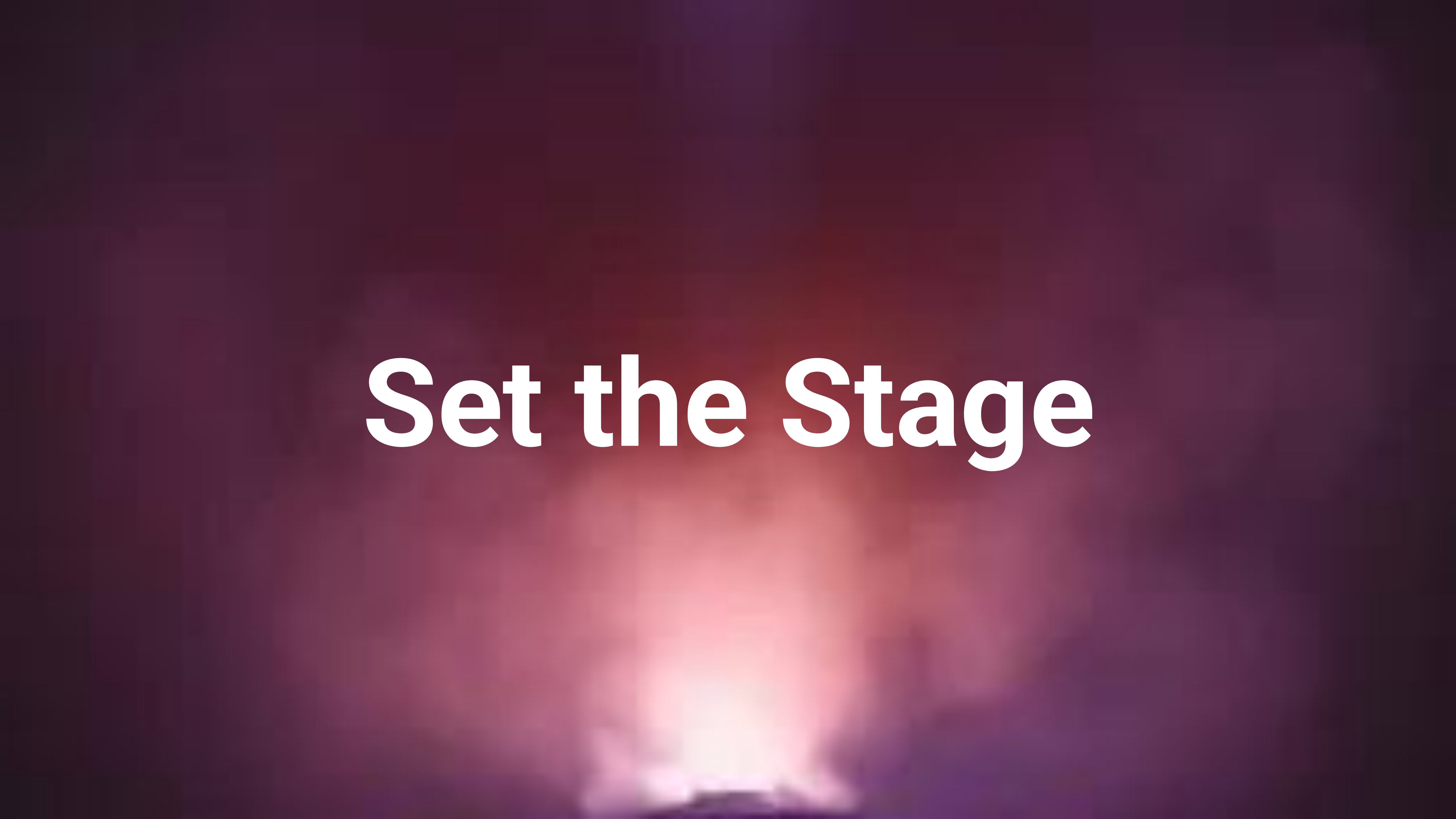
Security Awareness Training – Protection from Spam and Websites

Access Management – Limiting Access to Data and Systems

SIEM & SOC – Monitoring and Correlation of Events

Business Continuity / Disaster Recovery - Recover from Data Loss / Manipulation

Cybersecurity Insurance



Set the Stage

What is a Tabletop Exercise (TTX)?

