gocyber

COLLECTIVE

January Announcements

Serving Our Communities

Happy New Year!

Thank You, Extreme Networks!

TechCred Paused

GoCyber/Cincinnati InfraGard Collaboration

Internship Summit – Feb. 25, 10 AM – 11:30 AM

Cyber Insurance Summit – March 17, 10 AM – 11:30 AM

TRIUMVIRATE CYBERSECURITY

CMMC for the Little Guy: How Small Businesses Can Achieve Compliance

Expert Guidance on CMMC

Professional guidance to help attendees understand the complexities of the CMMC framework.

Compliance Strategies

Participants will learn practical strategies to achieve and maintain CMMC compliance.

Real-World Experiences

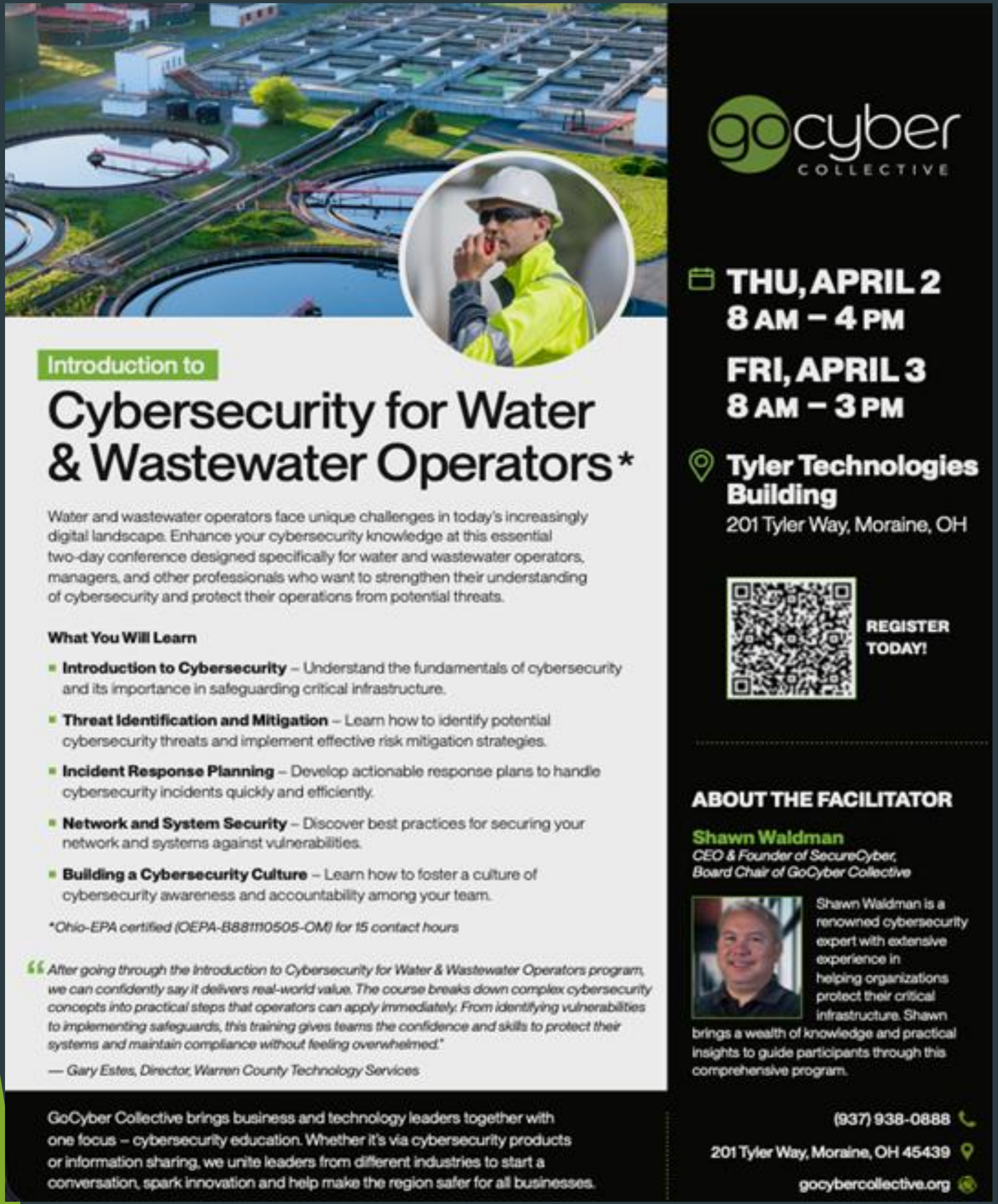
Insights from real client stories and case studies to effectively address common compliance challenges.

TRIUMVIRATE CYBERSECURITY

January 27 1 PM – 2:30 PM

Triumvirate Cybersecurity will give you actionable steps to begin or maintain your CMMC journey.

Introduction to Cybersecurity for Water & Wastewater Operators



gocyber COLLECTIVE

Introduction to

Cybersecurity for Water & Wastewater Operators*

Water and wastewater operators face unique challenges in today's increasingly digital landscape. Enhance your cybersecurity knowledge at this essential two-day conference designed specifically for water and wastewater operators, managers, and other professionals who want to strengthen their understanding of cybersecurity and protect their operations from potential threats.

What You Will Learn

- **Introduction to Cybersecurity** – Understand the fundamentals of cybersecurity and its importance in safeguarding critical infrastructure.
- **Threat Identification and Mitigation** – Learn how to identify potential cybersecurity threats and implement effective risk mitigation strategies.
- **Incident Response Planning** – Develop actionable response plans to handle cybersecurity incidents quickly and efficiently.
- **Network and System Security** – Discover best practices for securing your network and systems against vulnerabilities.
- **Building a Cybersecurity Culture** – Learn how to foster a culture of cybersecurity awareness and accountability among your team.

THU, APRIL 2
8 AM – 4 PM

FRI, APRIL 3
8 AM – 3 PM

Tyler Technologies Building
201 Tyler Way, Moraine, OH

REGISTER TODAY!

**Ohio-EPA certified (OEPA-B881110505-OM) for 15 contact hours*

> *“After going through the Introduction to Cybersecurity for Water & Wastewater Operators program, we can confidently say it delivers real-world value. The course breaks down complex cybersecurity concepts into practical steps that operators can apply immediately. From identifying vulnerabilities to implementing safeguards, this training gives teams the confidence and skills to protect their systems and maintain compliance without feeling overwhelmed."*
>
> *— Gary Estes, Director, Warren County Technology Services*

ABOUT THE FACILITATOR

Shawn Waldman
CEO & Founder of SecureCyber,
Board Chair of GoCyber Collective

Shawn Waldman is a renowned cybersecurity expert with extensive experience in helping organizations protect their critical infrastructure. Shawn brings a wealth of knowledge and practical insights to guide participants through this comprehensive program.

GoCyber Collective brings business and technology leaders together with one focus – cybersecurity education. Whether it's via cybersecurity products or information sharing, we unite leaders from different industries to start a conversation, spark innovation and help make the region safer for all businesses.

