



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



Certified Red Team Fundamentals

RED TEAM
WORKSHO

- ▶ 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!

Certified Red Team Fundamentals





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.

***OHIO EPA approved for 15 contact hours (OEPA-B88110505-OM)**

“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

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.



THU, APRIL 2
8 AM – 4:30 PM

FRI, APRIL 3
8 AM – 3:30 PM

Tyler Technologies Building
201 Tyler Way, Moraine, OH



REGISTER TODAY!

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.

(937) 938-0888

201 Tyler Way, Moraine, OH 45439

gocybercollective.org

Introduction to Cybersecurity for Water & Wastewater Operators

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

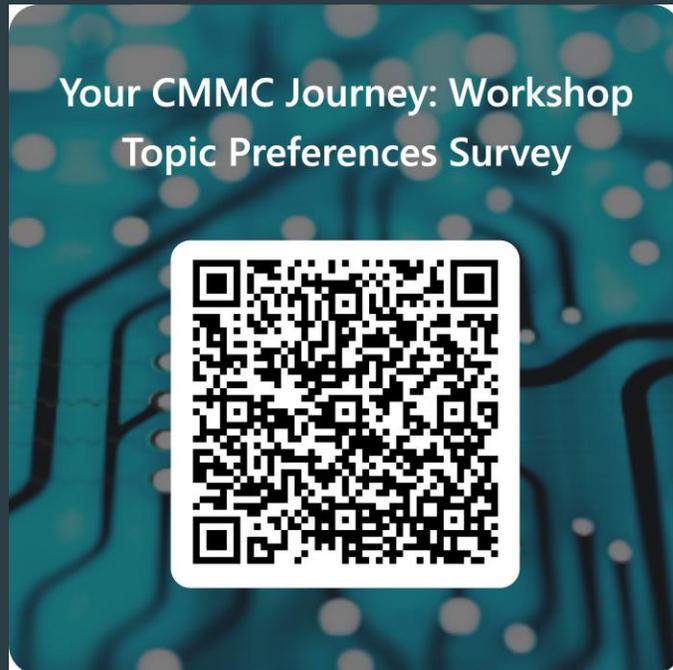


Your CMMC Journey



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





February GoCyber Collective Keynote Speaker

- Helen Patton - Cisco
- Cybersecurity Exec. Advisor
- Product CISO - Cisco
- CISO: The Ohio State University
- Adjunct Professor: University of
Canberra



Technical Debt

Eliminating Risk and Accelerating Business Outcomes

Helen Patton, Executive Cybersecurity Advisor



Why This Topic?