- Facilitated discussion of scripted scenarios
- Conducted in an informal, stress-free environment
- Based on current applicable policies, plans and procedures
- Establishes an environment for problem solving

Ground Rules

- No judgement
- Confidentiality – Protect your proprietary information, share only what you feel comfortable sharing in a group setting
- Participate in all group conversations
- Give everyone a place to speak – this is about learning, not about always being right
- Listen to the group insight and apply it to your organization

Tabletop Setup

- You will be presented with various AI-centric scenarios.
- We will provide the overview and discuss how you would respond.
- Group discussion
- We are available to assist with any questions or discussion during the exercise

ONEcon

Incident Response Scenarios

Scenario – Copyright Infringement

- You’ve been served!
- The allegations are Copyright Infringement
- A staff member has used copyrighted images in a publication advertising an event for your business.
- Getty images litigation
- Obtained thru a GPT

ONEcon

Scenario 2 – Loss of Intellectual Property

- Your competitor beats you to market on a novel non-surgical cure for an eye lift to repair hooded eyes and remove bags.
- The solution is remarkably close, even identical to the research and testing you’ve been funding in your Los Álamos lab.
- Lab staff was using AI to write/publish findings.

Scenario 3a – Deep Fake Video

- A deep fake of your CEO announcing the merger of your business with a similar business with a terrible reputation is making the rounds while you are trying to secure VC funding/about to IPO.

ONEcon

Scenario 3b – Deep Fake Audio

- You are in the financial industry and have called a client to confirm a pre-arranged financial transfer of $100k US.
- You have used the correct phone number from your contacts, verified all pertinent information, and sent an MFA-like PIN code to their registered device. They successfully confirmed their identity.
- As per your firm's funds transfer policy, you confirm the required wire transfer details with the client. The client states the information is incorrect. You update the information per the client’s instructions and complete the wire before the close of business Friday afternoon.
- The customer calls you back in 2 business days and asks what happened to the wire transfer you discussed. The funds have been withdrawn from the origin account. However, no corresponding deposit has been posted to the destination account.
- You’ve both been audio-jacked and now the funds have been transferred to an unknown threat actor.

Audio-jacking: Using generative AI to distort live audio transactions (securityintelligence.com)

ONEon

Scenario 4 – Reputation Damages

- You receive hundreds of fake Tech Giant business reviews with a few 1-star reviews here and there. You notice that you are starting to receive more and more 1-star reviews, some state you are offering money for 5-star reviews.
- The reviews seem to be AI-generated. They all contain similar content and were posted within the last 2 weeks.
- You appeal as many reviews as possible and are successful in having the 1-star reviews about compensation removed.
- You are terrified that this is going to turn into some type of extortion scheme.

Hundreds of fake reviews - mostly positive - Google Business Profile Community

ONEcon

Scenario 5 – Reputation Damages

- An article including allegations of <something bad> have appeared on a reputable trade association website.
- Although the article appears genuine, it was in-fact generated by AI with enough truth to sound plausible.

