



September Announcements

Protecting Our Communities

Thank you, SilverSky!

AI Headlines Creating
Concern: Are We Really In
Danger?

TechCred Opening October 1
at 9:00 AM

Cyber Resilience
Conference: Healthcare
2026

Cyber Resilience Conference: Healthcare 2026

- ▶ Wednesday October 14th
- ▶ 8:30 AM - 2:30 PM
- ▶ One-day event brings together healthcare executives, cybersecurity professionals, technology leaders, legal experts, emergency management personnel, and trusted industry partners
- ▶ Focused on practical strategies, meaningful collaboration, and real-world solutions
- ▶ \$20 - Working professional
- ▶ \$10 - Student
- ▶ Sponsorship available



CYBER RESILIENCE CONFERENCE

HEALTHCARE 2026

PRESENTED BY



GDAHA
Greater Dayton Area Hospital Association





September GoCyber Collective Keynote Speaker

Pamela LaPine

- President & CEO
- HipLink Software
- Cybersecurity Command and Control: Are You Ready to Respond





Cybersecurity

Command and Control

Coordinating Response When Every Minute Matters

CLICON

Presenter

Pamela LaPine

CEO, HipLink

CONFIDENTIAL

Cybersecurity Has an **Alert Fatigue Problem**

More detection does not automatically produce better response

77%

of security teams cite
alert fatigue as a top
challenge

46%

of SOC alerts are
estimated to be false
positives

42%

of SOC alerts are
estimated to go
uninvestigated

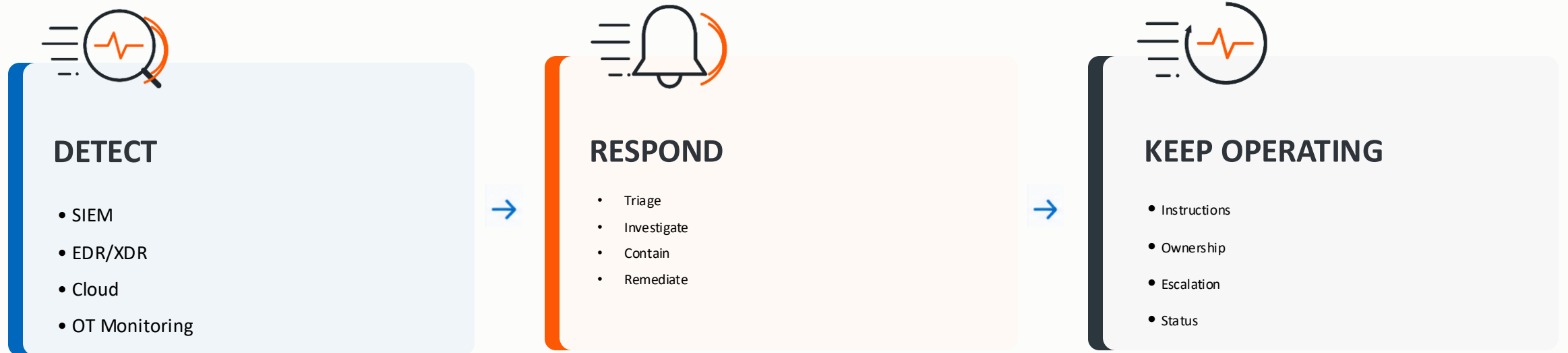
Command and control begins when the critical signal reaches the person responsible and ownership is confirmed

Sources: Microsoft Security citing IDC; Microsoft and Omdia, State of the SOC, 2026.