(937) 938-0888 ☎
201 Tyler Way, Moraine, OH 45439
gocybercollective.org

January GoCyber Collective Keynote Speaker

-General Paul Craft

-Former Commander U.S. Army Cyber Command

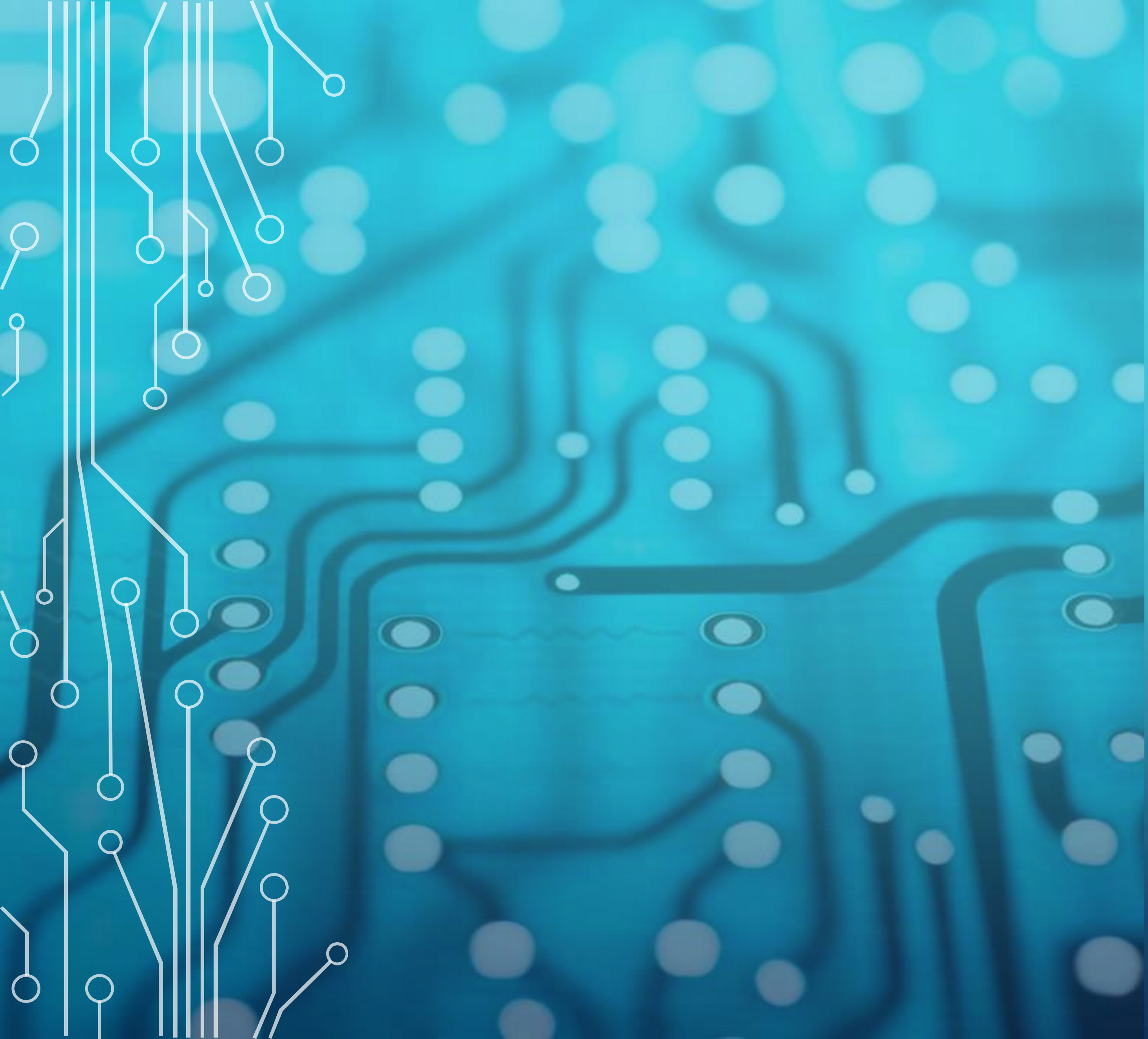
-GoCyber Collective Board Member

-Pres. DataShapes AI

-Senior Advisor/Board Member of Numerous Organizations

TOP CYBER THREATS FOR 2026

BG PAUL CRAFT, US ARMY (RET)

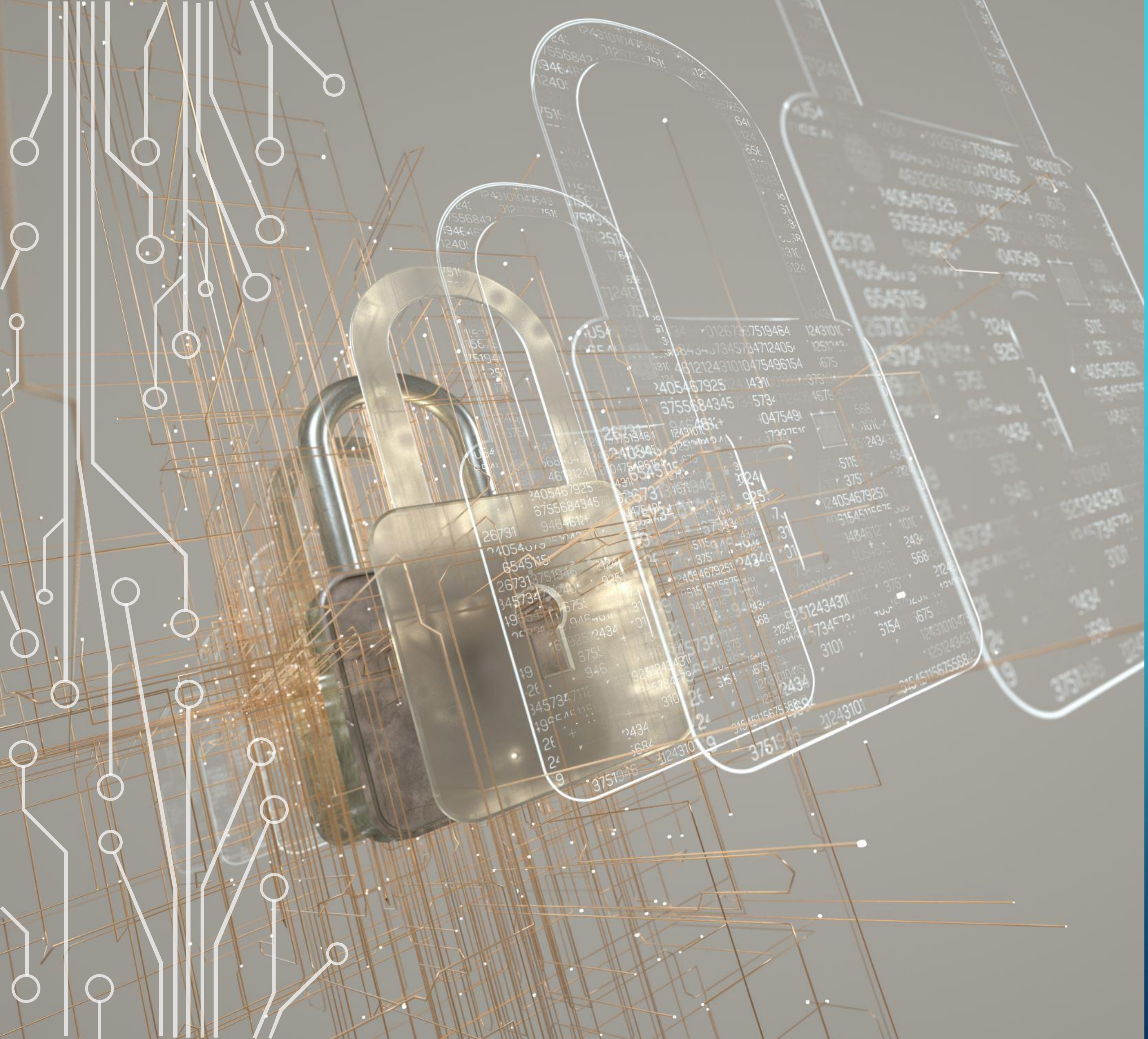


BACKGROUND

- Local kid, graduated from Miami (County) East H.S. then United States Military Academy in West Point, NY
- First 20 years, lead DoD IT networking organizations across the U.S. and globally from Republic of Korea to Afghanistan
- Last 10 year, shifted to leading U.S. and International cyber operations first on the defense then on the offense
- In between playing defense and offense, was the US Army's Chief of Cyber and Electronic Warfare and Chancellor of a military university
- Since retiring at the end of 2024, I find companies with capabilities I wish I had in uniform and causes I care about – like GoCyber Collective