Scarce
Resources

AI
Acceleration

Quantum

Complexity

Agenda

Understanding Tech Debt

Public Policies

Why Eliminating It Is Hard

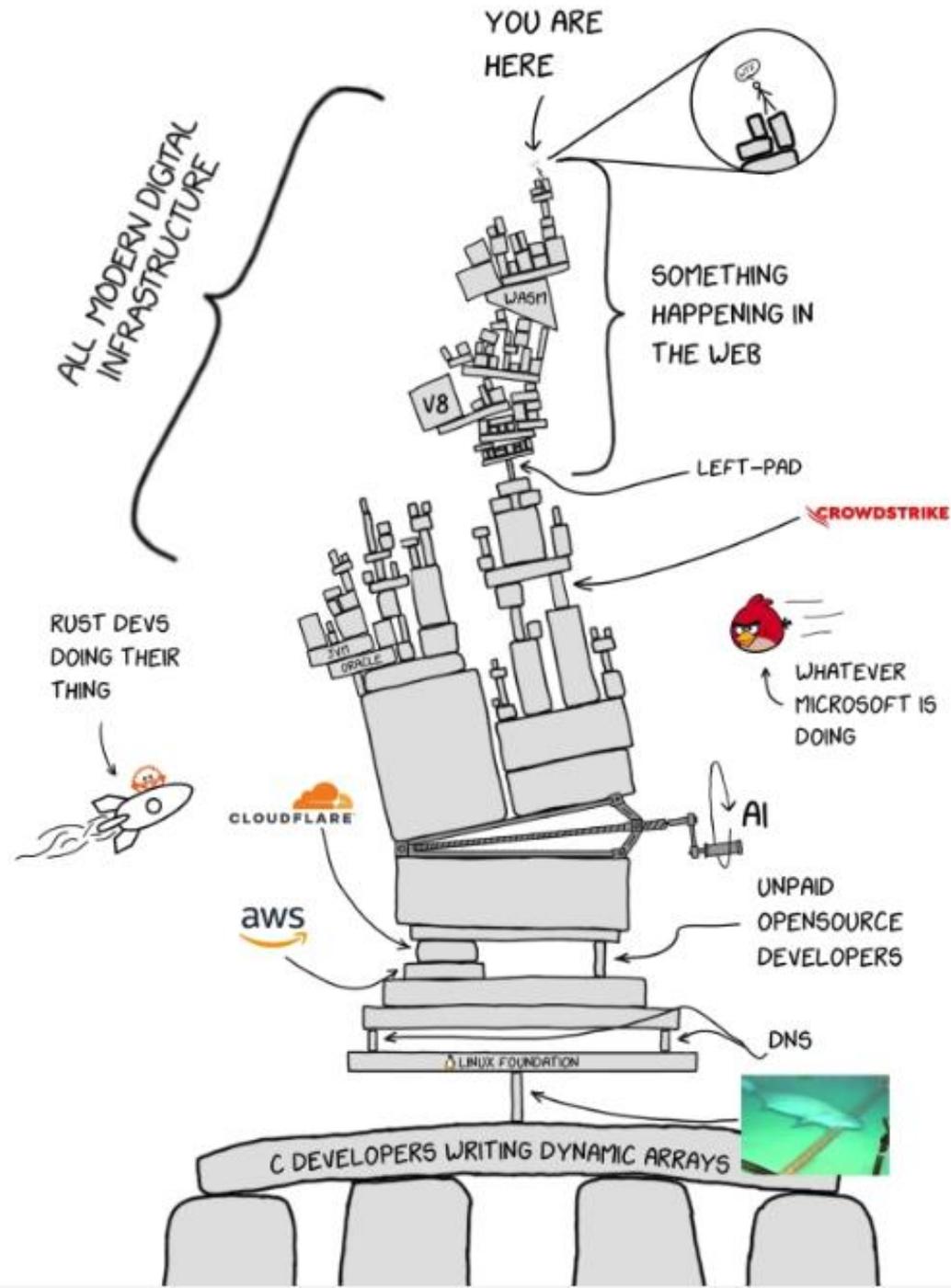
Strategies

Case Study

Wrapping Up

Understanding Technical Debt

What Is Tech Debt?