The Alert Fired. **Now What?**

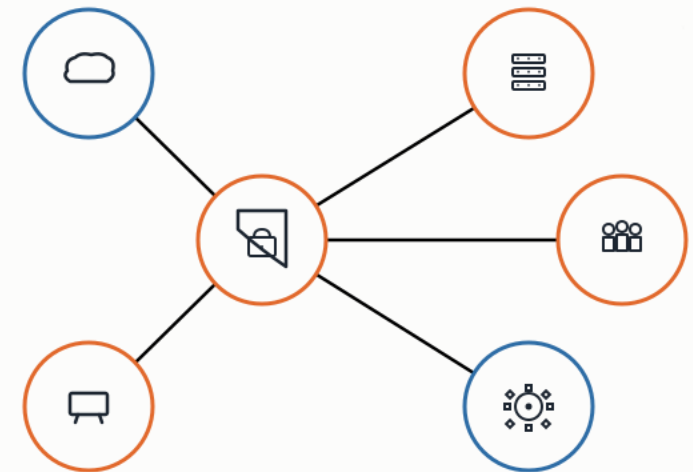
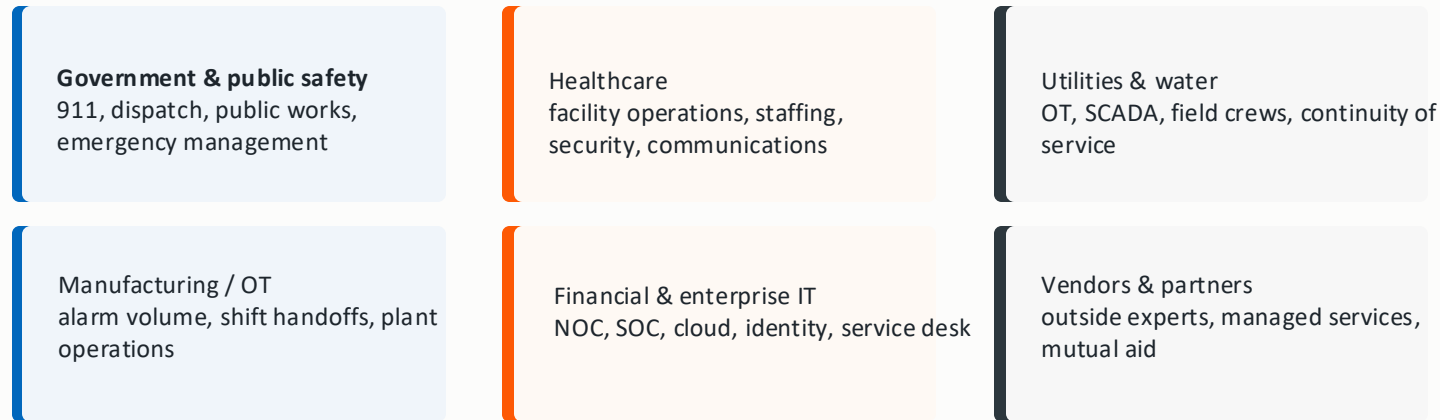
Detection is only valuable when it leads to accountable action



A tool can tell you something happened. It **cannot**, by itself, prove the right person is responding

Cyber Disruption Is a **Cross-Industry** Operating Problem

Cyber incidents look different by sector, but the response questions are remarkably similar



When systems are isolated or untrusted, people become part of the control layer

What **Cyber** Takes Away

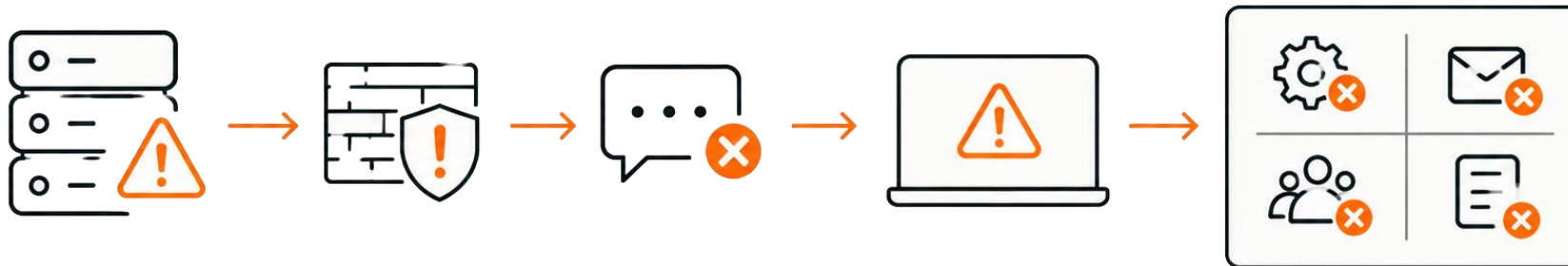
The urgency is not just the attack. It is the loss of the normal ways the organization works

Normal workflows
disappear

Communication paths
become untrusted

Responsibility
becomes harder

Leadership visibility
decreases



Cyber controls may detect and contain. Command and control keeps the response moving

Cyber Has an Alarm **Management** Problem

More detection does not automatically mean faster response



SIGNAL VOLUME

- SIEM
- EDR/XDR
- Cloud
- Infrastructure
- OT
- ITSM



RESPONSE DECISION

- Is it actionable?
- How urgent?
- Who owns it?
- What can wait?



