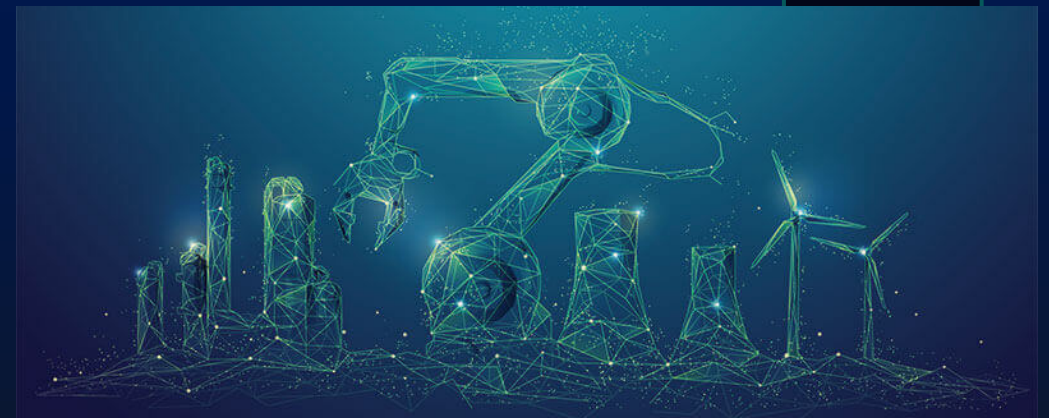


BUILDING A RESILIENT AI-OT SOC STRATEGY

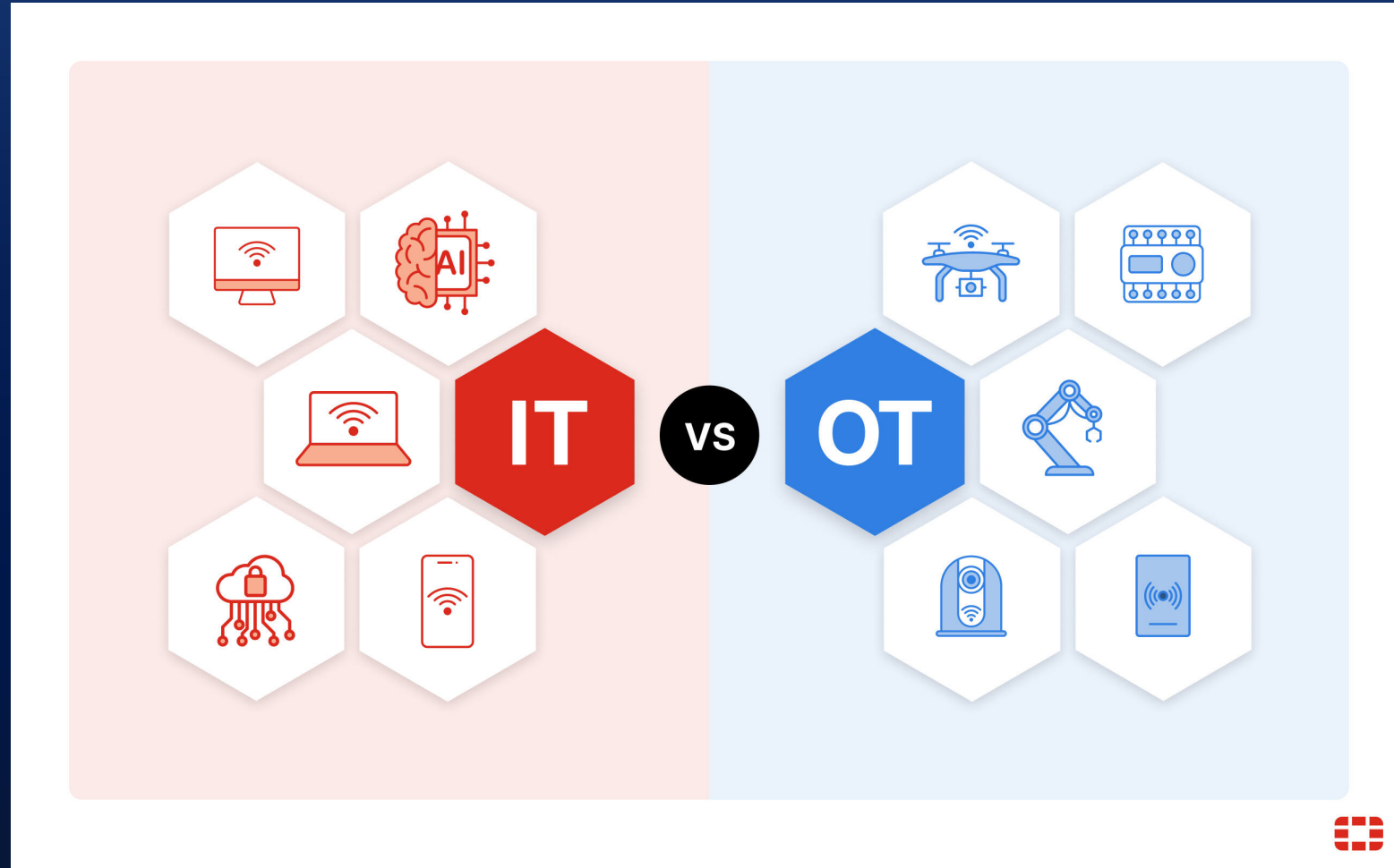
Rich Springer, Sr. Director
Product Marketing, OT Solutions
Fortinet, Inc.



