
go
cyber
COLLECTIVE

February Announcements

Serving Our Communities

- Thank you, Xerox IT Solutions!
- GoCyber Website Complete
- Cyber 101 for Law Enforcement – March 4 - $250 (201 for LE is April 8)
- GoCyber/Cincinnati InfraGard February 23 – Members Only
- Internship Summit – Feb. 25, 10 AM – 11:30 AM
- Cyber Insurance Summit – March 17, 10 AM – 11:30 AM

gocyber COLLECTIVE

Certified Red Team Fundamentals

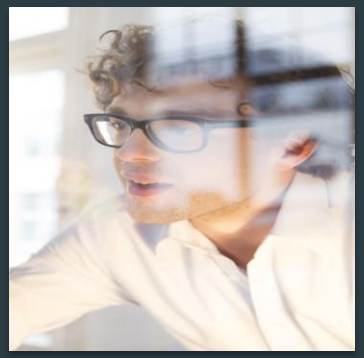
- An Introduction to Thinking Like an Attacker
- Tuesday, March 24th, 2026
- 9:00 AM – 3:30 PM (Check-in begins at 8:30 AM)
- $999
- Lunch provided
- Register today!

gocyber COLLECTIVE

Introduction to Cybersecurity for Water & Wastewater Operators

- Ohio EPA Certified
- 15 Contact Hours
- $1,800

Your CMMC Journey



2026 CMMC Workshops

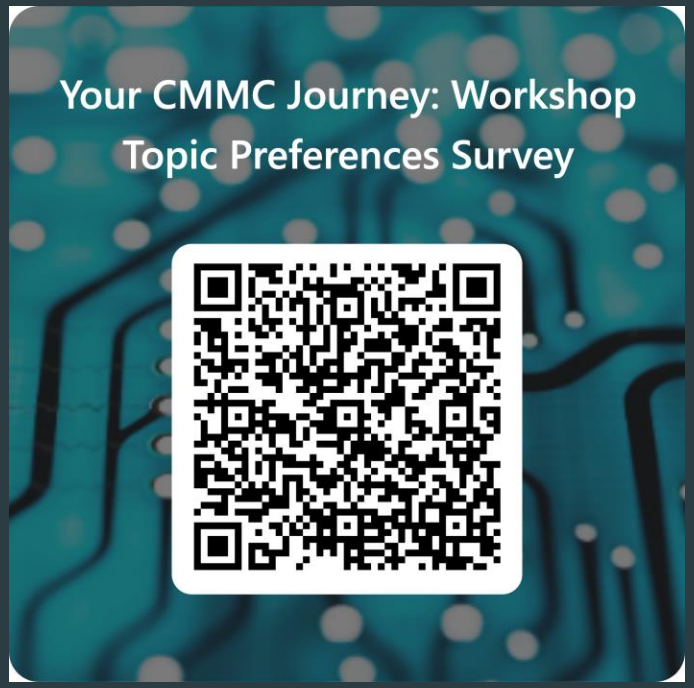
-April 7th

-June 9th

-August 4th

-October 6th

-December 8th



CMMC Focus Topics

-Defining Scope & Boundary

-Creating, Populating, and Updating SSP & POAMs

-Service Providers & Cloud

-Selecting & Working with C3PAO

-Categorizing Assets per CMMC Scoping

-Understanding Regs, Resources, Contracts, and Flow Down Requirements

gocyber COLLECTIVE

February GoCyber Collective Keynote Speaker

-Helen Patton - Cisco

-Cybersecurity Exec. Advisor

-Product CISO - Cisco

-CISO: The Ohio State University

-Adjunct Professor: University of Canberra

gocyber COLLECTIVE

Technical Debt

Eliminating Risk and Accelerating Business Outcomes

Helen Patton, Executive Cybersecurity Advisor

February 2026

Why This Topic?