HUMAN ACTION

- Reach
- Confirm
- Escalate
- Act
- Record

The objective is not to send every alarm faster. It is to make the critical alarm impossible to miss

The Last Mile: From Detection to **Accountable Action**



PRIORITY FILTERING IS THE FIRST COMMAND DECISION



Detection identifies the event - Command and control moves the response response

Routing Must Reflect **Live Responsibility**

The right alert sent to the wrong person is still a failed response

RESPONSIBILITY MAY DEPEND ON

- Role or skill set
- On-duty status / schedule
- Location or site
- System ownership
- Severity or incident phase

2:00 AM REALITY

The normal system owner may not be the person handling the workaround overnight.

The response question becomes:

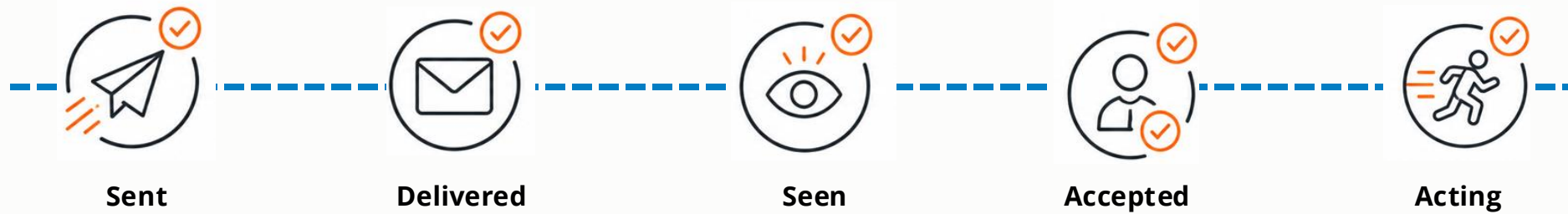
Who owns this action right now?

Live role-based routing turns “**who is on the list?**” into “**who is responsible now?**”