- Rich Springer | Sr. Director of Product Marketing, OT Solutions



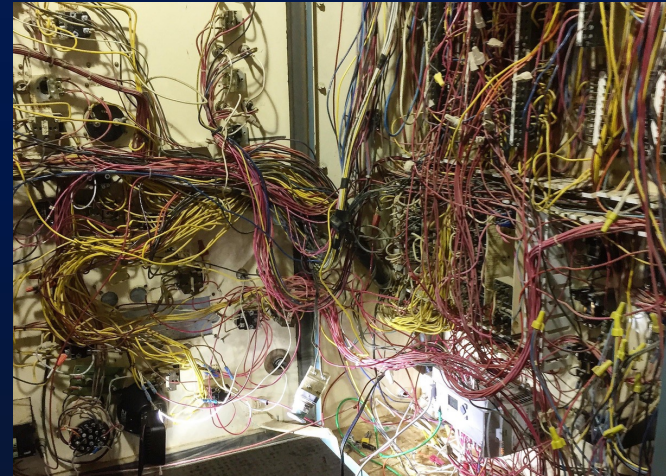
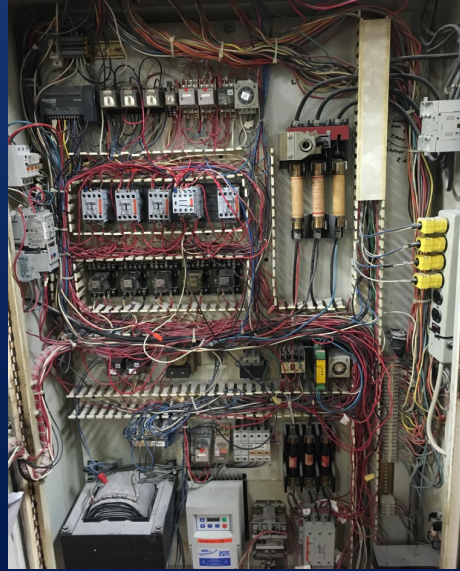
IT and OT ARE Different