Scarce Resources

AI Acceleration

Quantum

Complexity

Agenda

Understanding Tech Debt

Public Policies

Why Eliminating It Is Hard

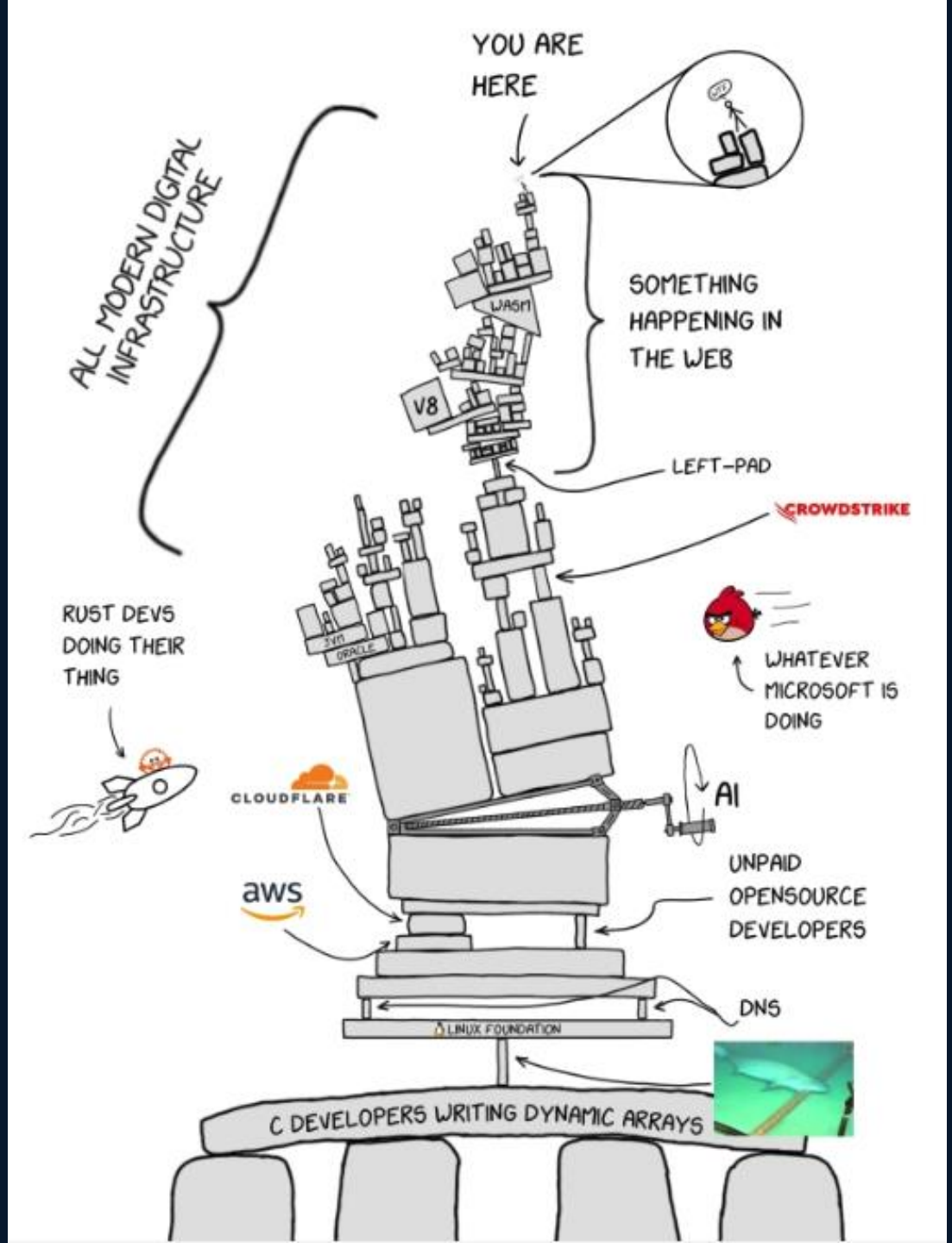
Strategies

Case Study

Wrapping Up

Understanding Technical Debt

What Is Tech Debt?



https://programmerhumor.io/memes/tech-stack

The cost, in terms of money and effort, required for a company to keep its IT systems up to date and capable of meeting business needs

Accenture (2024)

What Is Tech Debt?

Software/ Code

- Insecure Code
- Lack of Testing
- Legacy Protocols

Design/ Architecture

- Limited Scalability or Flexibility
- Limited Maintainability
- Lack of Automation

Infrastructure

- EOL or EOS Hardware
- Inefficient CI/CD Pipelines

Processes

- Manual
- Missing Design Review
- Vendor Lock In

Documentation/ Knowledge

- Staffing Single Points of Failure
- Undocumented
- Poor Onboarding Practice
- Untrained staff