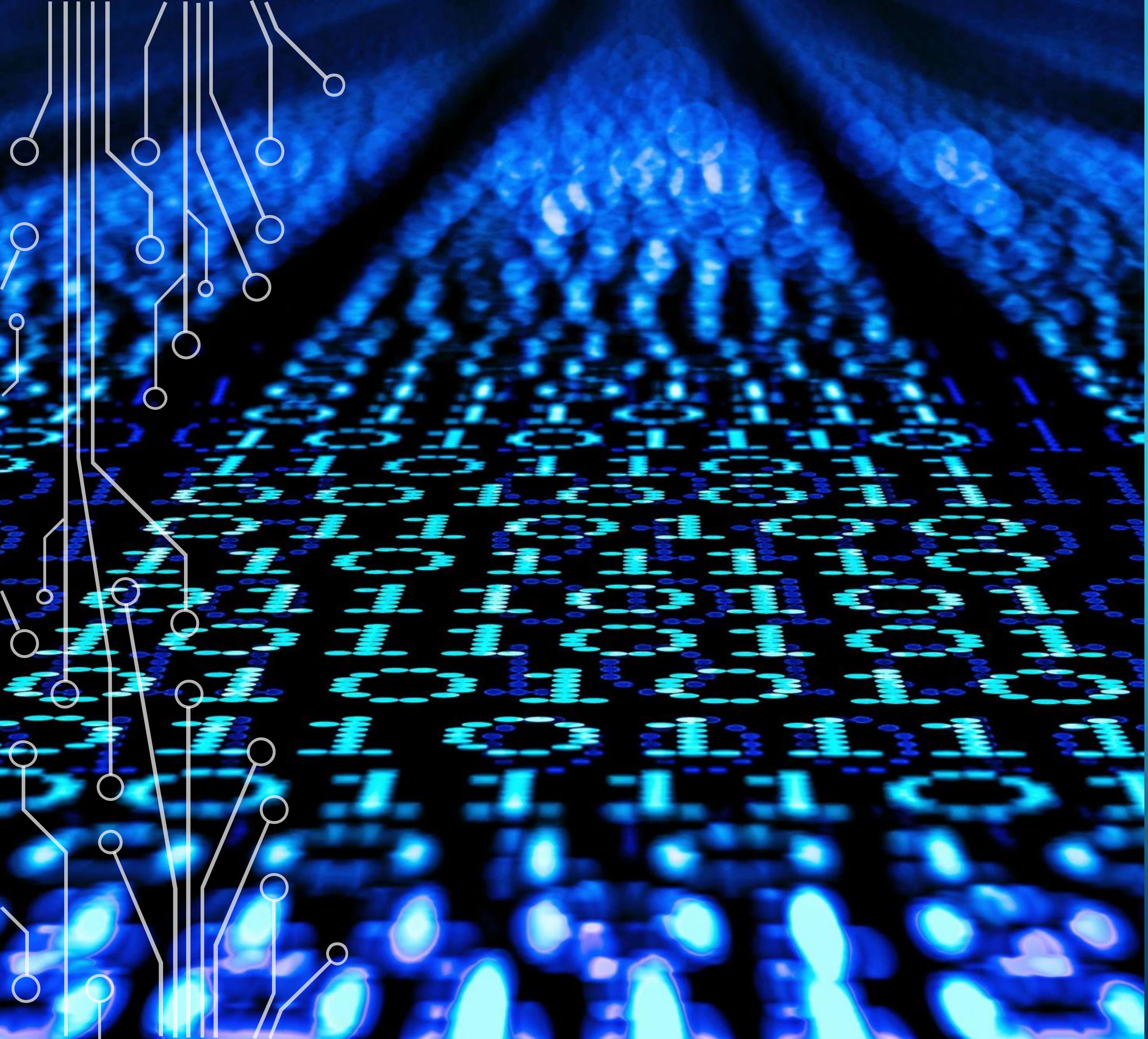
UPFRONT

- Threats are ever increasing – Volume, Speed, Complexity – No Bar to Entry
- The more ways to network, the more ways to attack, the more that has to be defended
- Networking is always about better/faster ways to connect, easier ways to communicate
- Security will slow network access and network performance
- AI has had an exponential impact on attack vectors and new security requirements
- **Most fails still happen due to simply not keeping systems up to date with patches**



SOCIAL ENGINEERING AND PHISHING/SMISHING

- We (people) can be the weakest link on the network
- Lack of cyber education / training on threats
- Not understanding how to turn on security controls on an end device (laptop or phone)
- AI adds to great volumes and sophistication to all attacks



RANSOMWARE ATTACKS

- Biggest money maker for criminals – avg payout is $2.4M
- Focus in manufacturing and finance

CLOUD VULNERABILITIES

- Many companies shift to clouds without understanding how they work, how they are secured, etc
- Leads to misconfigurations, insecure APIs, poor access controls
- Cloud providers (depending on your contract) aren't required to tell you if your data was exposed

INTERNET OF THINGS (IOT) ATTACKS

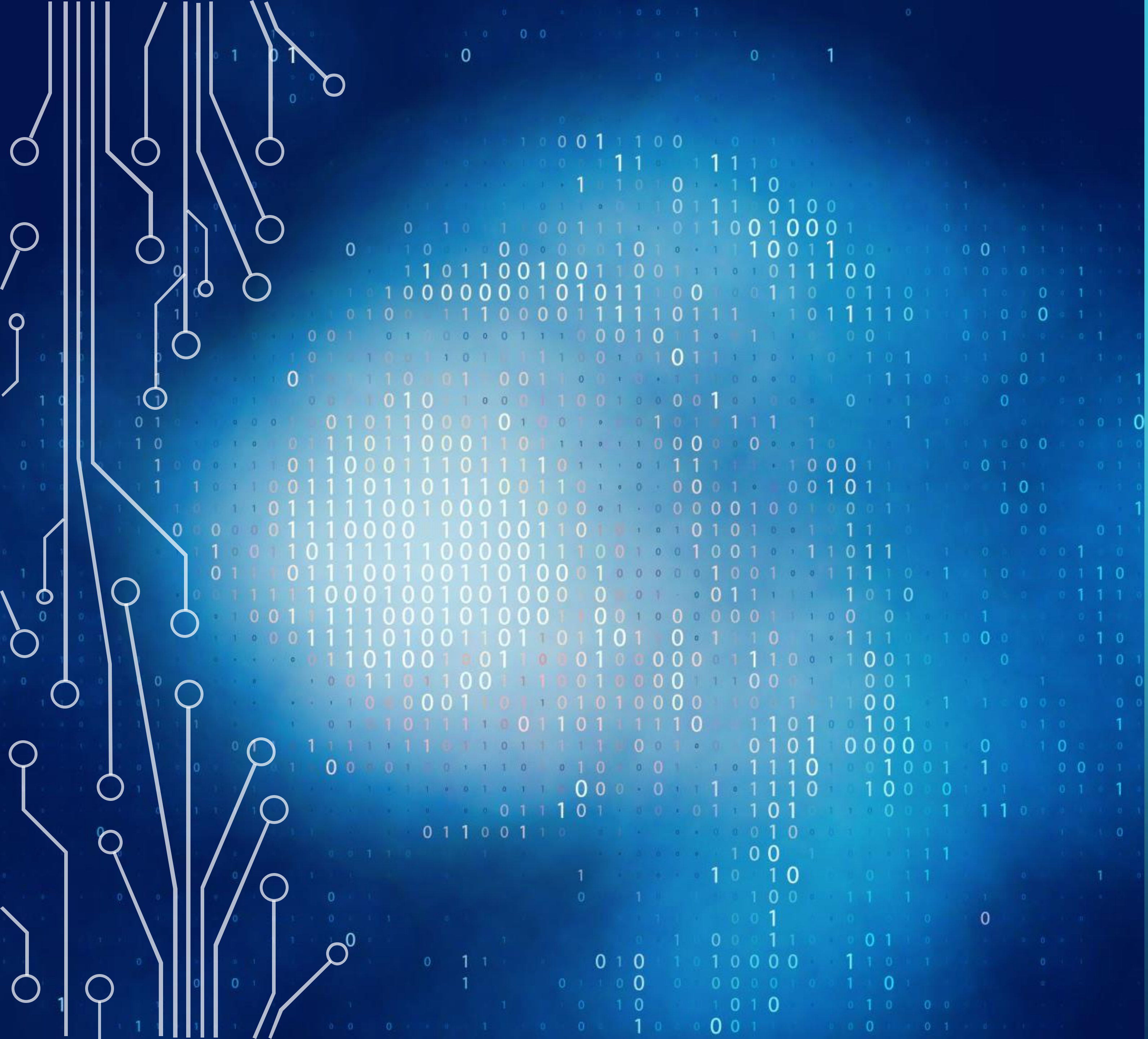
- Smart Devices / Cars
- Doors
- HVAC
- Security Cameras
- Industrial Control Systems

ADVANCED PERSISTENT THREATS (APT)

- China, Russia, Iran, North Korea
- Sophisticated, long-term
- Well Financed
- Aimed primary at gov't agencies, defense industrial base, and critical infrastructure

INSIDER THREATS

- Accidental or malicious
- Some opportunities created by company policies (work from home, remote work, BYOD, single sign on, etc) – without requisite cybersecurity controls
- Big problem is failing to delete accounts for employees who have departed