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

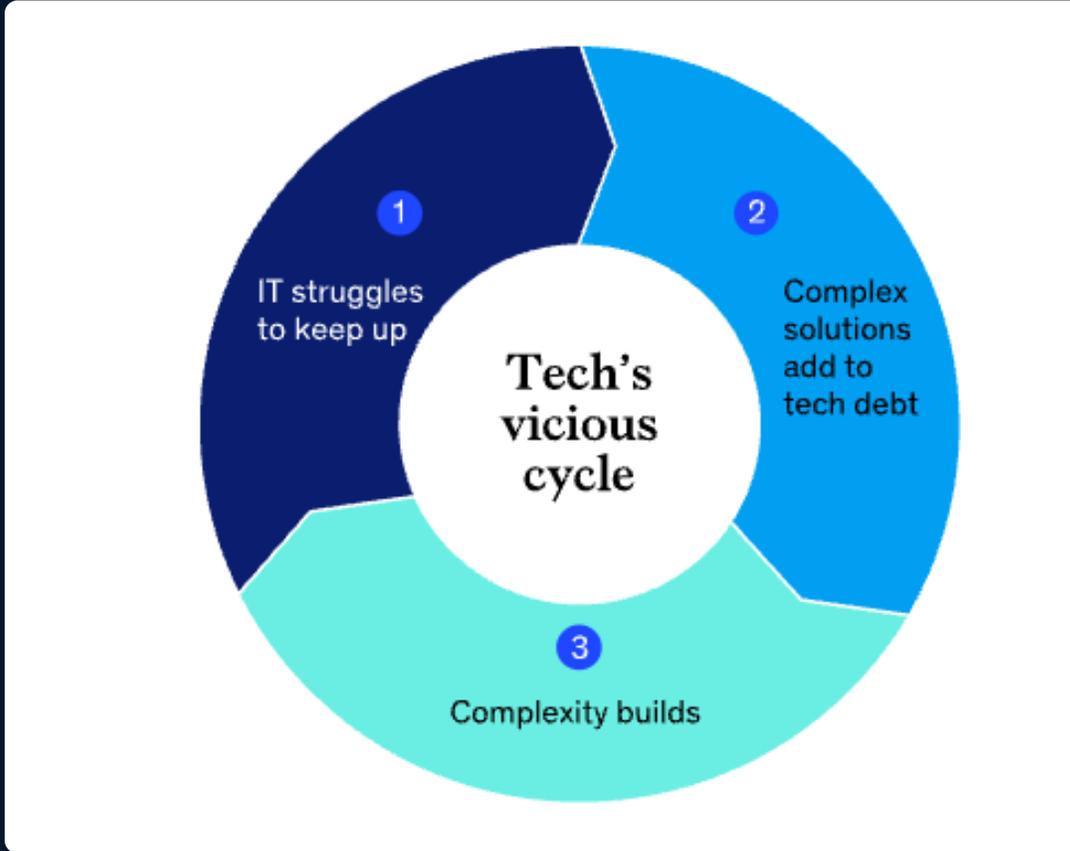
Data

- Old/ Inaccurate
- Duplication
- Past Retention Date

Intentional/Strategic

Accidental/Negligent

Tech Debt Tetris



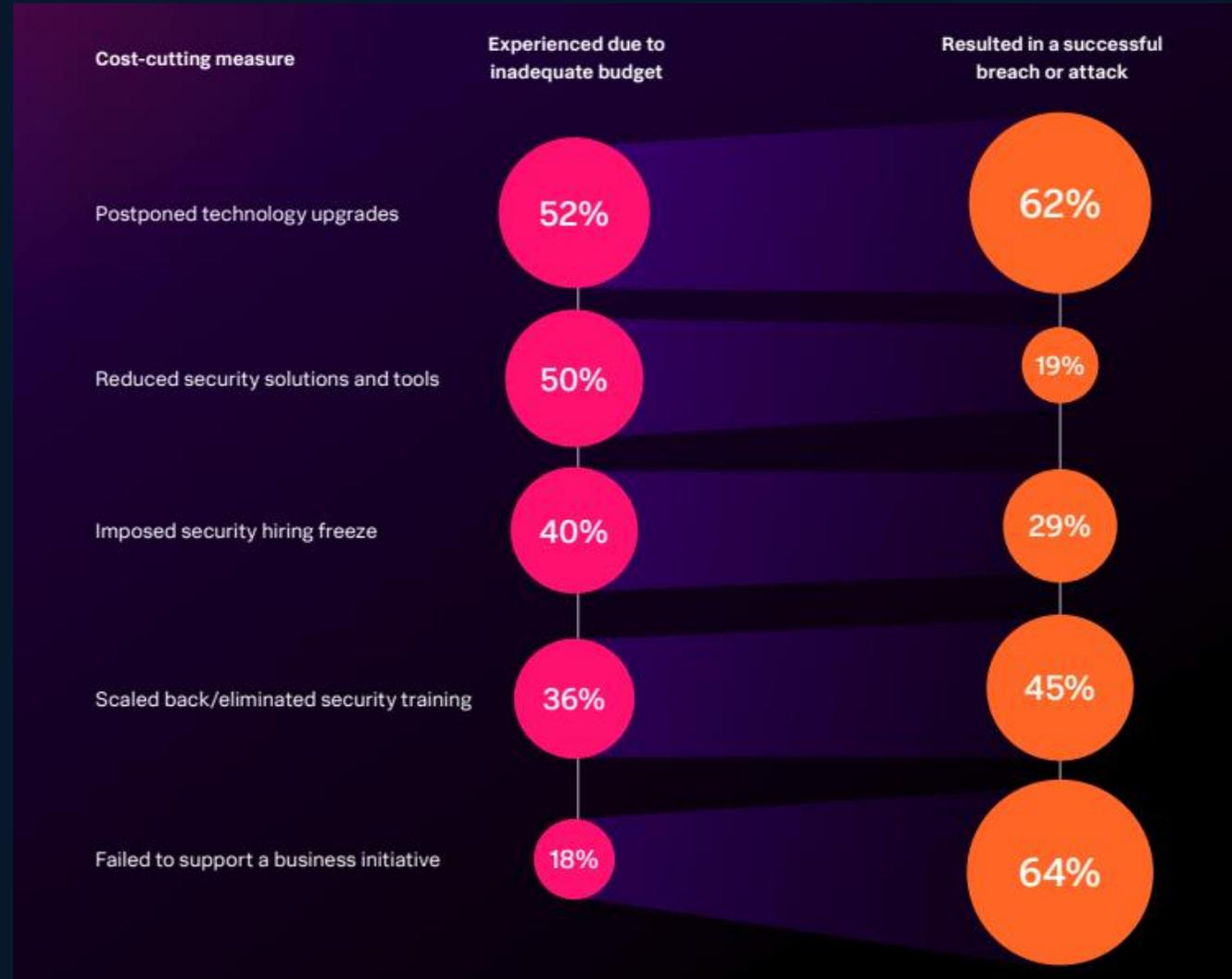
[McKinsey 2023: Breaking Technical Debt's Vicious Cycle To Modernize Your Business](#)

The screenshot shows the top portion of a web article. At the top left is the "InfoWorld" logo. On the right, there are navigation links: "Topics", "Spotlight: Cloud Computing", "Latest", and "N". Below the navigation is a breadcrumb trail: "Home • Software Development". The author's name and title are displayed: "by Matthew Tyson, Contributing Writer". The main title of the article is "Is vibe coding the new gateway to technical debt?". Below the title, it says "Opinion" and "Dec 10, 2025 • 7 mins". A short introductory paragraph begins: "The exhilarating speed of AI-assisted development must be united with a human mind that bridges inspiration and engineering. Without it, vibe coding becomes a fast track to crushing technical debt." On the right side, there is a "Related" link.

<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...

Increases
Operational Costs

Slows Innovation

Increases Attack
Surface

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, 26)	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
----	----------	---------	--------------	--------------	---------------------	-----------