ONEcon

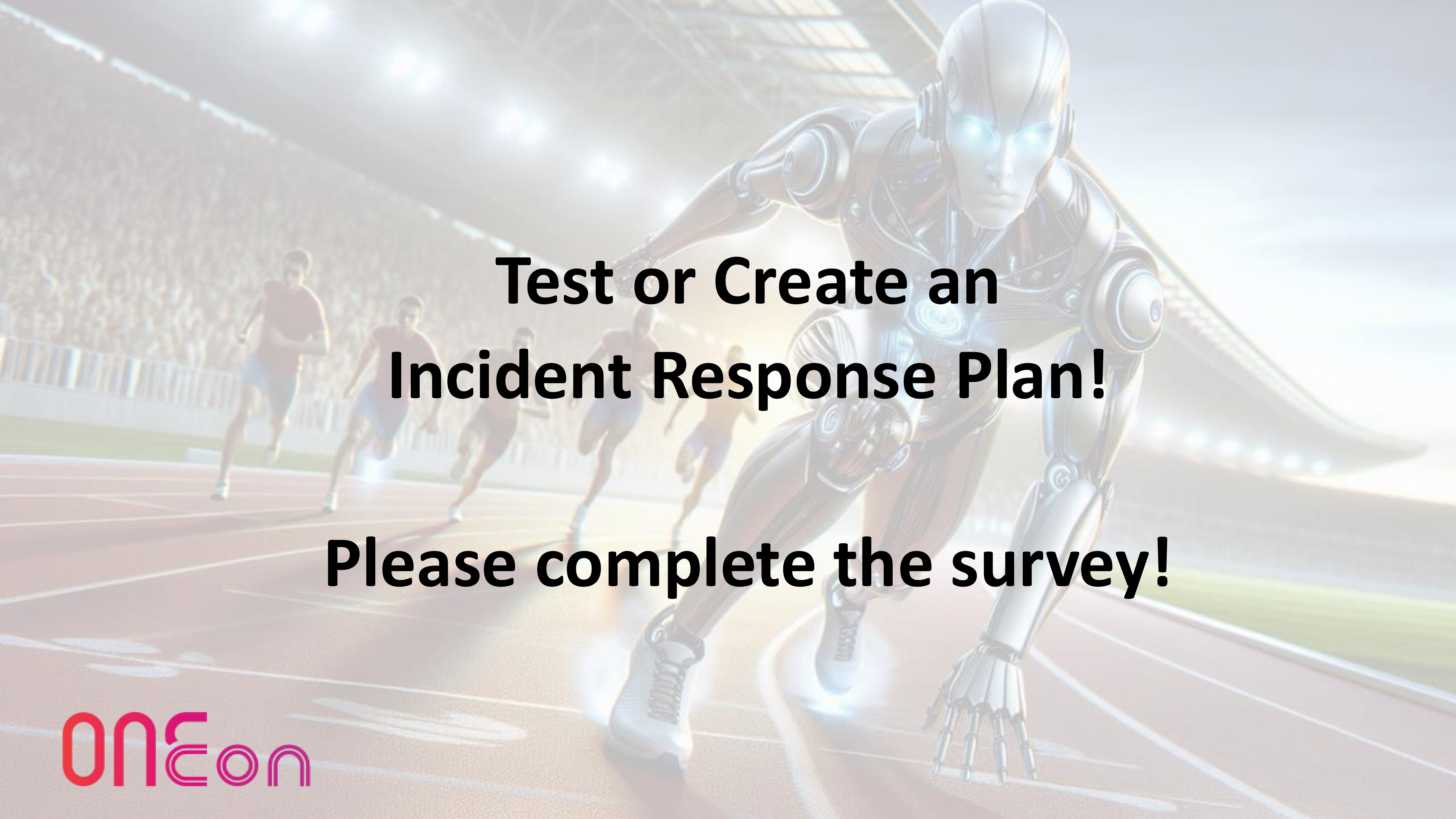
ONEon

After Action Report

1. How would you assess and adjust following the incident?
2. How do you mitigate and prevent the incident from occurring again?
3. How would you change the way you plan and prepare for an incident?
4. What changes are you going to make to your incident response plan?
5. Do you make changes to your Security Awareness Training?
6. Do you need additional policies and procedures to mitigate risk?

ONEon

ONEon



Test or Create an Incident Response Plan!

Please complete the survey!

ONEcon

Q&A

Thank you