MALWARE

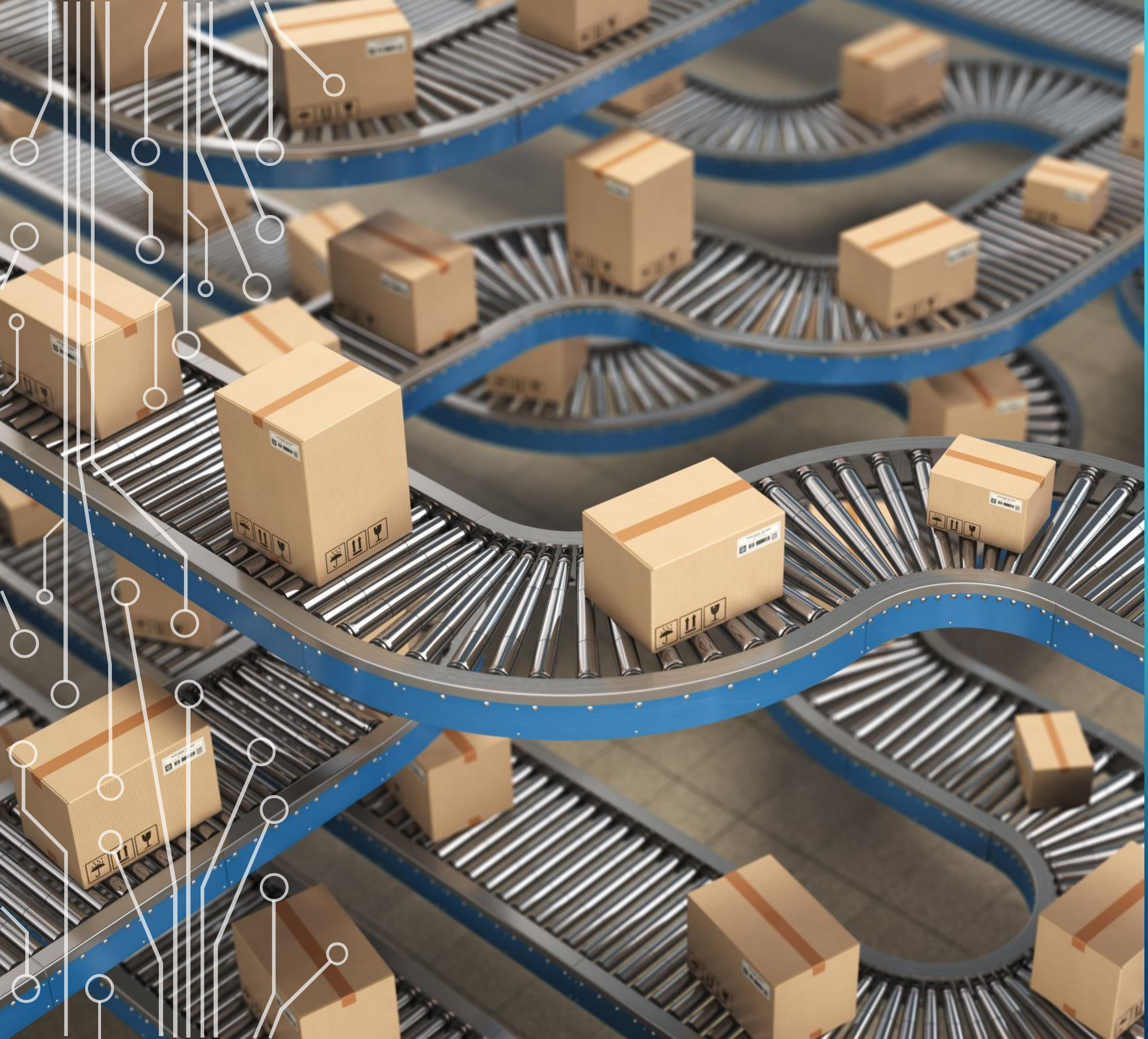
- Viruses, spyware, trojan horses, ransomware, etc
- How does your device get infected? going to malicious website, downloading a document with an executable, playing a game with adware on your phone, etc

DISTRIBUTED DENIAL OF SERVICE (DDOS)

- The OG of large scale cyber attacks along with malware.
- Financial loss / reputation loss (usually for websites that have the ability to login)
- Saw the first use of malicious bots in 2017-2020

MAN-IN-THE-MIDDLE ATTACKS

- All about stealing info/data in transit
- Goal to impact data integrity and confidence
- Grabbing credentials as you login, banking info, texts, emails, etc
- Popular at all free wifi spots: airports, big hotels, sporting events



SUPPLY CHAIN ATTACKS

- Hackers look for the weakest link in the product that will make it fail or be permanently compromised
- Targets can be big companies of 1000s, or small businesses with 10-50 employees
- Hardware or software manufacturing

SOME RECOMMENDATIONS …AND SOME QUESTIONS

Social Engineering and Phishing → *Security Education and Training*

Ransomware Attacks → *Back-up data offsite*

Cloud Vulnerabilities → *Don’t dive into water with checking*

Internet of Things Attacks → *If connected to Internet, secure it*

Advanced Persistent Threats → *Patch, Patch, Patch, Patch…*

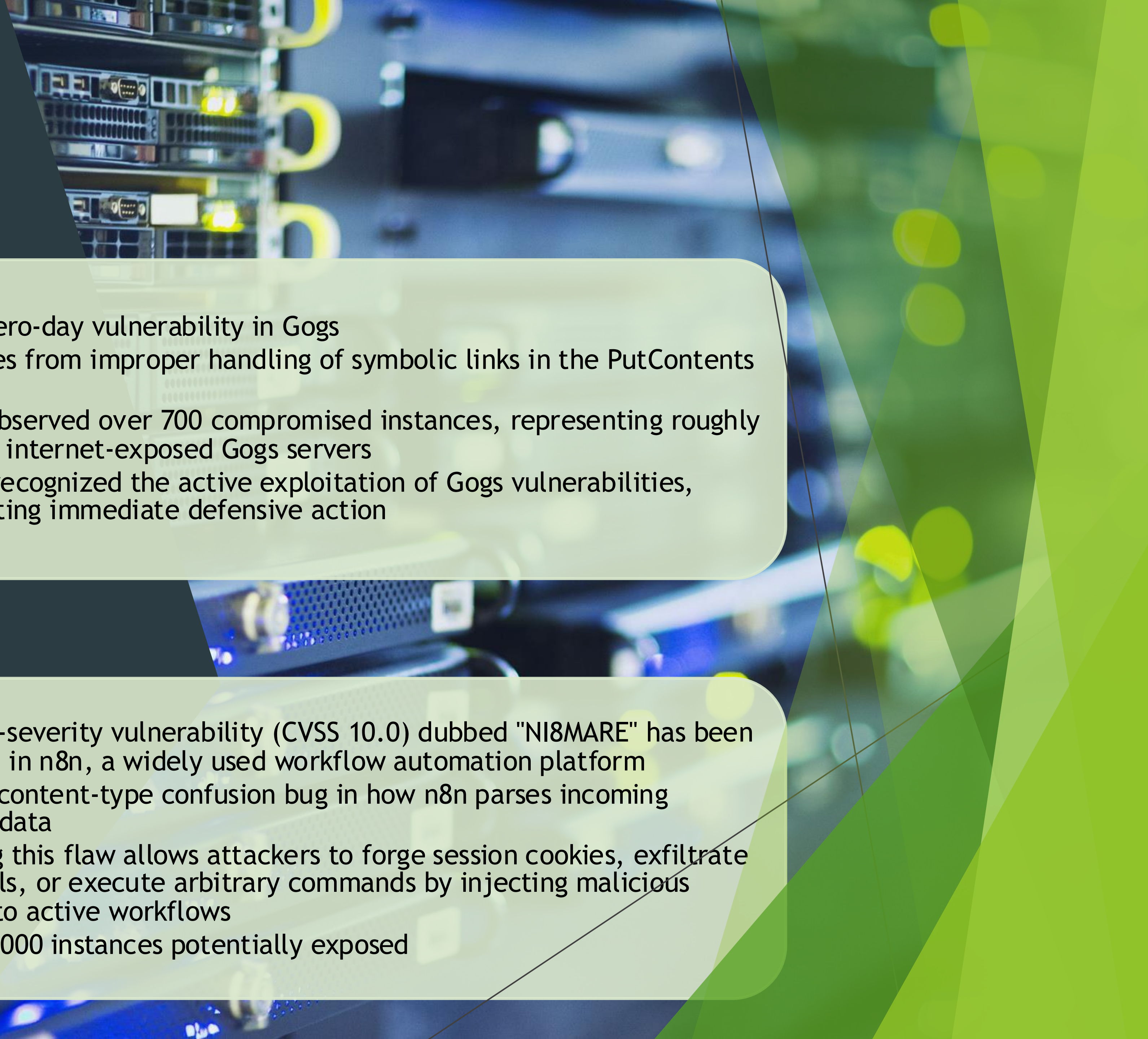
SOME RECOMMENDATIONS
…AND SOME QUESTIONS