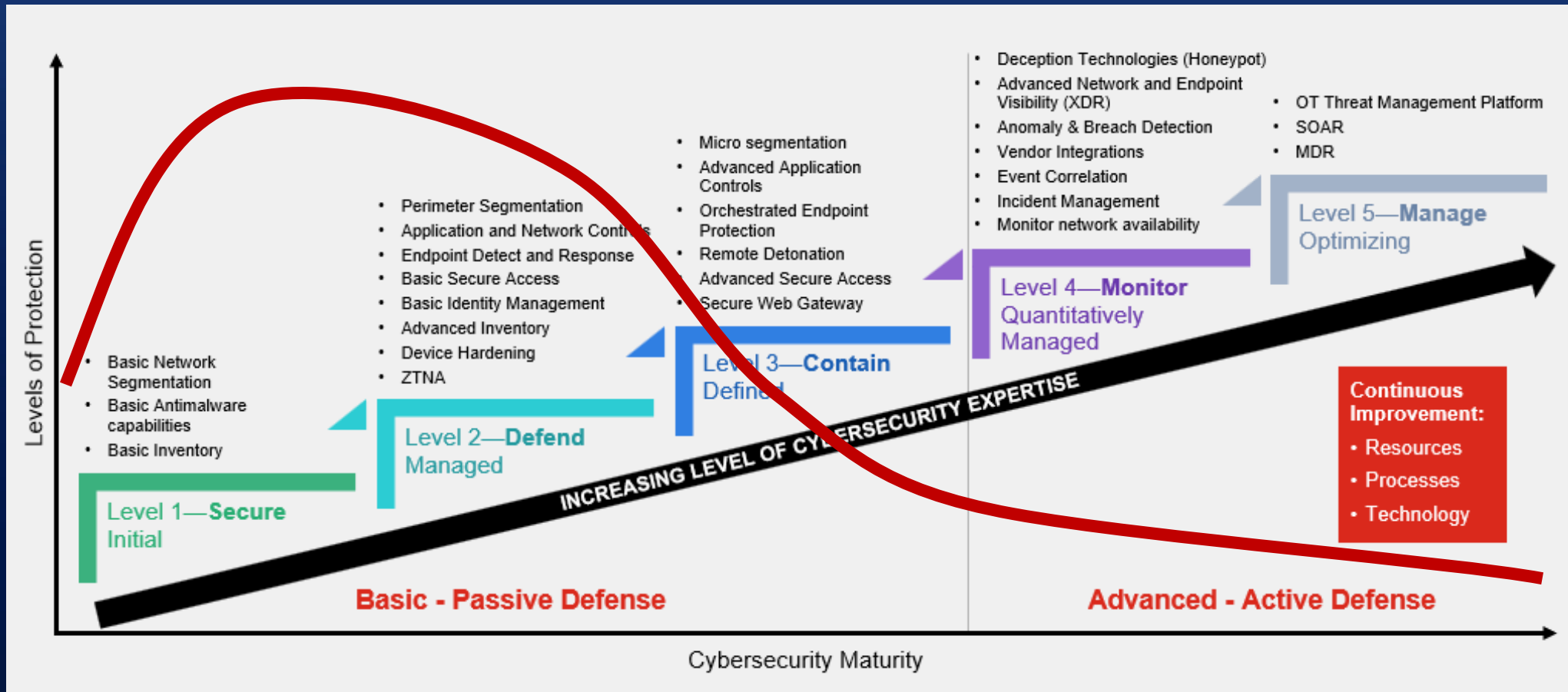
IT and OT People ARE Different



OT Devices are also a little Different



OT Focus is on the Basics: Requires Serial Progression to Maturity



What about the SOC People Skillset?

**4.7 Million unfilled cyber jobs
10x or 100x the deficit in OT?**



IT/OT SOC Response, or Lack There of



OT SOC & Operations Analyst: Mythology?