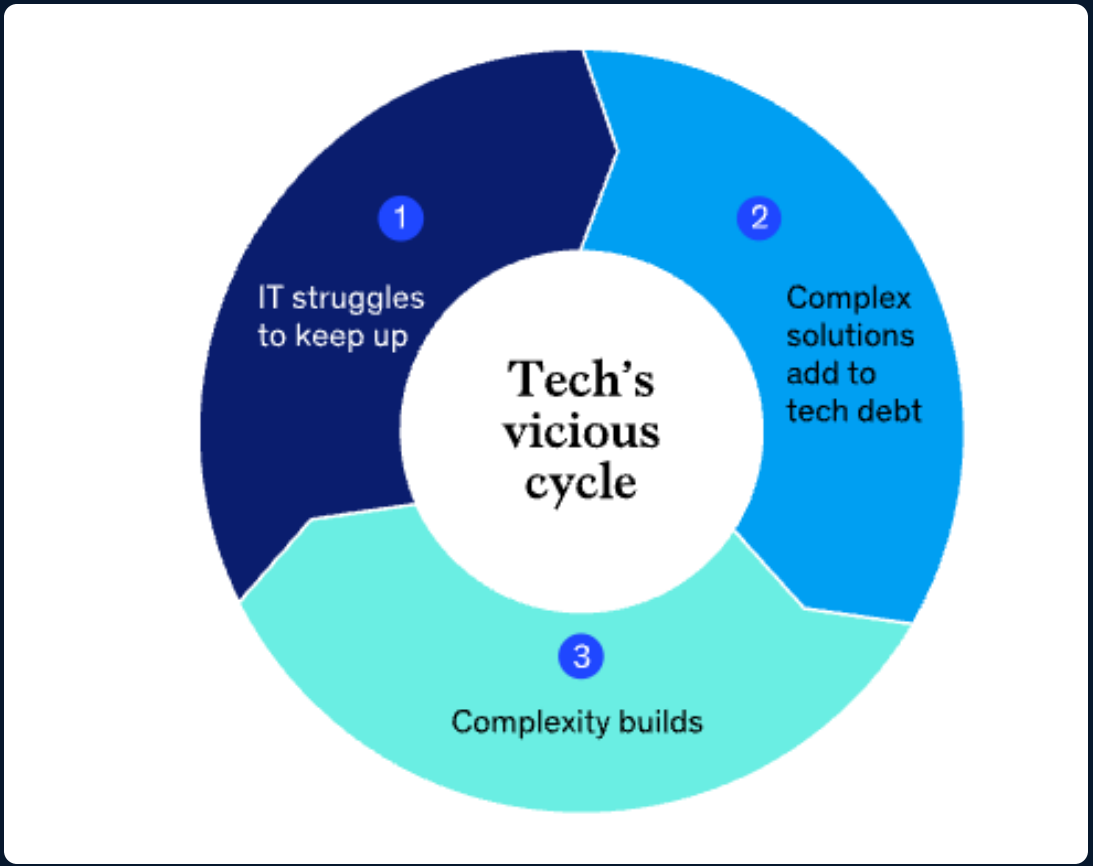
Data

- Old/ Inaccurate
- Duplication
- Past Retention Date

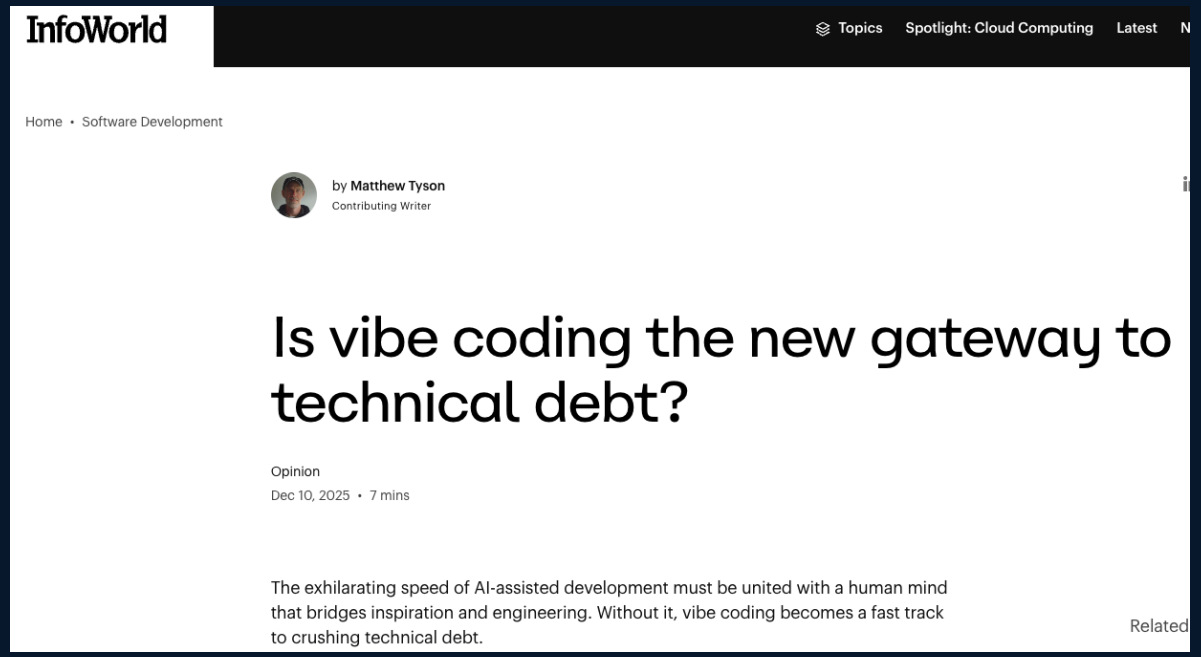
Intentional/Strategic

Accidental/Negligent

Tech Debt Tetris



[McKinsey 2023: Breaking Technical Debt's Vicious Cycle To Modernize Your Business]



https://www.infoworld.com/article/4098925/is-vibe-coding-the-new-gateway-to-technical-debt.html

So What? Part 2

Splunk: 2025 CISO Report: https://www.splunk.com/en_us/pdfs/gated/ebooks/ciso-report-2025.pdf

If It Ain’t Broke…

Slows Innovation

Increases Attack Surface

Increases Operational Costs

Technical Lock-in

Reduces Business Agility

Talent/Morale Impact

…Compounds Over Time

Technical Debt Public Policies

US Public Policies

Jurisdiction	Policy/Initiative	Focus Area	Effect on Tech Debt	Notes
Federal	Modernizing Government Technology Act (MGT Act) / Technology Modernization Fund (TMF)	Legacy IT Modernization	Provides funding and mandates for federal agencies to modernize outdated systems	Enables debt reduction through infrastructure and system updates
	Executive Order 14028 (Cybersecurity)	Cybersecurity Standards	Mandates modernization for security compliance, impacting legacy tech systems	Pushes agencies to adopt zero-trust, MFA, encryption, etc.
	Federal Information Security Modernization Act (FISMA 2014)	Information Security	Pressures agencies to replace systems that can't meet current security standards	Indirectly drives tech debt remediation
	GAO Oversight & Reports (2025)	IT Accountability	Identifies high-risk legacy systems and recommends modernization plans	Encourages policy adoption and remediation tracking
	DoD Software Modernization Strategy (2025‚Äì26)	Defense IT Modernization	Strategy to update software, platforms, and processes; addresses broad technical debt	Includes infrastructure, tools, and workforce readiness
U.S. States (various)	State Cybersecurity Laws	Security Compliance	Incentivizes upgrading insecure or legacy systems	Enacted in nearly all states; focuses on breach notification, data protection
California	FI$Cal Modernization Project	State Financial Systems	Replaced hundreds of legacy systems with unified modern platform	Large-scale example of state-level tech debt remediation
Various States (2025 bills)	State IT Modernization Bills	Cybersecurity & Innovation	Funds and plans proposed to modernize state systems and enhance security	Emerging trend, still fragmented