Insider Threats	→	*90-day access controls*
Malware	→	*Regularly run anti-virus*
Distributed Denial of Service	→	*Do not advertise internal IP addresses*
Man-in-the-Middle Attacks	→	*Do not use airport or hotel wifi*
Supply Chain Attacks	→	*Triple check if remote work is worth it*

Threat Briefing

- Charles Zugaro – Cybersecurity Analyst – Warren County Telecommunications

January Threat Briefing



Gogs Symlink Bypass Remote Code Execution (CVE-2025-8110)

- Critical zero-day vulnerability in Gogs
- Flaw arises from improper handling of symbolic links in the PutContents API
- Wiz has observed over 700 compromised instances, representing roughly 50% of all internet-exposed Gogs servers
- CISA has recognized the active exploitation of Gogs vulnerabilities, necessitating immediate defensive action

n8n "NI8MARE" Content-Type Confusion(CVE-2026-21858)

- Maximum-severity vulnerability (CVSS 10.0) dubbed "NI8MARE" has been identified in n8n, a widely used workflow automation platform
- Flaw is a content-type confusion bug in how n8n parses incoming webhook data
- Exploiting this flaw allows attackers to forge session cookies, exfiltrate credentials, or execute arbitrary commands by injecting malicious scripts into active workflows
- Over 100,000 instances potentially exposed

January Threat Briefing

HPE OneView Unauthenticated RCE (CVE-2025-37164)

- On December 17, 2025, Hewlett Packard Enterprise (HPE) disclosed a CVSS 10.0 vulnerability in HPE OneView
- Flaw allows an unauthenticated remote attacker to execute arbitrary code via the /rest/id pools/executeCommand REST API endpoint
- CISA has added this vulnerability to the Known Exploited Vulnerabilities (KEV) catalog following reports of active exploitation in the wild
- Because OneView is a "trusted" management platform typically deployed deep within internal networks, it is a prime target for lateral movement and state-sponsored espionage.

January GoCyberCollective Sponsor – Extreme Networks

Glenn Mitchell - Senior SLED Account Executive

Extreme Networks' Fabric Connect SPB – Shortest Path Bridging

Jeff Sabella – Solutions Engineer
Jsabella@extremenetworks.com

Glenn Mitchell – Account Executive
Gmitchell@extremenetworks.com

Extreme networks

Jetson Technology Running on Flintstone Networking

Extreme's IEEE/IETF Fabric Connect TECHNOLOGY

Smart Phones
Artificial Intelligence
Virtual Reality
Connected Edge Devices (IoT)
Sensors, Beacons and Robotics

Standards Based and Interoperable With ANY Network

DYNAMIC, MOBILE, REAL-TIME

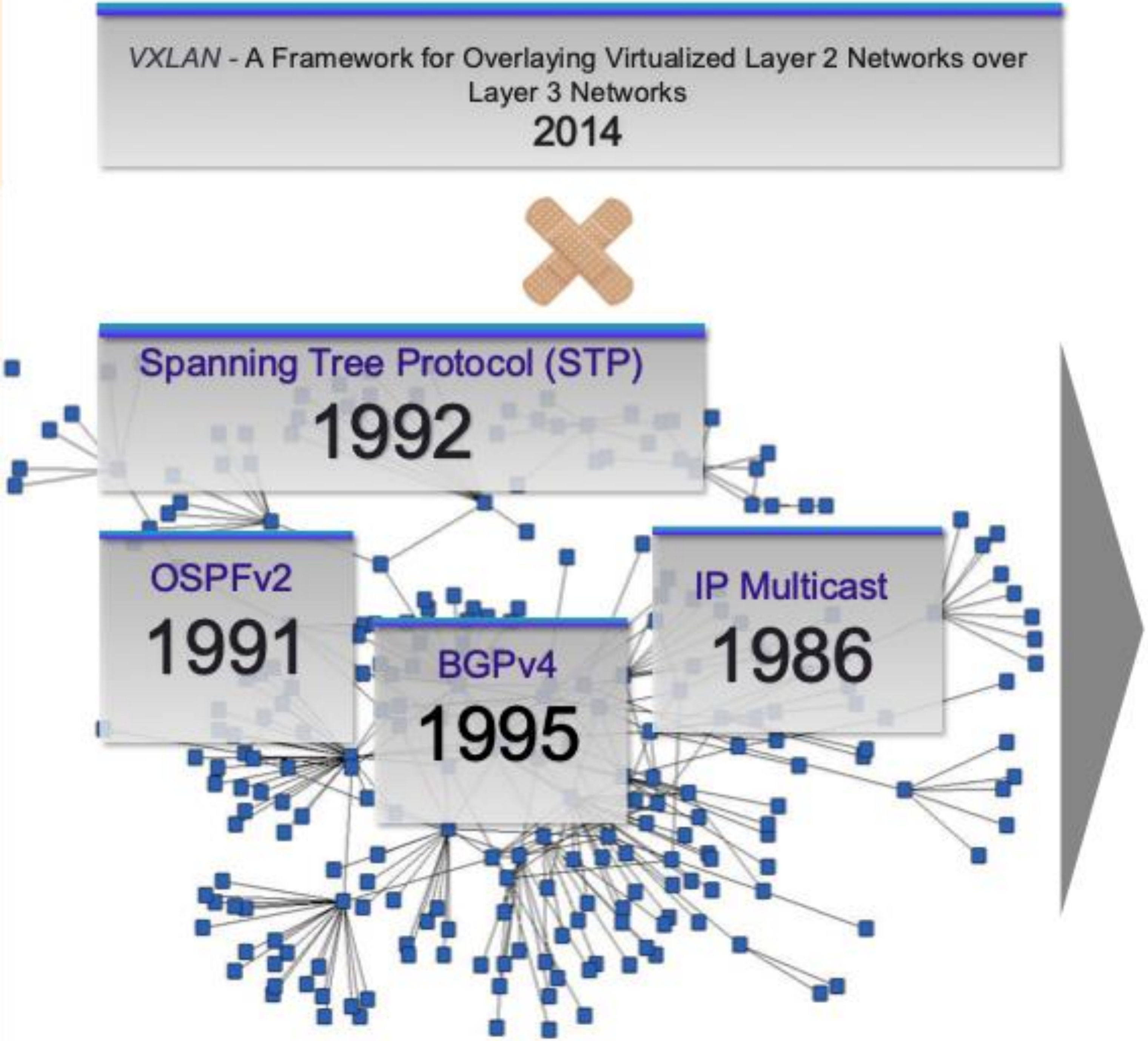
Conventional NETWORK

Dated Protocols
Dated Network Designs
Architectures built for static environments

LACK OF EVOLUTION

← **TODAY'S REALITY** →

Single Protocol – ISIS SPBm, Flexible Topology, Hyper Segmentation, Onboarding Automation, Provision only on edge switches,



VXLAN - A Framework for Overlaying Virtualized Layer 2 Networks over Layer 3 Networks
2014

Spanning Tree Protocol (STP)
1992

OSPFv2
1991

BGPv4
1995

IP Multicast
1986

Addresses the root issues

IEEE Advancing Technology for Humanity

IETF

Shortest Path Bridging
2012

- Only Technology jointly standardized by IEEE (802.1Q) and IETF (RFC 6329)
- Origins in Service Provider Space
- MPLS like functionality without complexity
- Service provider backbone bridging standard IEEE 802.1ah – Interoperate with ANY conventional network stack
- SPBm – Shortest Path Bridging using mac-in-mac encapsulation
- IS-IS control plane – single protocol