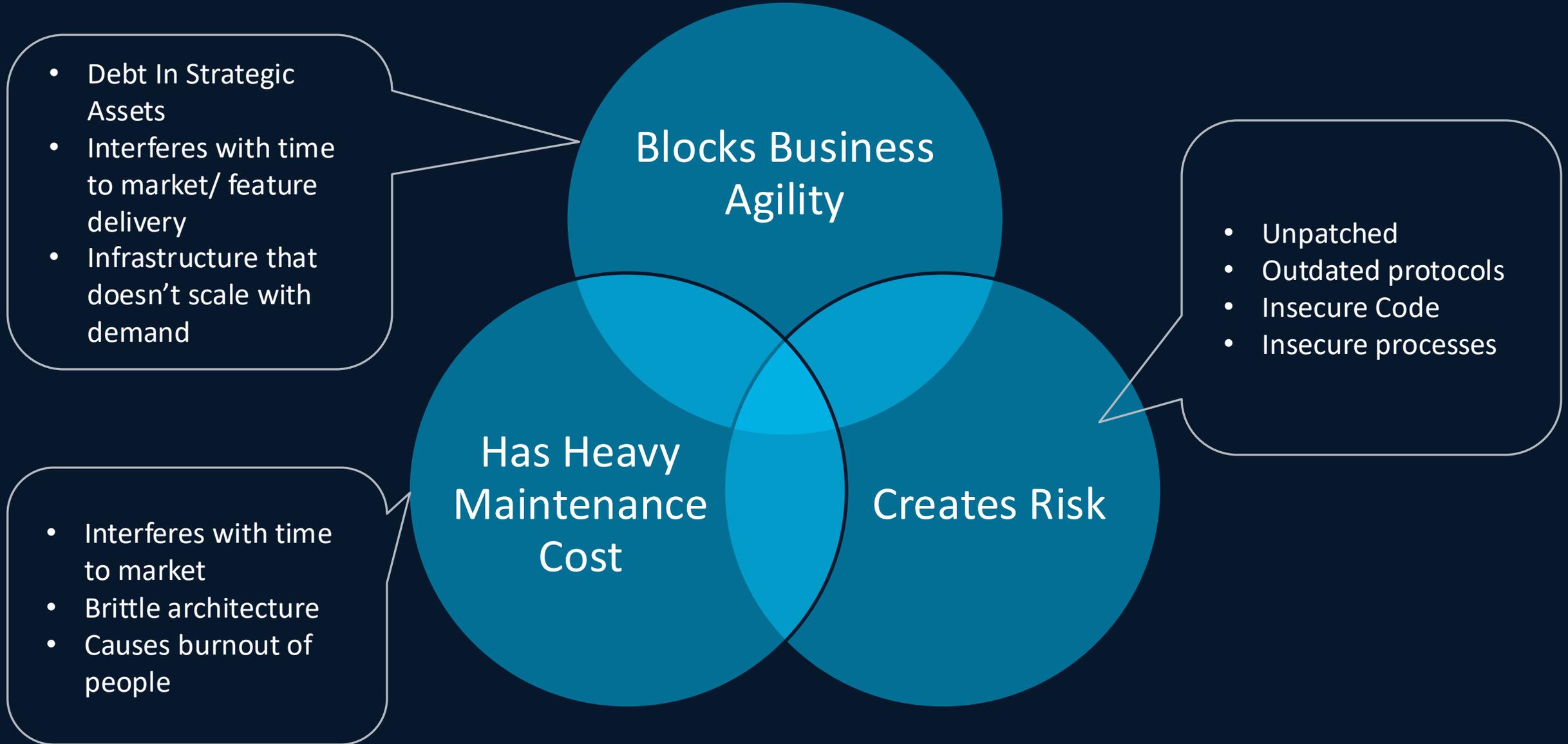
Tech Debt Elimination Strategies



Not All Tech Debt Is Equal (in Harm)

Not All Tech Debt Needs To Be Paid Off

Focus Your Program on Debt That:



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

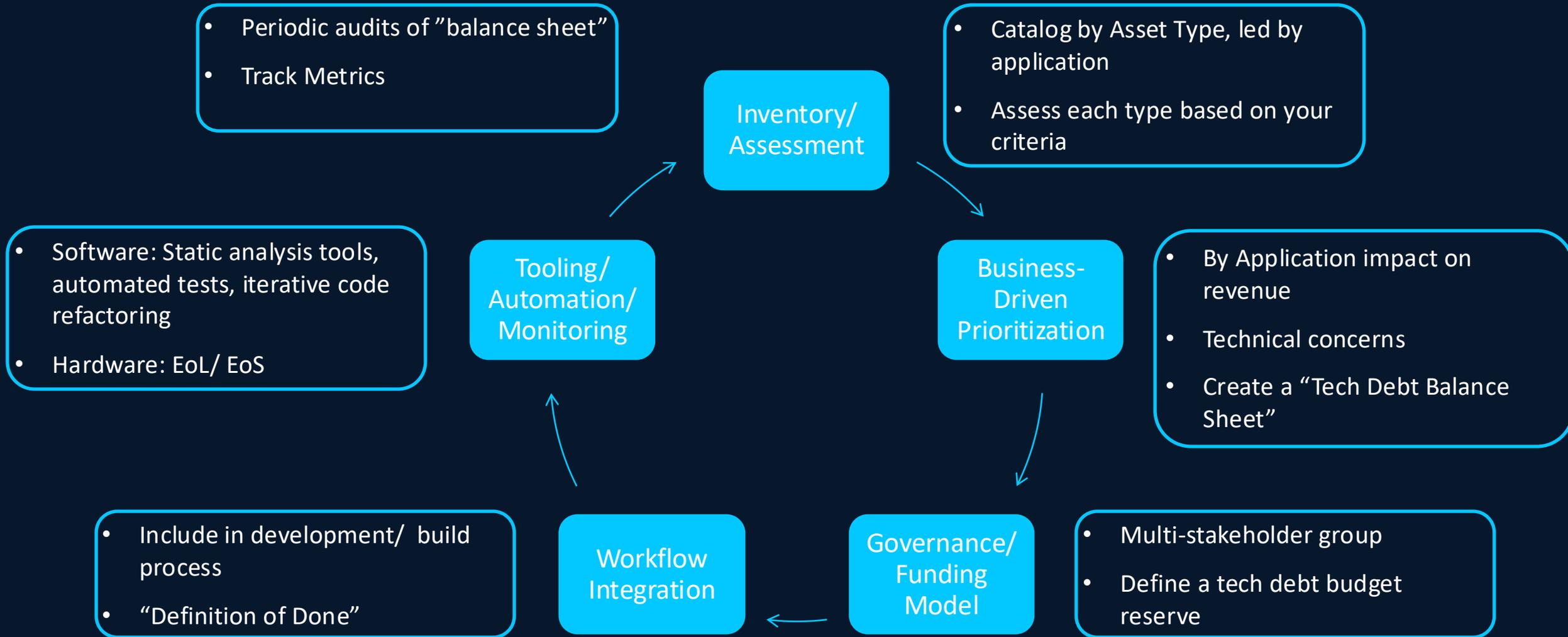
Tech Debt Balance Sheet

- 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

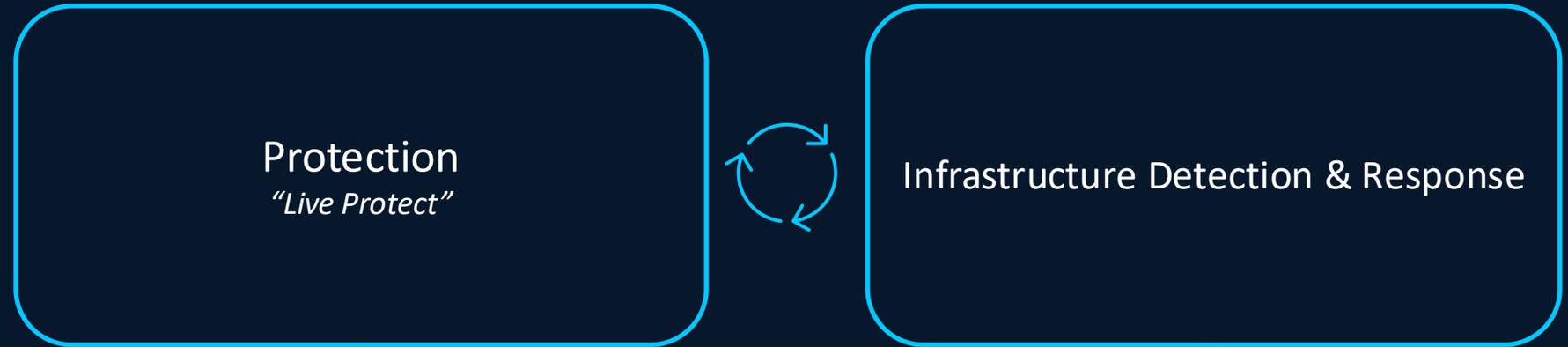


Detect & Respond

Ensure platforms provide for higher level protections and monitoring

A compelling vision of security and resilience

Enhanced Detections & Protections



Compensating Controls

Detections Enablement

Cisco Resilient Infrastructure

New Feature Enablement
(TACACS+ over TLS, Tetragon, FIDO2 over SSH, etc...)