Why Eliminating Tech Debt Is Hard

Common Barriers & Cultural Challenges

Short Term Thinking

Limited Budget/ Unclear ROI

Lack of Visibility/ Awareness

Unclear Prioritization Criteria

Cultural Resistance

Assuming Newer = Better

Insecure/ Unhardened Products

Shared Accountability

Cultural Resistance

- Cross-Functional Ownership is needed
- Business stakeholders MUST be involved

IT	Security	Finance	Architecture	Product Mgmt	Business Leadership	Risk Mgmt

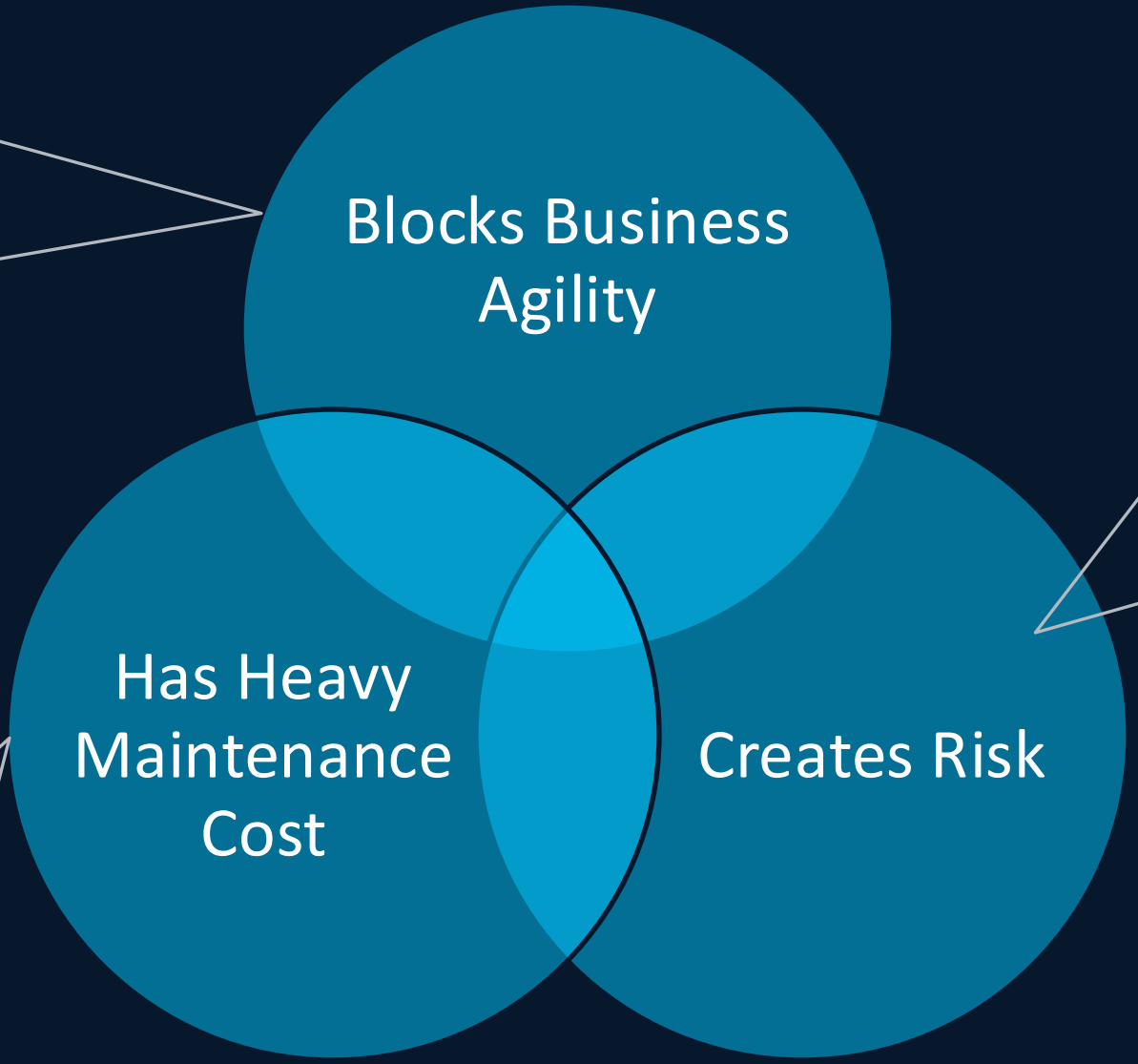
Tech Debt Elimination Strategies

Not All Tech Debt Is Equal (in Harm)

Not All Tech Debt Needs To Be Paid Off

Focus Your Program on Debt That:

- Debt In Strategic Assets
- Interferes with time to market/ feature delivery
- Infrastructure that doesn't scale with demand



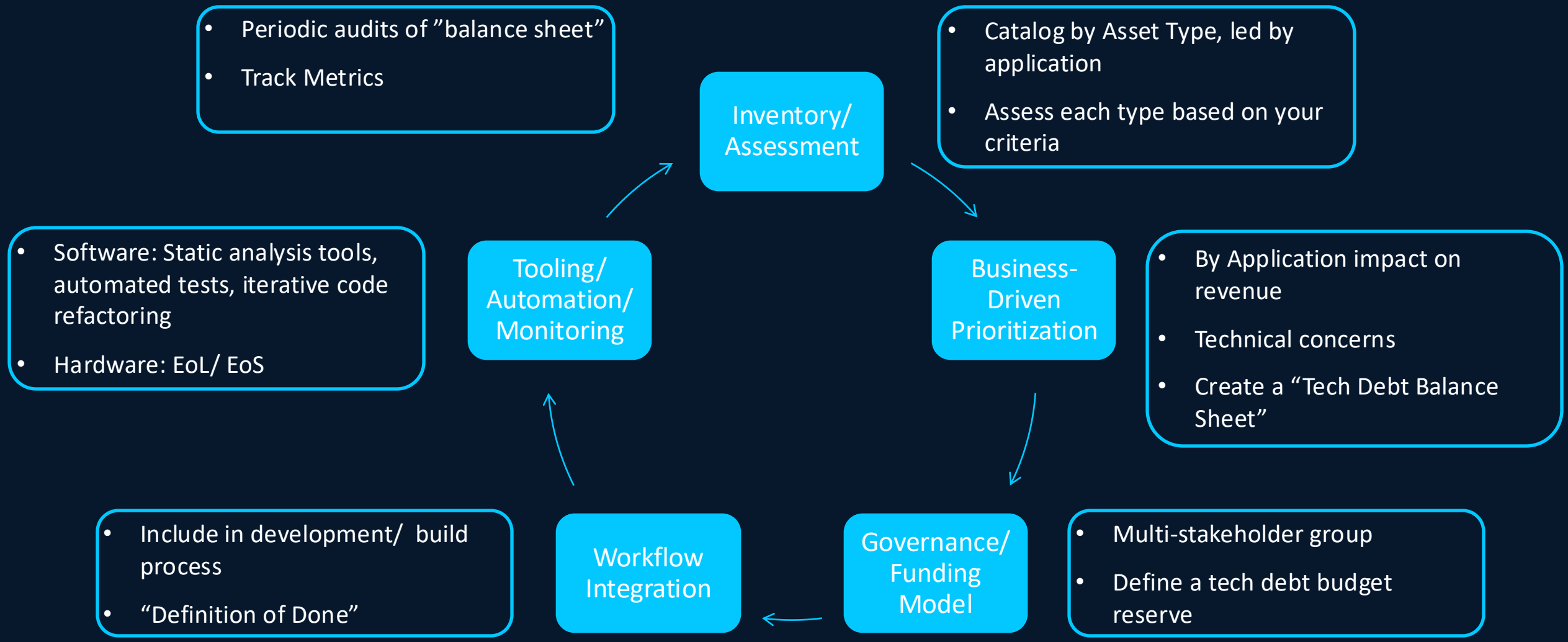
- Unpatched
- Outdated protocols
- Insecure Code
- Insecure processes

- Interferes with time to market
- Brittle architecture
- Causes burnout of people

Tech Debt Governance Includes:

General Items	• End of Life/Support activities • Upgrade cadence • Mandatory periodic review
Budget Allocation	• Enforce tech refresh reserve (15%?) of IT Spend
Exceptions	• Explicit executive approval of exceptions must include payback plan
"Definition of Done"	• Require clearance any debt before production release
Tech Debt Balance Sheet	• Liabilities = Assets/Systems • Interest = Ongoing Maintenance Cost (people, process, licensing, security)
Automation	• Require tools to detect, track, and avoid debt accumulation • Establish and monitor program metrics