Today’s Common Network Segmentation Practices

VLANs with ACLs

Very operationally complex
Lack of scale
Global routing table

Distributed Firewalls

Very high CAPEX
High OPEX

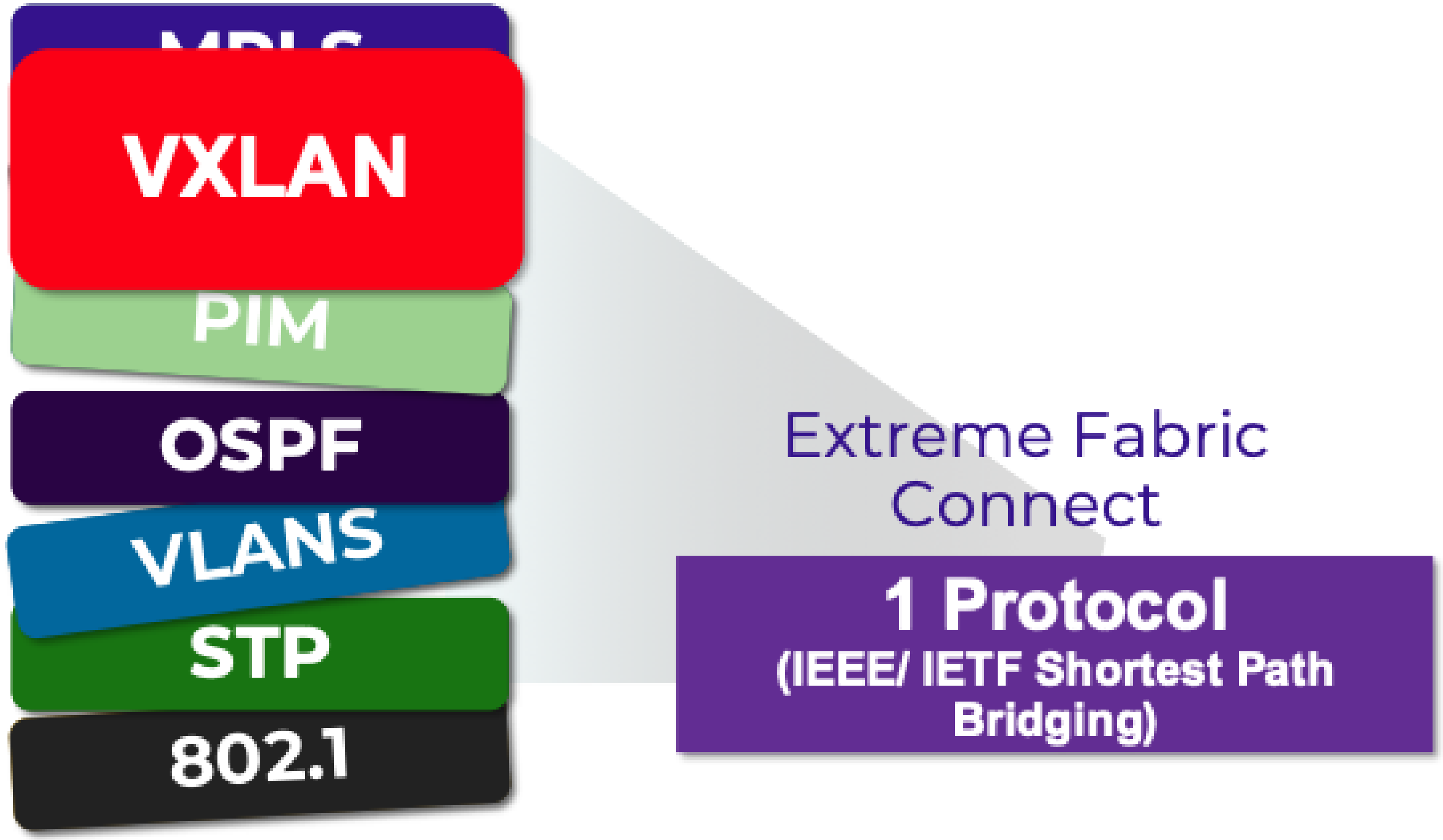
IP-VPNs (VRF-Lite) / MPLS

Segmented routing table
Operationally complex; complex provisioning

Tunnel Overlays (VXLAN, IPSec, GRE)

Underlay and overlay complexity
Limited scale for large numbers of IoT devices

Fabric Connect is Simple: From 4-10 Protocols to 1



Extreme Fabric Connect

1 Protocol
(IEEE/ IETF Shortest Path Bridging)

Fabric Connect Benefits:

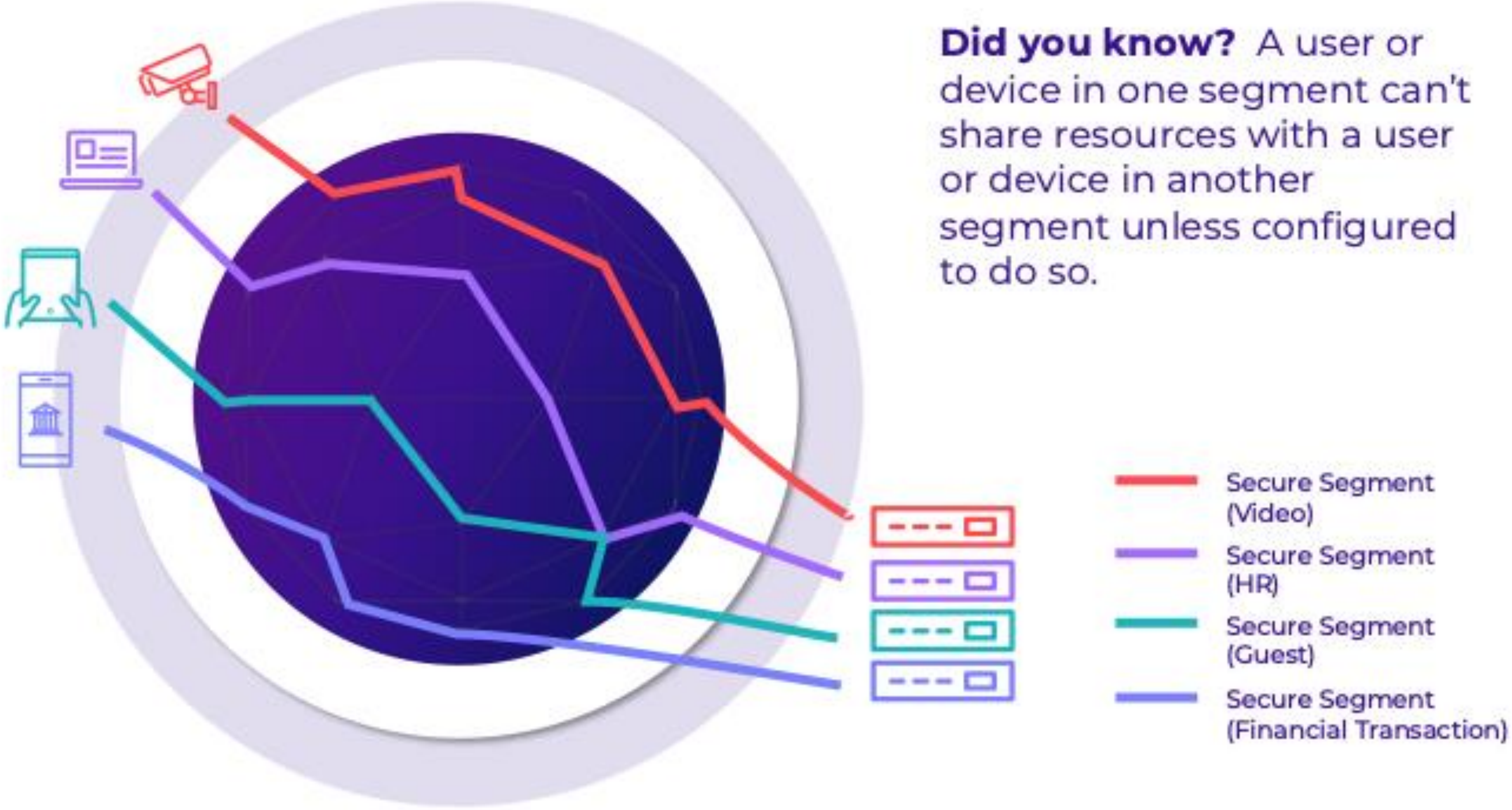
- Faster to Deploy
- Increased Stability
- Easier Troubleshooting
- Faster Resiliency
- Enhanced Security
- Lower Costs