Now, We Understand the Challenge

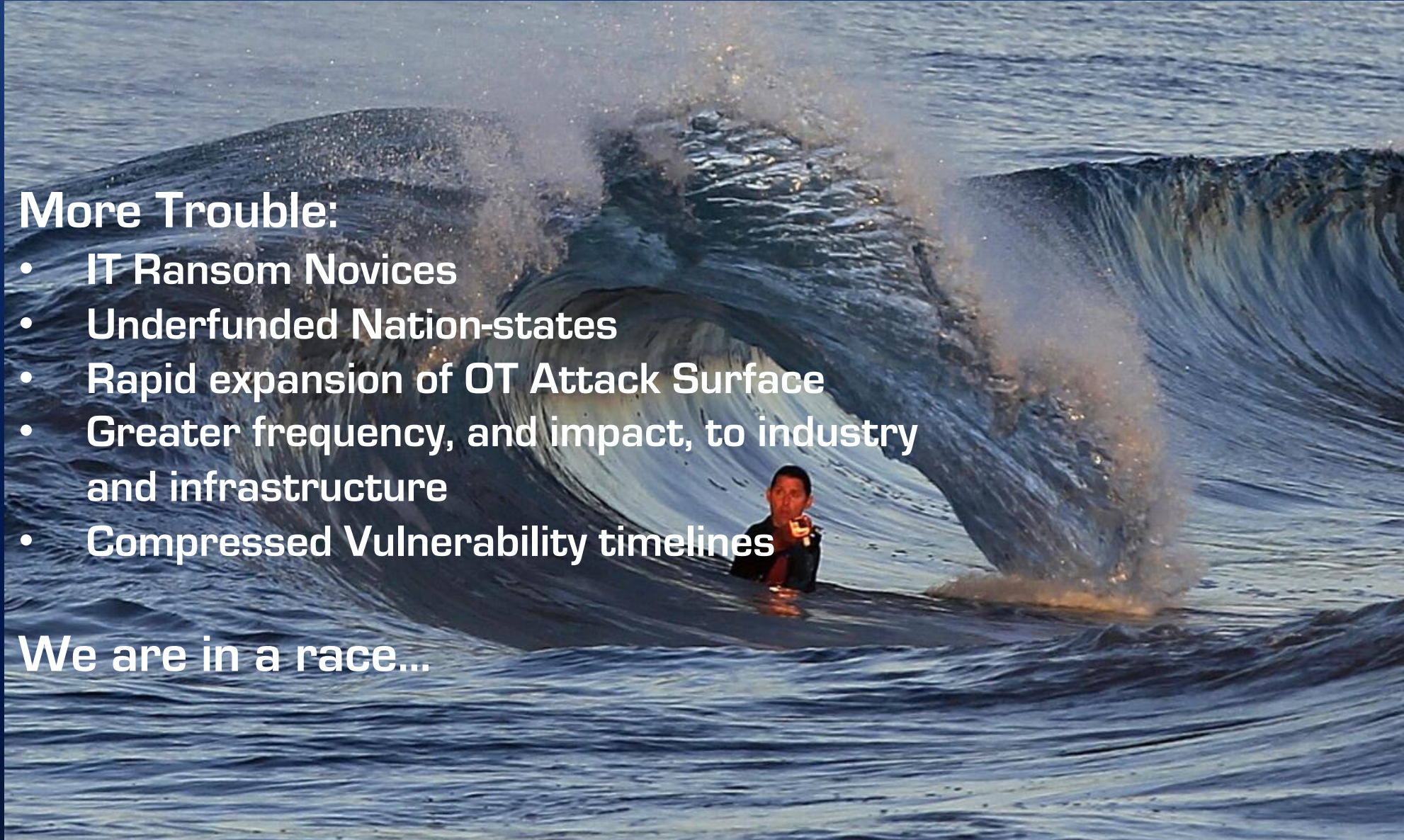


Meanwhile, AI will Enable Additional OT events

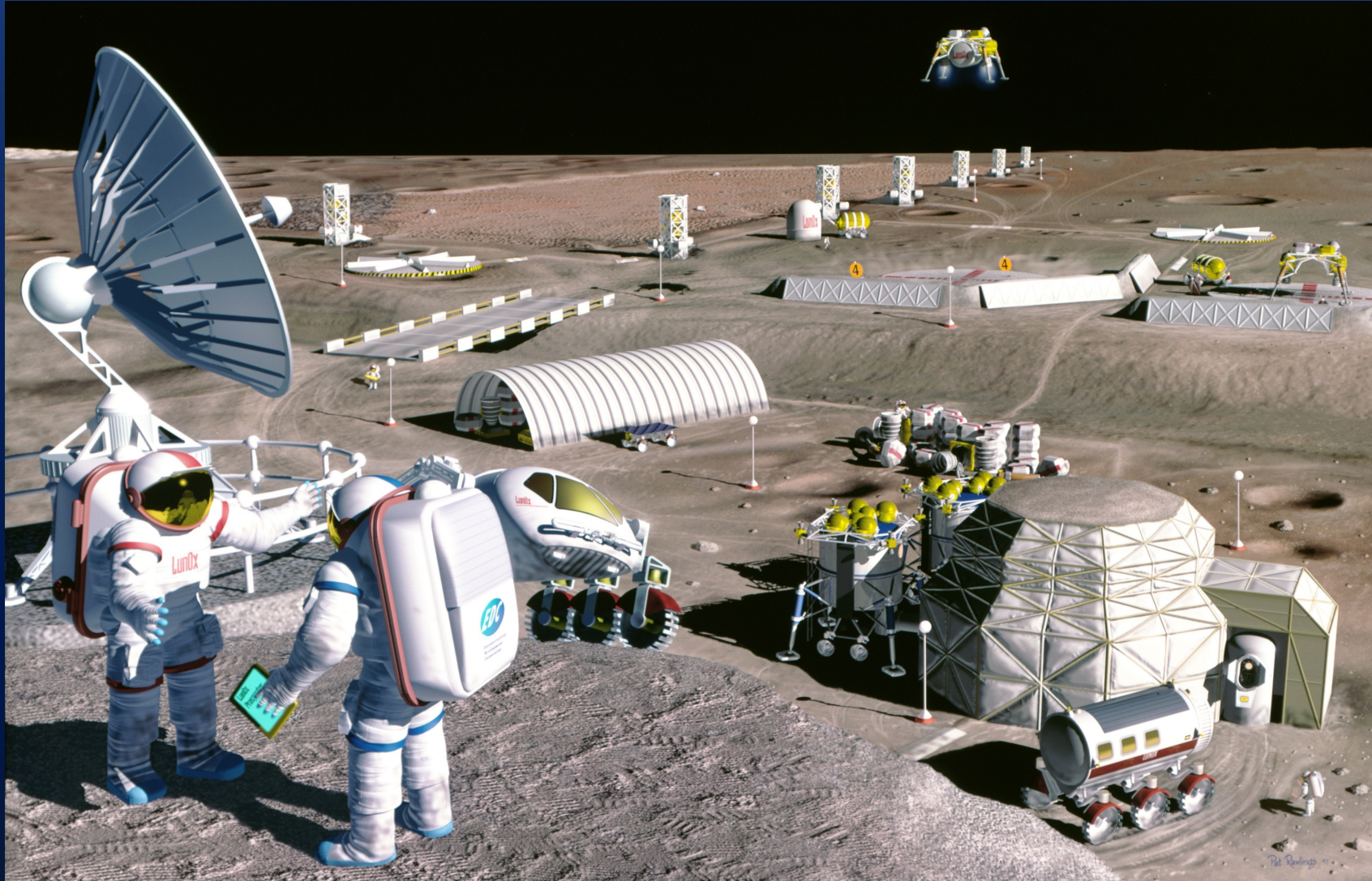
More Trouble:

- IT Ransom Novices
- Underfunded Nation-states
- Rapid expansion of OT Attack Surface
- Greater frequency, and impact, to industry and infrastructure
- Compressed Vulnerability timelines

We are in a race...



Getting to Level 6+ in OT?