Delivery Is Not Ownership

The message can work but the response fails

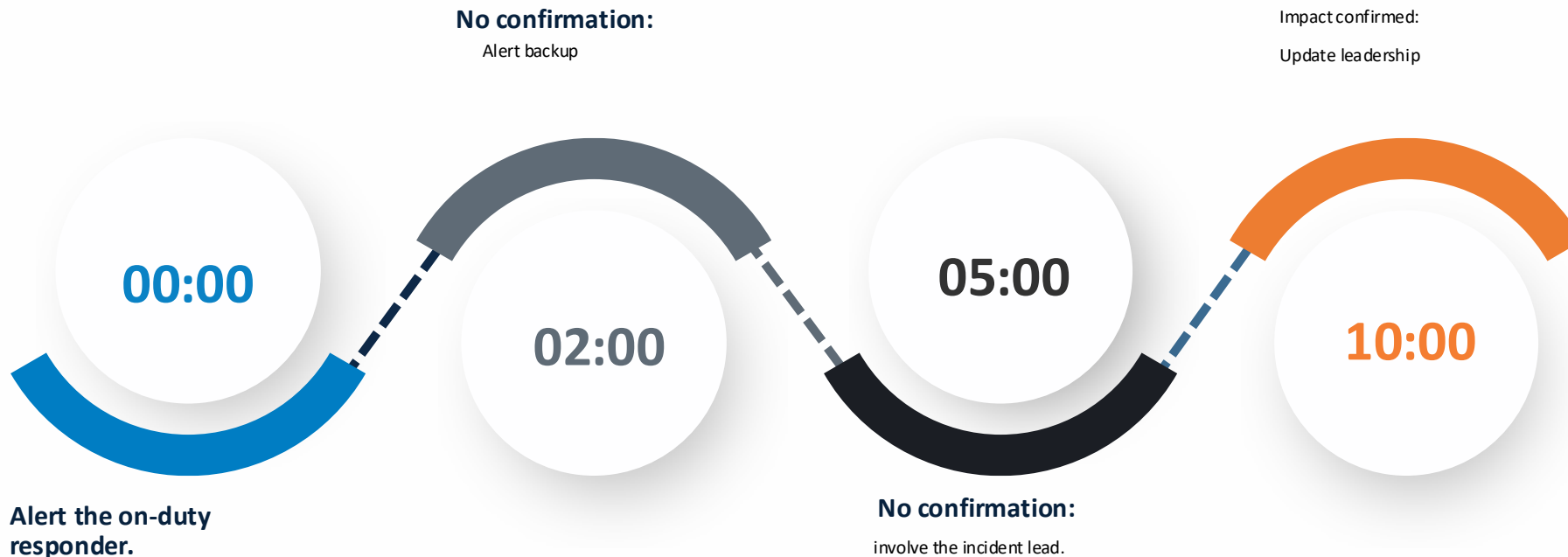


The threshold that matters is **OWNERSHIP**

During disruption, delayed ownership can mean equipment stays offline, field teams wait, or manual procedures never begin.

Escalation Should Be Policy, **Not Memory**

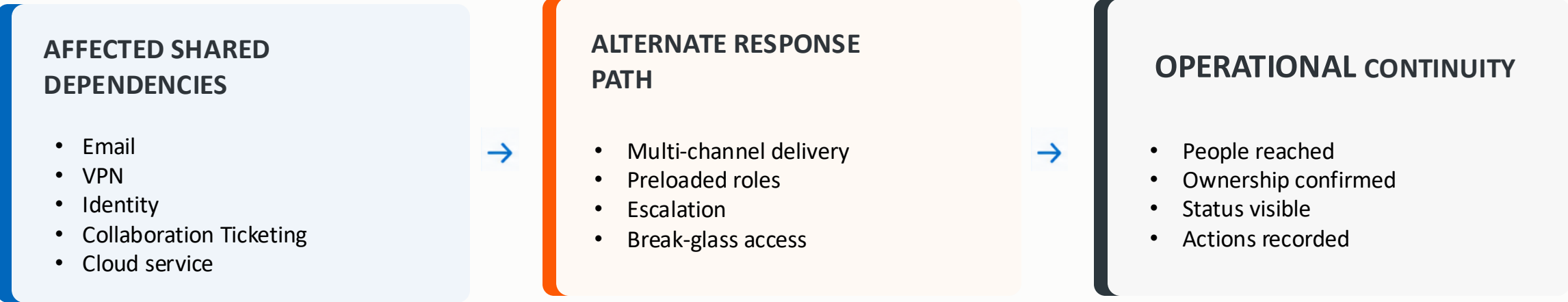
Silence is information - The response path should recognize it



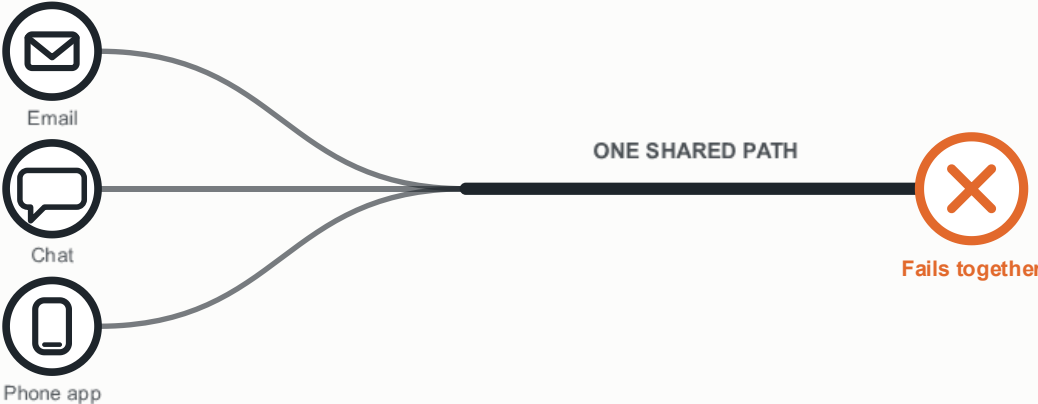
If a critical system is down, waiting for someone to realize nobody responded is not a plan

Build an Out-of-Band Communication Path

The response path cannot disappear at the same time the operating systems do



Another app is not necessarily another path



From Confirmed Ownership to **Approved Action**

Closing the gap between “I know” and “the approved next action happened”

HUMAN-TRIGGERED

A responder accepts ownership and starts an approved action from the response workflow.