SECURE: Hyper-segmentation locks down network traffic, services

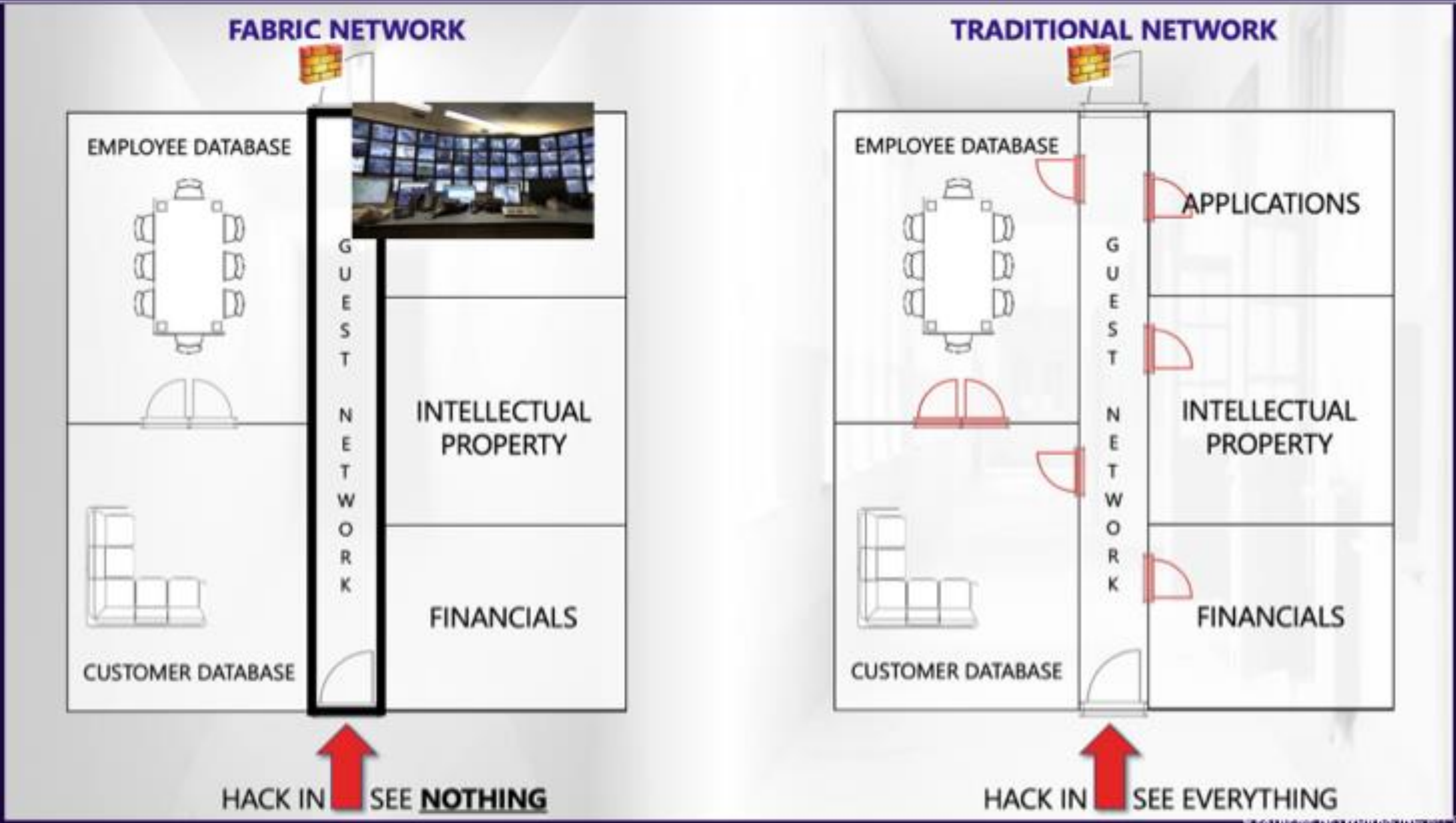
Key Values:

- **Isolated by design:** Segments are separate and secure
- **Provisioned at the edges:** Users and devices are hidden from the core
- **Massive scaling:** Assignments follow the user or device
- **Segments extend network-wide**
- **Control** secure segment access through policy/NAC

Did you know? A user or device in one segment can't share resources with a user or device in another segment unless configured to do so.



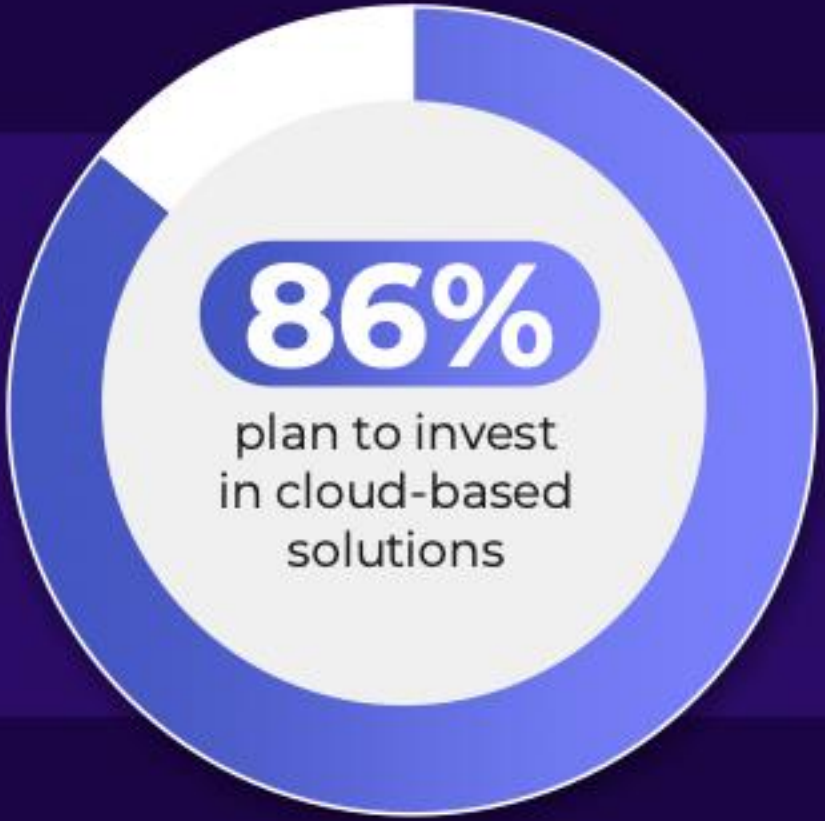
What would your network look like?



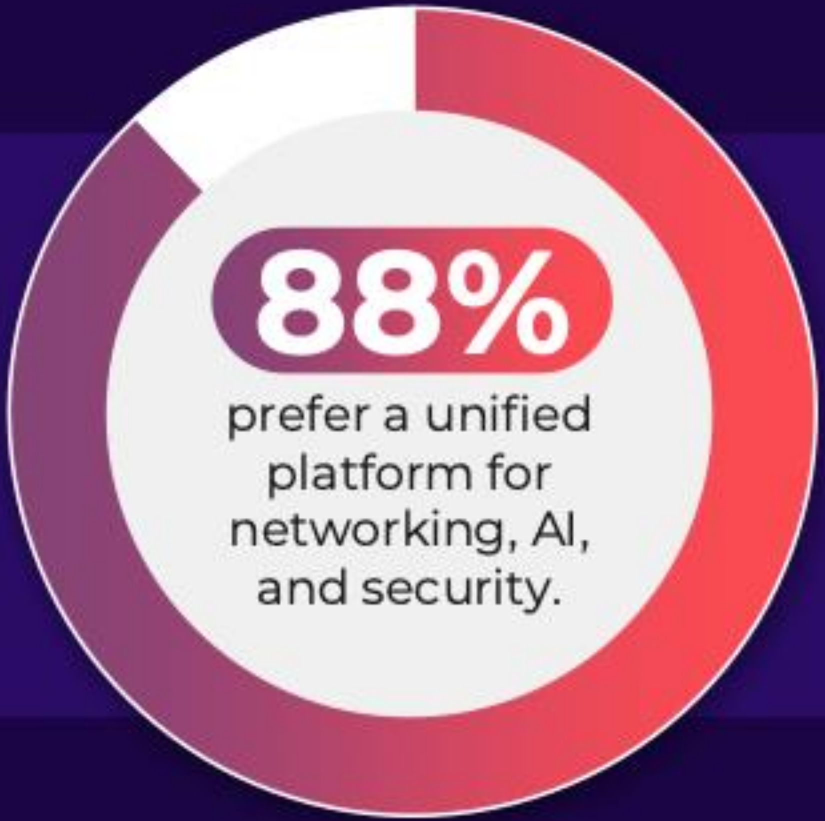
Why Fabric?