Can't Avoid Programmatic Steps: Don't Head Straight to Mars



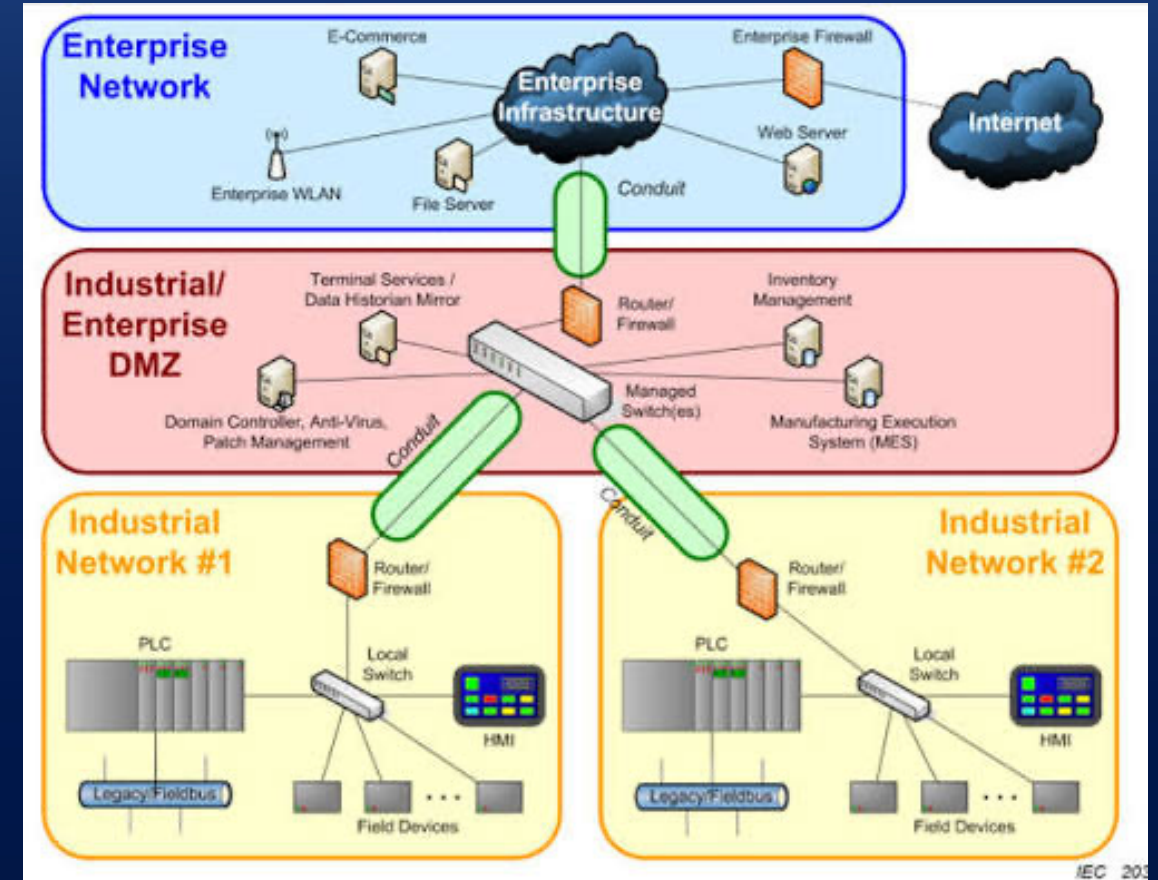
Mission: OT Level 6+, Step 1

Basics: determine & create OT network architecture

- Purdue Model – basic “stack” of Internet, IT and OT network Levels
- More advanced and realistic: IEC 62443 Zones & Conduits
 - Zones = segments Conduits = data flow
- Segmentation, micro-segmentation – reduce blast radius
- Secure Remote Access, aspects of Zero Trust – vendors & employees
- IT/OT tabletop exercises and IR – learn operational contingencies
- Build Resiliency and plan for Restore and Recover

Must build the Network Security Foundation

- Flat networks or too many connections create numerous attack vectors and lateral movement inside OT networks



Mission: OT Level 6+, Step 2

Basics: protect unsecure OT devices

- Visibility - must “see” unique OT devices to defend them
- Vulnerability Management – OT Threat Intel, unique OT vulns
- NGFW with IPS for IT and OT devices – make data “actionable” by blocking malicious IT and unique OT traffic
- EDR - still need to protect those old Windows XP boxes
- SIEM/SOAR/Deception/NDR – designed to “see” OT network traffic

Use Compensating Controls to protect vulnerable OT devices & fill the OT Cybersecurity Data Lake