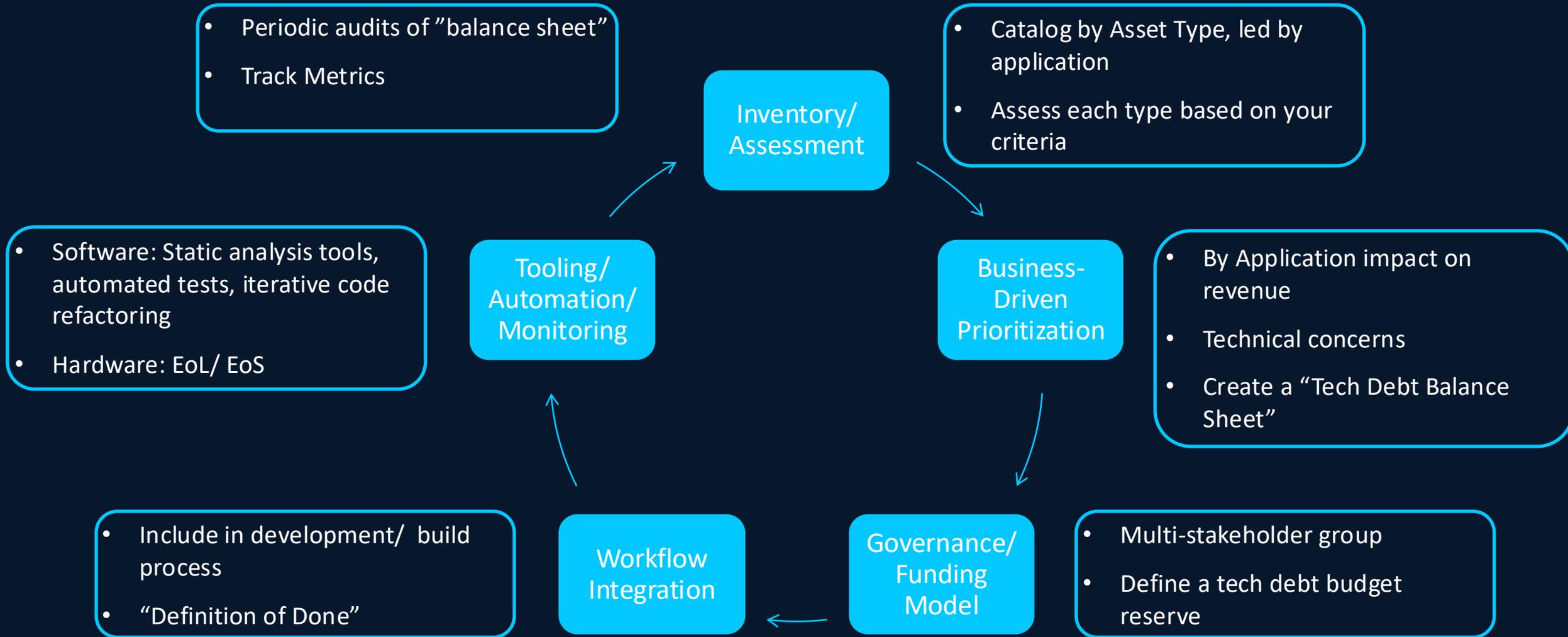
Secure by Default

Feature Deprecation / Removal

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



February GoCyber
Collective Sponsor –
Xerox IT Solutions

Jim Meincke

-ISG Lead/Solutions Architect

Roger Gregory

-Director of Security Solutions

xerox IT Solutions