- Affordable – Same cost as any other NOS
- Hyper-Segmentation – L2 or L3 VRF design – multiple segmented routing tables – secure, no use of VLANs and ACLs
- True Service Provider capabilities – Create multiple secure separate networks on the same hardware
- Single protocol loopless topology - No more Spanning Tree Protocol pain and agony
- Handle Multi-cast with ease – Native with SBP - PIM not needed
- Never been hacked – Built on Ethernet switched paths which is inherently a dark topology
- Auto sensing ports at the edge – Auto provision new edge switches and wired devices – Secure zones created automatically as devices are moved to different ports
- Field Proven – Over 5k installations across the world
- Built using Industry Standards – IEEE 802.3aq and IETF - RFC 6329 – Interoperates with ANY network

Concord CIO Insights Report: Top 2 Findings

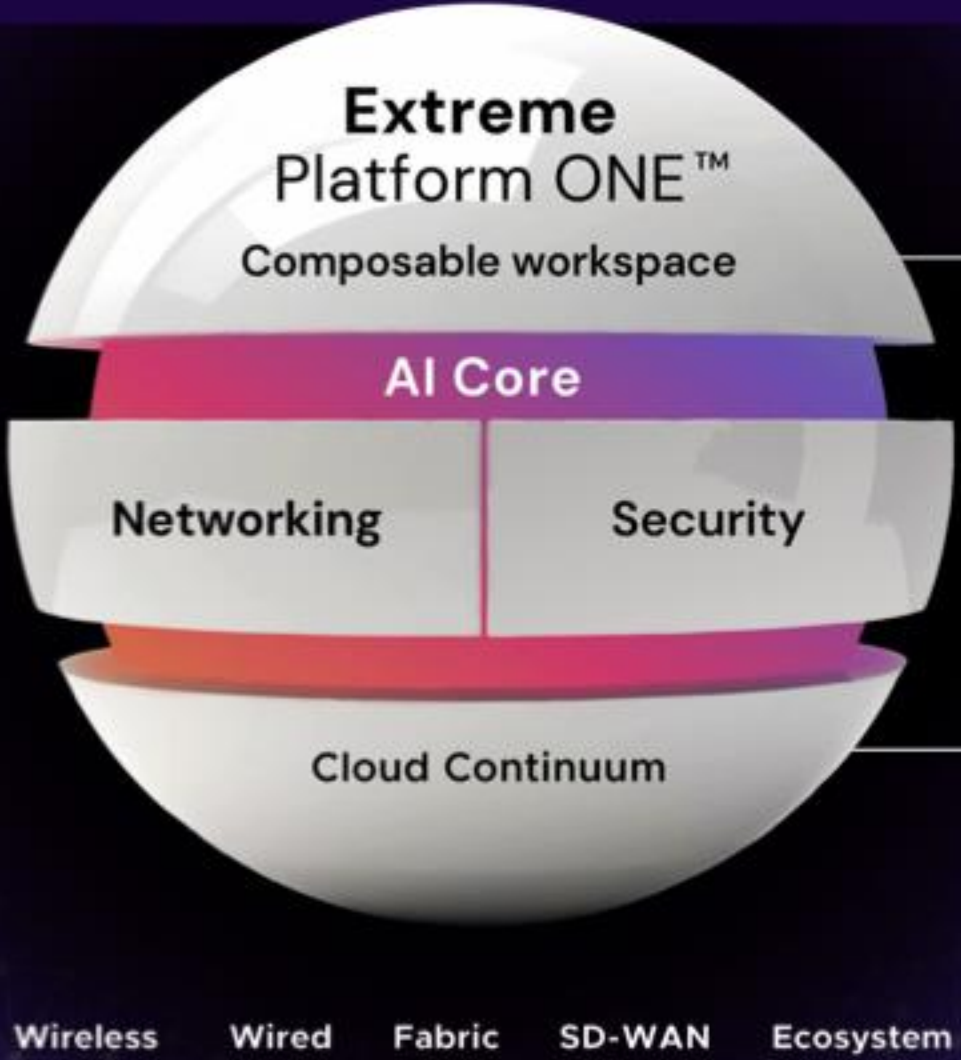


86% plan to invest in cloud-based solutions



88% prefer a unified platform for networking, AI, and security.

Secure Connectivity Made Simple



Secure, scale, and automate connectivity with Extreme Platform ONE, the first all-in-one networking platform with integrated security and conversational, multimodal,
and agentic AI.

Extremes Mission for the future is to provide a modern networking platform that delivers AI-Readiness Innovation, Management Simplicity, Built in Security, Fiscal Discipline and Compliance Policy Adherence

And the Future is Now!

Questions

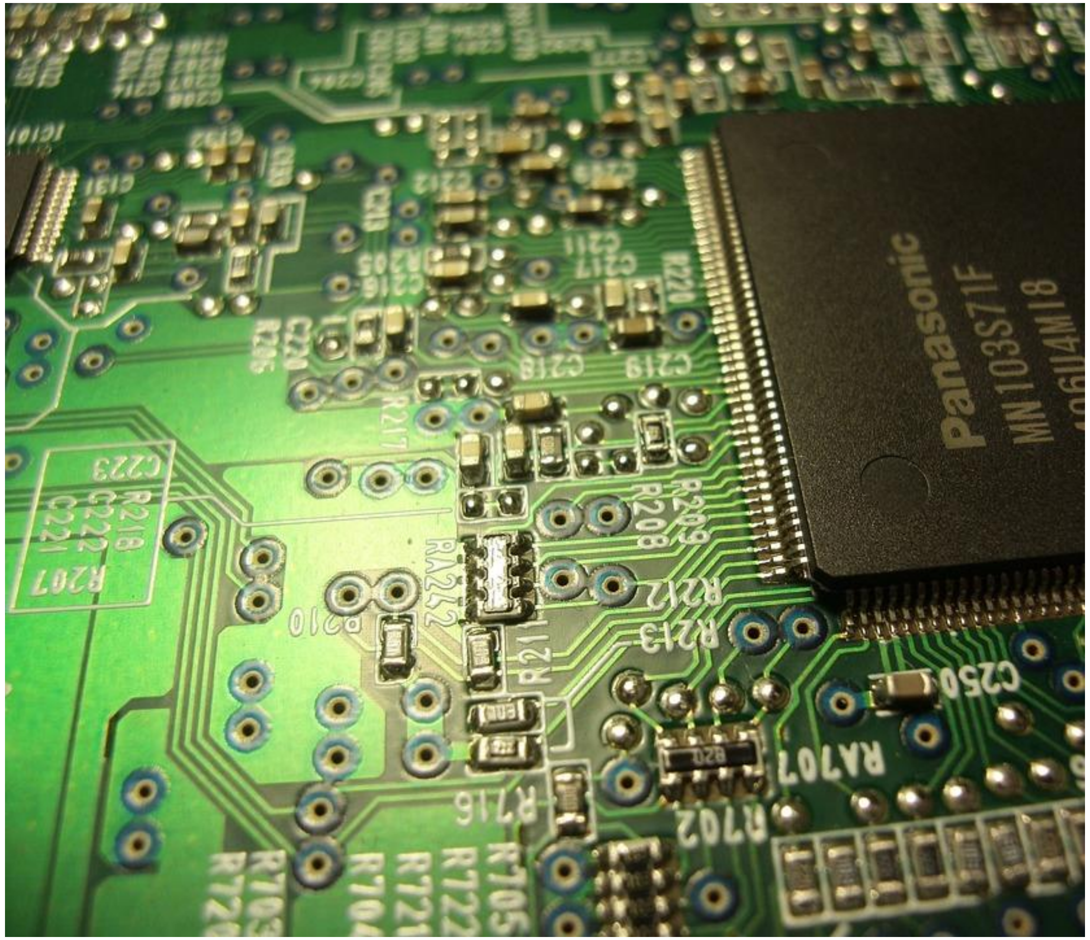
EXTREME NETWORKS

February Meeting: Managing Technical Debt

- ➢ Helen Patton - Cisco
- ➢ Cybersecurity Executive Advisor
- ➢ Adjunct Professor of Industry Practice
- ➢ Sponsored by Xerox IT Solutions

January Parting Shots

- Local Gov’t/Public Safety SIG – Sun Watch Room
- Education SIG – Wright Patt Room
- Defense Contractor SIG – Hawthorn Room
- Register for CMMC Workshop, Monthly Meetings
- Cyber Insurance Summit
- 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

Extreme® networks

SECURECYBER™

Proven. Proactive. Personalized.