Programmatic and Operational Actions

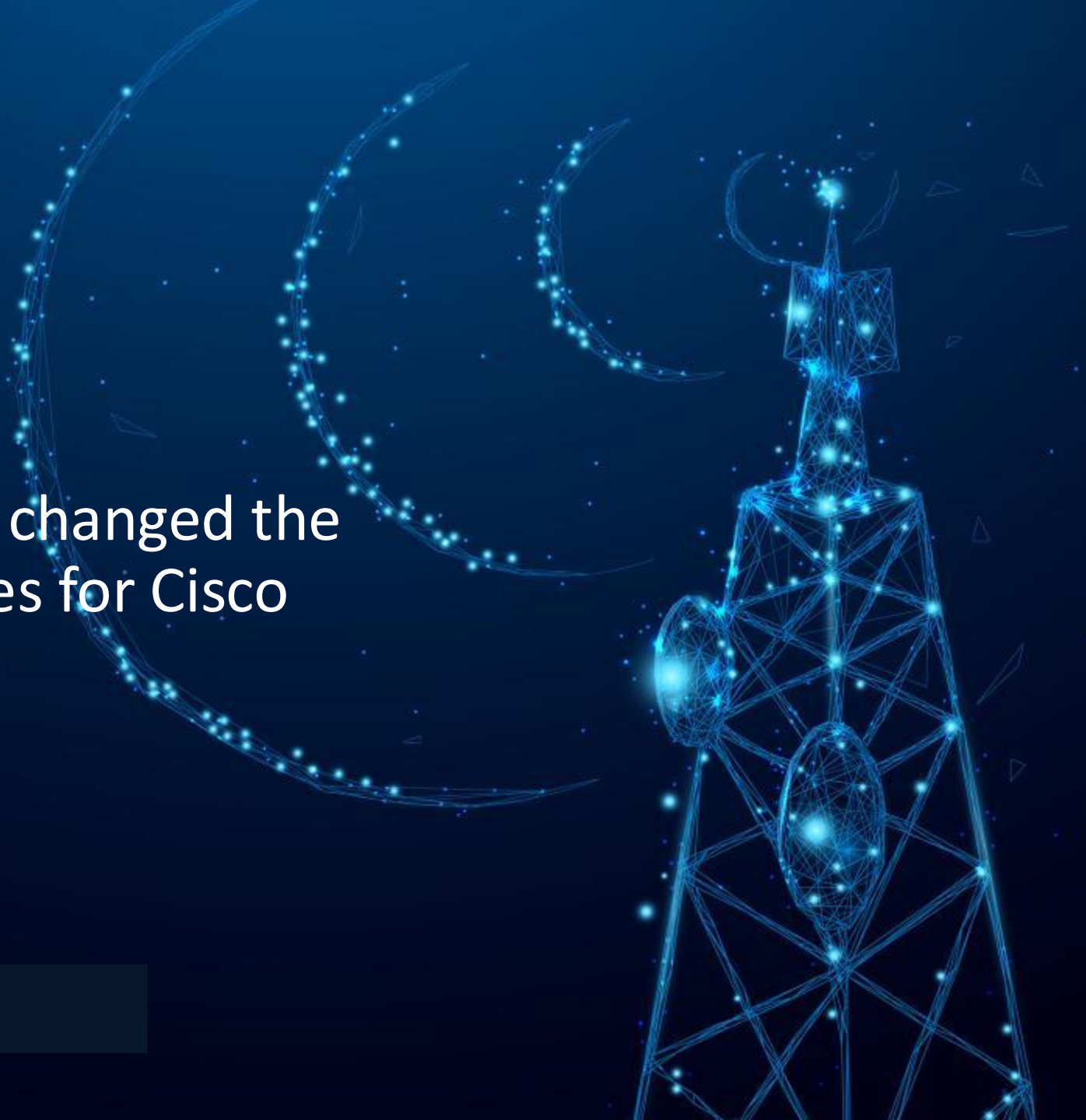


Cisco Case Study:

Resilient Infrastructure
aka
Project Broccoli

https://www.cisco.com/c/en/us/about/trust-center/resilient-infrastructure.html#~proactive-security

Global threat actors have changed the game and raised the stakes for Cisco and industry



For more information see the Talos Blog from February 2025
Weathering the storm: In the midst of a Typhoon

Cisco Resilient Infrastructure focus areas

Driving small but significant improvements for big impact

Secure by Default

Shift the dynamics in our portfolio so hardening guides are obsolete

Insecure Features

Deprecate and remove insecure features, protocols and ciphers in our code

New Capabilities

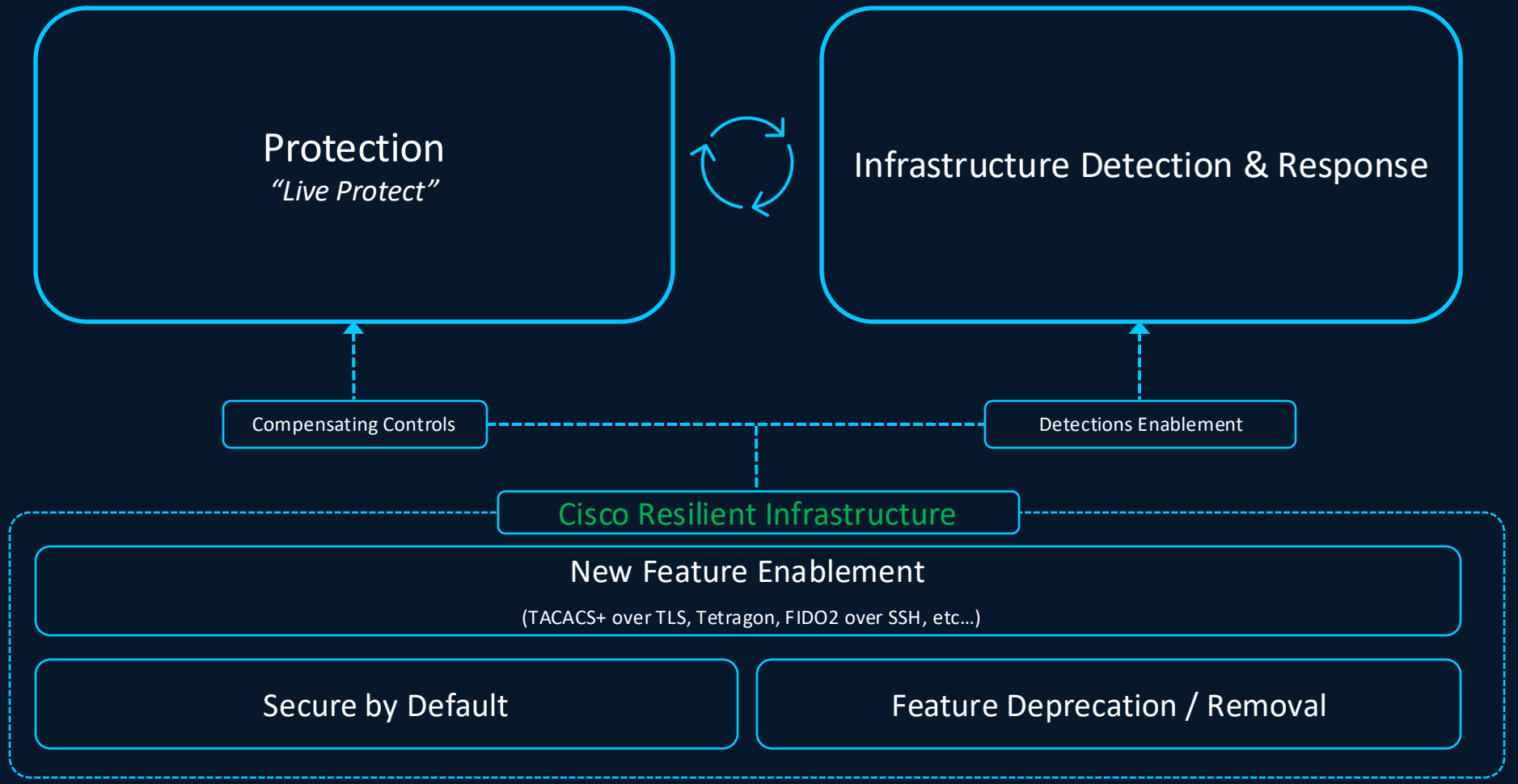
Implement new and modern security capabilities that enrich our product security