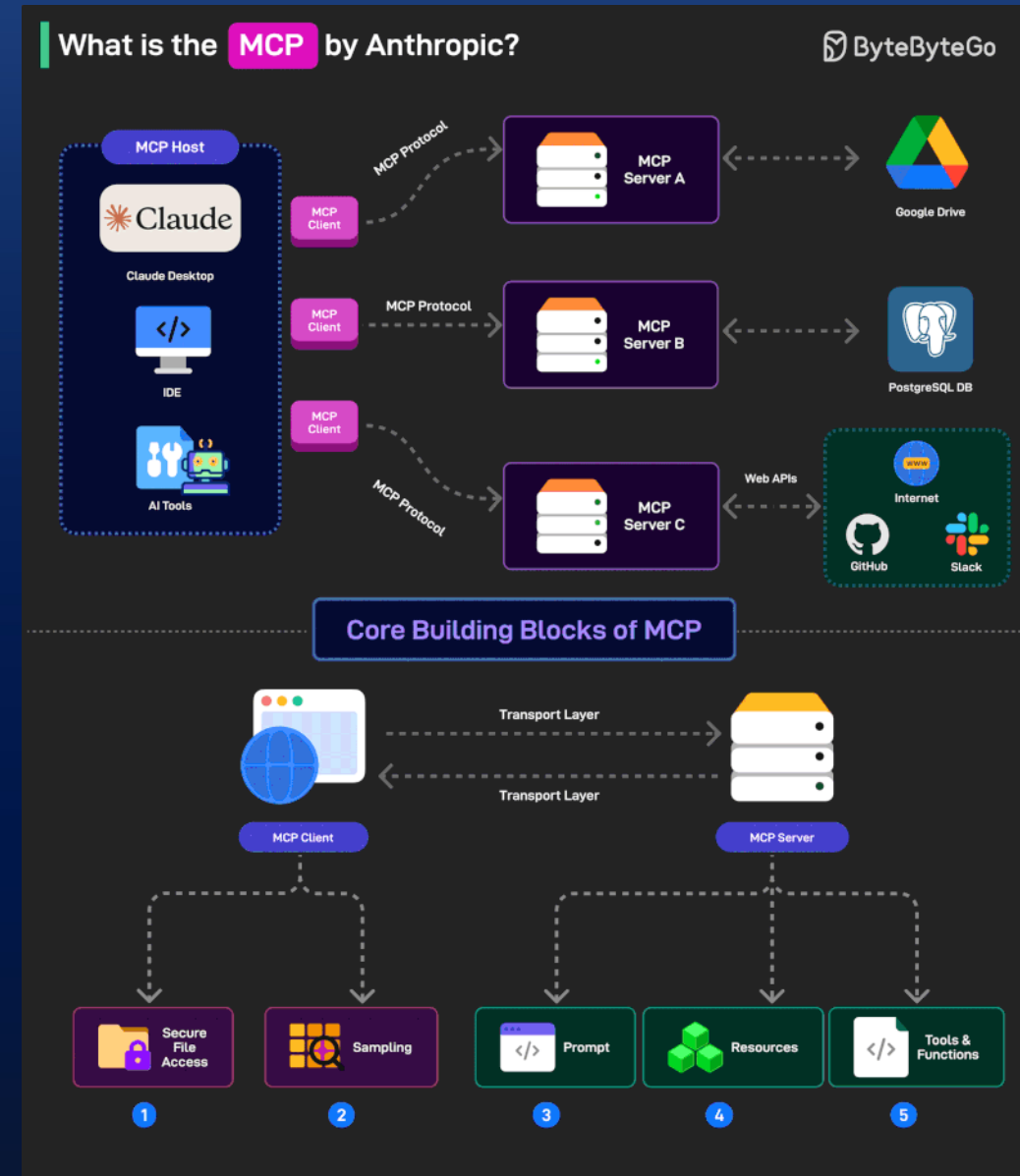
A Brief Message on MCP Servers: Your new AI API

Model Context Protocol – USB-C port for AI

- Created by Anthropic, next-gen API for AI
- How LLMs interact, “permanent” connections