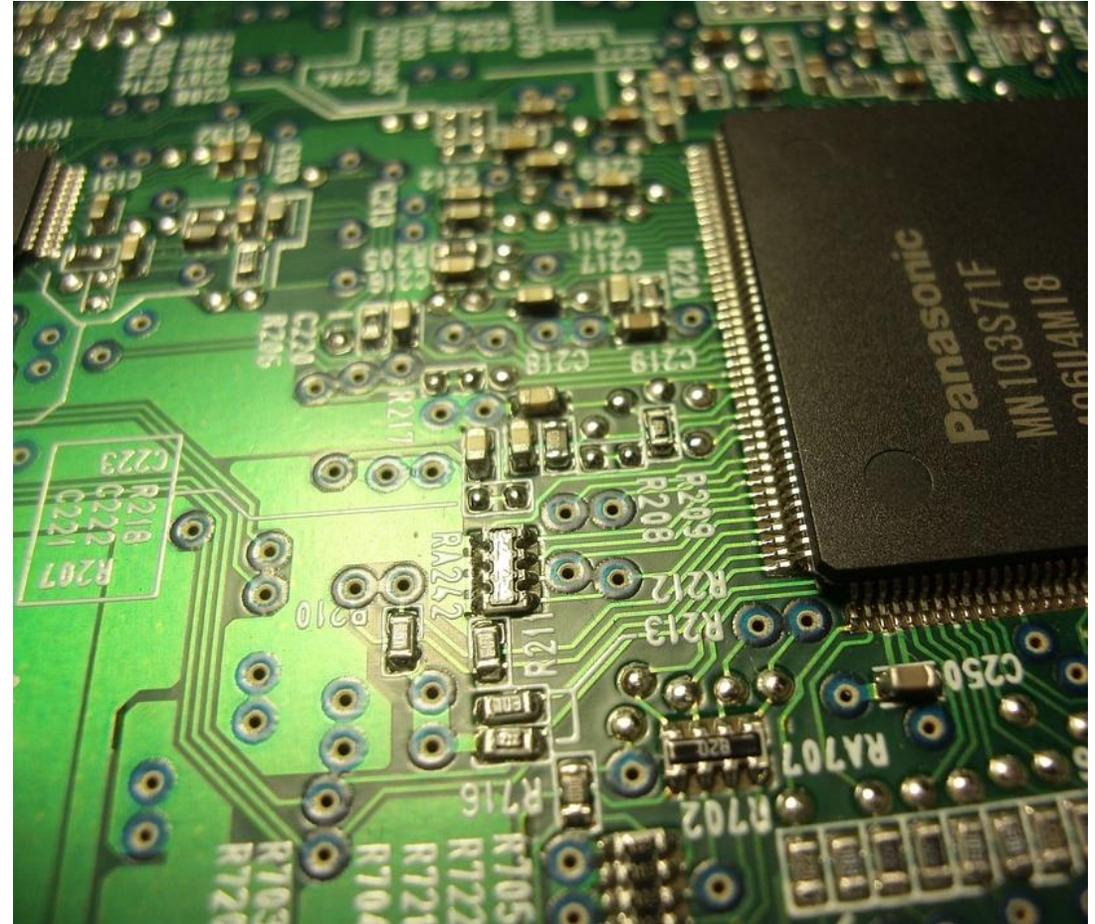


March Meeting:

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

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





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



xerox IT Solutions

Event Sponsors



SECURECYBERTM

Proven. Proactive. Personalized.

gocyber
COLLECTIVE