SYSTEM-TO-SYSTEM

One trusted event triggers an approved workflow or integration in another system.

GOVERNED & LOGGED

- Defined in advance
- Authorized
- Constrained
- Included in the response record

Start a bridge • Run an approved script • Call an API • Trigger a service workflow • Send a leadership update

The goal is not to automate everything

It is to safely remove unnecessary delay from actions already approved



Leadership Needs Operational Status, **Not Just Technical Status**

Leadership need to know who owns it, what is underway, and what is still at risk
risk

TECHNICAL STATUS

What systems are affected?
What indicators exist?
What is the containment status?

OPERATIONAL STATUS

Who owns the action?
What workaround is active?
What is waiting on people?

RESPONSE RECORD

Who was reached?
Who acknowledged?
What changed?
What action occurred?

Visibility during the incident becomes evidence after the incident

Review • Compliance • Insurance • Process improvement



How Ready Are You to Operate Through a **Cyber** Disruption?

These are not questions about whether detection works. They are questions about whether the organization can function after detection.

- 1 Can we reach responders if a primary channel is unavailable?
- 2 Can we prove who accepted ownership?
- 3 Does escalation happen automatically when nobody responds?

Also Test: responsible role • leadership visibility • complete response timeline

Every “no” or “not sure” reveals a gap worth testing



Test the Response **Before the Incident**

A tabletop tests the plan. A live test verifies what actually happens.



MEASURE time to confirmed ownership • time to escalation • time to verified action • leadership status • complete timeline

A plan you have never executed is still partly a theory

Where **HipLink** Fits

Coordinating people when the environment is disrupted

CYBER EVENT DETECTION

SIEM • EDR/XDR • ITSM/SecOps • OT/infrastructure monitoring

OPERATIONAL RESPONSE LAYER — HIPLINK

Prioritize • Route • Notify • Confirm • Escalate • Update • Act • Record

CONTINUITY & RECOVERY

Containment • Manual operations • Leadership updates • Restoration • Post-incident review

Built for integrated alerting, role-based routing, multi-channel delivery, acknowledgements, escalation, response actions, and audit-ready records.





If cyber took a critical system away tomorrow...

what would your operation need to keep moving?

Questions and Discussion

Detection starts the process. Command and control determine the outcome.

Pamela LaPine
CEO, HipLink

September Threat Briefing

- ▶ Joe Tinney
 - SecureCyber
 - VP of Cyber Operations



September Threat Briefing



Criminal Round Up

- Oleksii Oleksiyovych Lytvynenko (Conti ransomware group malware author) sentenced to 4 years in prison
- ATT employee sentenced to 16 months for SIM swapping

Remote Access Vulnerabilities

- ScreenConnect Guest agent vulnerability - allows you to transfer files and commands silently to the technician
- Check Point VPN - remote code execution as root on the firewall
- Citrix NetScaler/ADC August CVE - anonymous access to resources - default config for Citrix Receiver may land you nowhere, other configs land you until an SSL VPN like state

Patch Palooza

- September Microsoft patch Tuesday - most patched CVEs ever. Old components patched, chain- and worm-able CVEs patched with both Local and Remote Code Execution and Local Escalation of Privilege. ~1,000 vulns, 100 critical, 2 zero-day.



September Threat Briefing

But what about AI, Joe?

Lots of calls for immediate action in the face of AI doom - Anthropic CEO, Bill Gates, OpenAI Call for Action on Cyber Defense

Attacks continue to accelerate known, common weaknesses and Vulnerabilities. In some cases, novel exploits created but still an outlier. AI empowers attackers and is closing the 'security through obscurity' concept more fully especially when encountering uncommon or niche systems (like OT)



September Threat Briefing

But what about AI, Joe?

How are you approaching AI?
Governance Only? Control Only?
Employee AUP and security
training? Employee enablement
training/upskilling?

Chinese open weight AI models
perform one gen behind US
frontier with much less cyber
restriction - aka, the bad guys
are getting the good stuff without
having to hassle breaking
guardrails. Many AI guardrail
subversion techniques exist and
are effective.