Detect & Respond

Ensure platforms provide for higher level protections and monitoring

A compelling vision of security and resilience

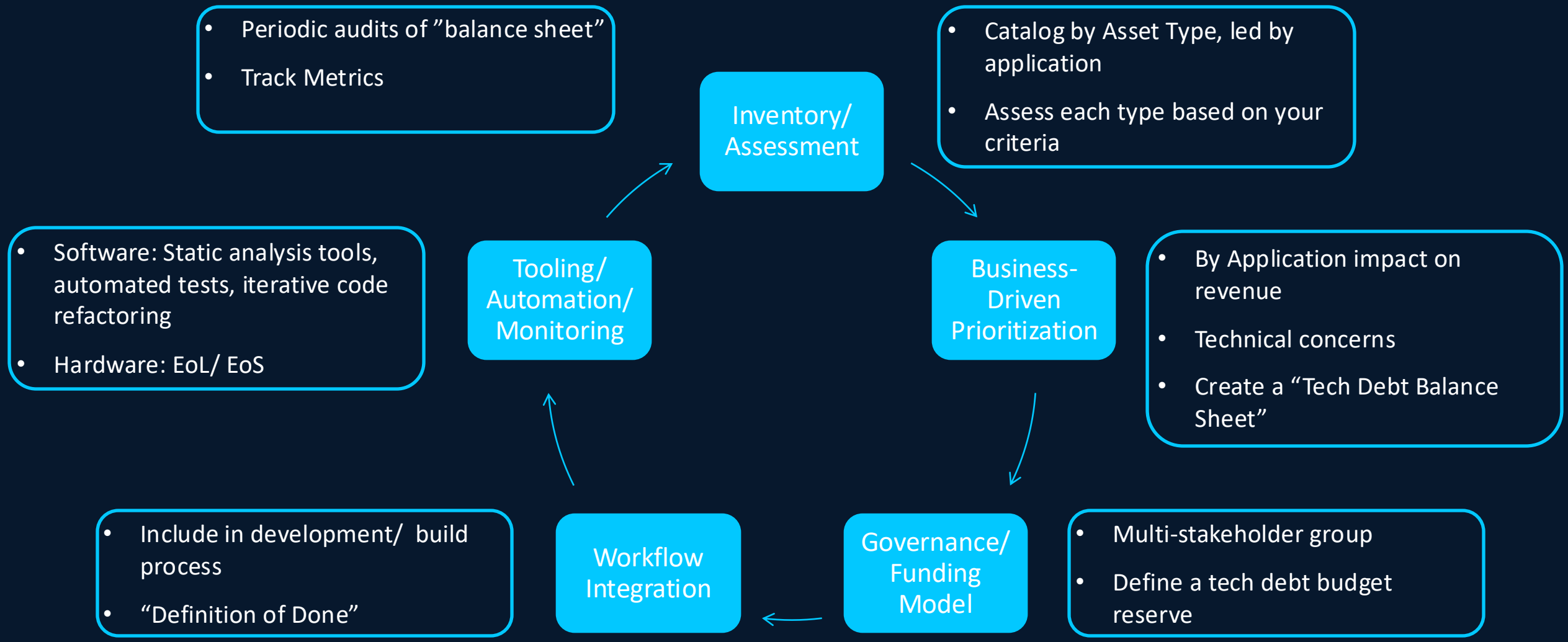
Enhanced Detections & Protections



Baseline Security Posture

Wrapping Up

What Are You Missing?



Final Thoughts

- Tech debt is more than just hardware/software refresh
- Use a business-aligned, governance-driven approach
- Expect hardened products from vendors
- Prioritize based on business impact, risk, and maintenance burden
- Look for the applications (and associated technologies) with the biggest business impact
- Treat tech debt like financial debt and be strategic about when to assume it, pay it back, and how to budget for it
- Emphasize cross-functional ownership and governance
- Have a programmatic and operational approach to tech debt avoidance and elimination