- 3 building blocks
 - Tools – actions to take, run code, etc.
 - Resources – data, files, API calls
 - Prompts – user-controlled interactions
- Developers use SDKs to create an MCP server

New Ecosystem of Compliant Models and Tools to connect AI-enabled security solutions



Mission: OT Level 6+, Step 3

Build AI Level “6” – build the Bots

- Generate OT context
 - Security vendors and own genAI usage
- Correlate niche OT solutions
 - MCP servers and agentic AI
- Must generate “holistic” view through AI to eliminate blind spots and data gaps

Build the AI Tools, Connect the AI Agents and MCP servers and Leverage the OT AI Data Lake



Mission: OT Level 6+, Step 4

Balance SOC Automation with Operations

- Establish the Bright Line of Operational Risk
- Multi-functional tabletop exercises
 - Contingencies
 - Unintended Consequences
 - Hallucinations and Human Oversight
 - Data gaps or bandwidth limited OT networks
- Discover where Automation Ends
 - When the OT SOC hands over to Operations
- Accept that OT SOC will never be 100% automated

Biggest “unknown” before Level 6+



Early Preview of Level 6+: Factory VPN scenario

VPN Overlay Creation & Troubleshooting with GenAI

- Create VPN Overlay
- Define Overlay Type
- Image Recognition
- Inline Configs Edits
- Troubleshoot Down VPN
- Identify Config Issue
- Run Playbook
- Reload Config
- VPN Overlay is “Green”

The screenshot displays the FortiNMS interface with the 'Install Wizard' tab active. The left sidebar shows the navigation menu, including 'SD-WAN Manager' and 'Templates'. The main content area shows a table of template groups and their associated provisioning templates.

Template Group Name	Provisioning Templates	Assigned to Device/Group	Description
CorpA_HUB1	CorpA_HUB1_IPsec, CorpA_HUB1_BGP, HUB_SDWAN, CorpA_HUB1_CLIGRP	1 Device in Total HUB1 [root]	[Create]
CorpA_HUB2	CorpA_HUB2_IPsec, CorpA_HUB2_BGP, HUB_SDWAN, CorpA_HUB2_CLIGRP	1 Device in Total HUB2 [root]	[Create]
CorpA_BRANCH	CorpA_BRANCH_IPsec, CorpA_BRANCH_BGP, Branch_SDWAN, CorpA_BRANCH_CLIGRP	2 Devices in Total Branches (2)	[Create]

On the right, a GenAI chat window is open, displaying a message from the AI assistant:

Hi admin, I am your VPN configuration advisor. I can help you write scripts to provision VPN topologies and check VPN tunnel status:

- VPN Configuration Setup:
 - Site-to-site VPN: provides secure, scalable, and high-performance connectivity between multiple locations, ensuring data privacy and seamless resource sharing across different network environments.
 - Dialup VPN: offers secure, flexible remote access for individual users, enabling encrypted connections to corporate networks from any location, ensuring data privacy and seamless access to resources.
- VPN Tunnel Monitoring:
 - Check VPN Tunnel Status: I can help to check the current status of VPN tunnels
 - Diagnose VPN Tunnel: I can help to diagnose the possible issues for a downed VPN tunnel

At the bottom of the chat window, there is a text input field with the text: "I would like to create an SD-WAN VPN Ove".

Where We are Starting



Where We Will Go

Level 6+ must overcome differences:

- Networks
- Priorities
- Maturity
- Personnel
- Attackers
- genAI, agentic AI and beyond

Result: AI SOC Harmony



Resilient AI-driven OT SOC Summary

- OT Requires the Basics
- OT is Reliant on AI to rapidly accelerate
- With AI, OT can protect in an AI world
- OT, with IT, evolves into the modern digital world

And, OT will have its Unicorns!



**AI-enabled OT
SOC in harmony
with Operations**

Thank You!



<https://www.linkedin.com/in/richardmspringer/>

2026 State of OT and Cybersecurity Report OT peer survey of 700 international respondents OT Cyber Trends, Solutions & Best Practices