October Meeting:

Mike Stark - VTScada Mid Atlantic
Manager/Trihedral

Working with water industry for 25
years protecting most precious resource

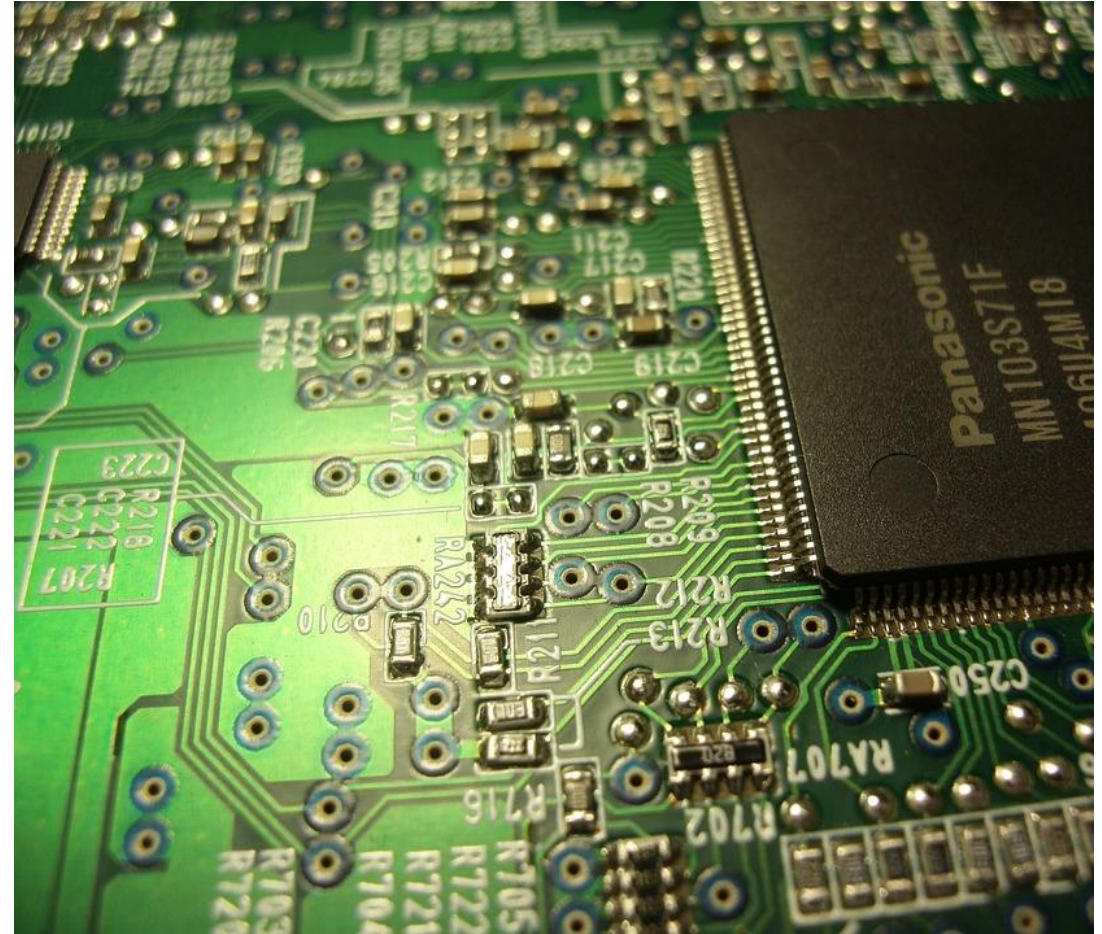
Is your water safe? Any gaps in your
cybersecurity?

How AI is impacting water safety



September Parting Shots

- Local Gov't/Public Safety SIG – Wright Patt Room
- Education SIG – Victoria Room
- Defense Contractor SIG – Hawthorn Room
- Register for Workshop, Monthly Meetings
- Turn in your lanyards at the desk





Information

Email me at john@GoCyberCollective.org.

If you have a suggestion on meeting topics, special interest groups, breakfast menu, or anything else we want to hear from you.

You can register for future breakfast meetings from the website.

□ GoCyberCollective.org



Event Sponsors