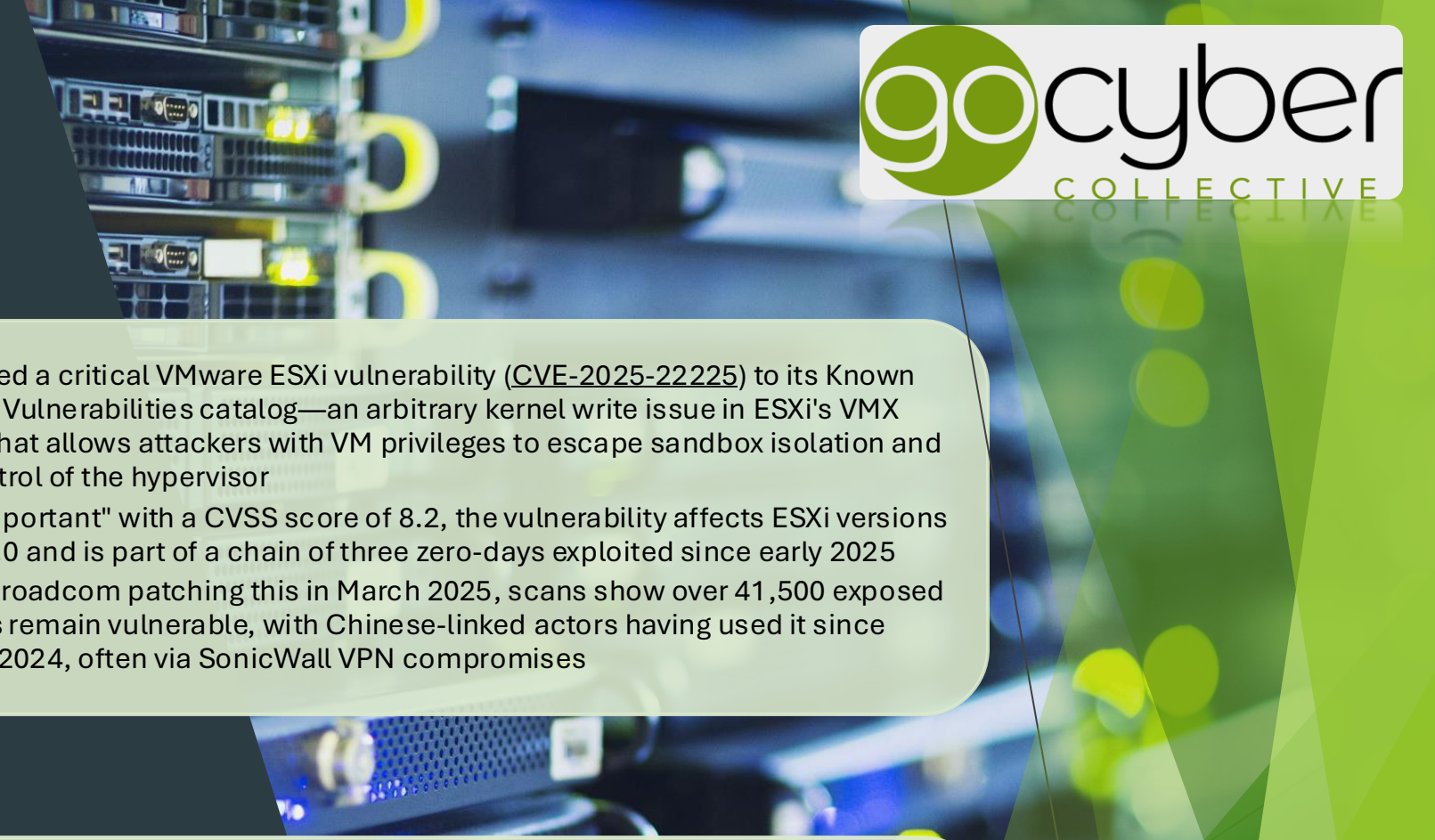
Thank You

hpatton@cisco.com
https://www.cisohelen.com

Threat Briefing

- Joe Tinney
  -SecureCyber
  -VP of Cyber Operations

February Threat Briefing



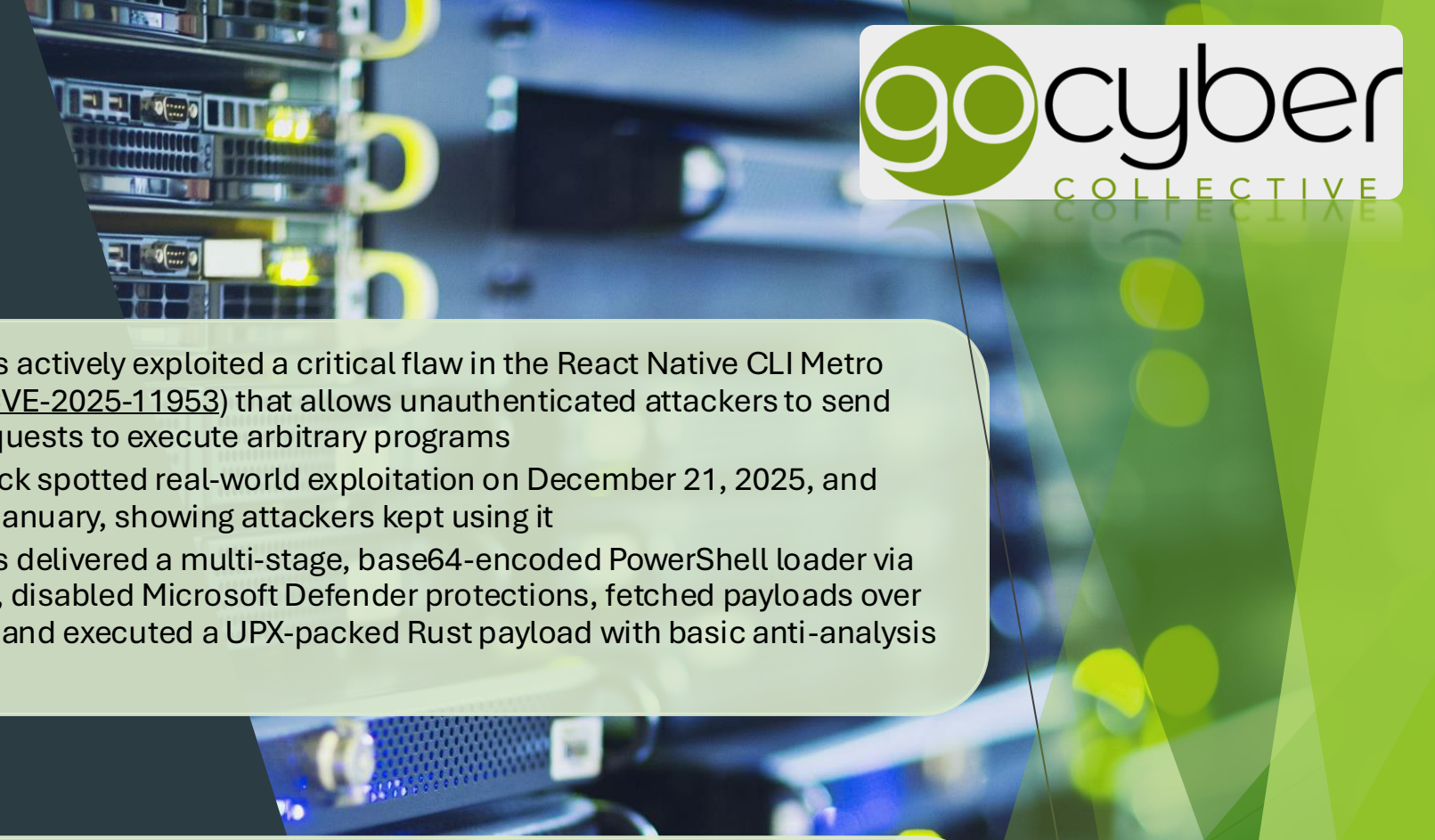
VMware ESXi Zero-Day Exploited by Ransomware Gangs

- CISA added a critical VMware ESXi vulnerability (CVE-2025-22225) to its Known Exploited Vulnerabilities catalog—an arbitrary kernel write issue in ESXi's VMX process that allows attackers with VM privileges to escape sandbox isolation and seize control of the hypervisor
- Rated "Important" with a CVSS score of 8.2, the vulnerability affects ESXi versions 7.0 and 8.0 and is part of a chain of three zero-days exploited since early 2025
- Despite Broadcom patching this in March 2025, scans show over 41,500 exposed instances remain vulnerable, with Chinese-linked actors having used it since February 2024, often via SonicWall VPN compromises

SolarWinds Web Help Desk RCE Under Active Exploitation

- CISA flagged a critical remote code execution vulnerability in SolarWinds Web Help Desk (CVE-2025-40551) as actively exploited, with this untrusted data deserialization bug (CVSS 9.8) allowing unauthenticated attackers to run arbitrary commands on hosts
- Affecting versions up to 12.8.8 Hotfix 1, it's one of four critical flaws patched in January 2026, with exploitation being low-complexity and requiring no privileges

February Threat Briefing



React Native CLI Zero-Day Exploited Before Disclosure

- Attackers actively exploited a critical flaw in the React Native CLI Metro server (CVE-2025-11953) that allows unauthenticated attackers to send POST requests to execute arbitrary programs
- VulnCheck spotted real-world exploitation on December 21, 2025, and again in January, showing attackers kept using it
- Attackers delivered a multi-stage, base64-encoded PowerShell loader via cmd.exe, disabled Microsoft Defender protections, fetched payloads over raw TCP, and executed a UPX-packed Rust payload with basic anti-analysis features

Fortinet FortiGate SSO Vulnerabilities Under Automated Attack

- Fortinet FortiGate firewalls faced a wave of automated attacks exploiting vulnerabilities in their Single Sign-On features (CVE-2025-59718 and CVE-2025-59719), enabling attackers to add unauthorized admin users, enable VPN access, and export firewall configurations in seconds
- Fortinet confirmed working to completely plug a FortiCloud SSO authentication bypass vulnerability following reports of fresh exploitation activity on fully-patched firewalls, with the activity found to exploit an incomplete patch for CVE-2025-59718 and CVE-2025-59719

February Threat Briefing

Chrome Zero-Day Actively Exploited in the Wild

A use after free vulnerability in CSS in Google Chrome prior to 145.0.7632.75 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page

The vulnerability is actively being exploited in the wild and was added to the CISA Known Exploited Vulnerability list, with one proof-of-concept exploit available on GitHub

Attackers can exploit this by hosting malicious web pages that victims visit, triggering code execution within the Chrome sandbox when users interact with the malicious page, enabling attackers to steal sensitive data, harvest credentials, and compromise system integrity

gocyber COLLECTIVE

February GoCyber Collective Sponsor – Xerox IT Solutions

Jim Meincke
-ISG Lead/Solutions Architect

Roger Gregory
-Director of Security Solutions

xerox IT Solutions

gocyber COLLECTIVE

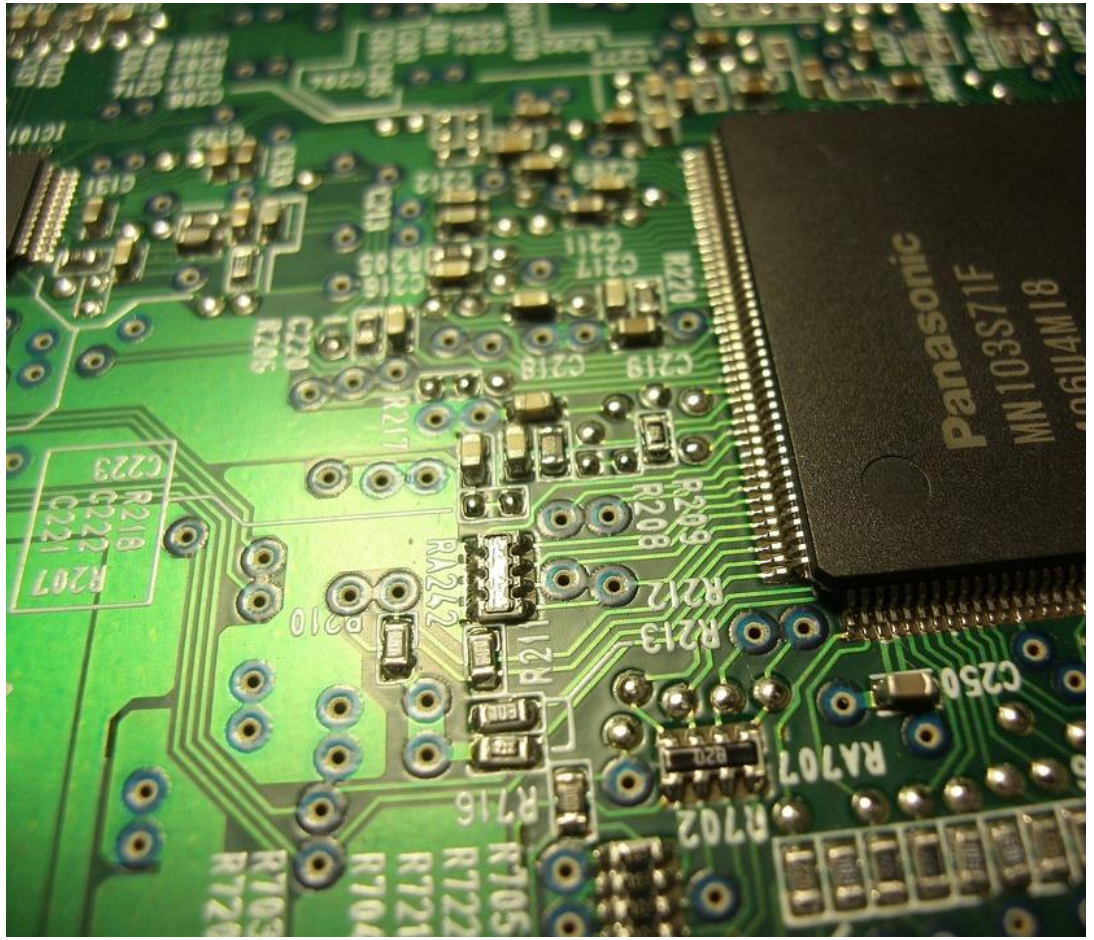
March Meeting:

- Ken Fanger – On Technology Partners
- Consultant: Risk, Security, DR
- Security: There is no Cybersecurity
- Sponsored by T-Mobile

gocyber COLLECTIVE

February Parting Shots

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



gocyber COLLECTIVE

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

xerox IT Solutions

SECURECYBER™
Proven. Proactive. Personalized.

gocyber COLLECTIVE