
go
cyber
COLLECTIVE

# May Announcements

## Protecting Our Communities

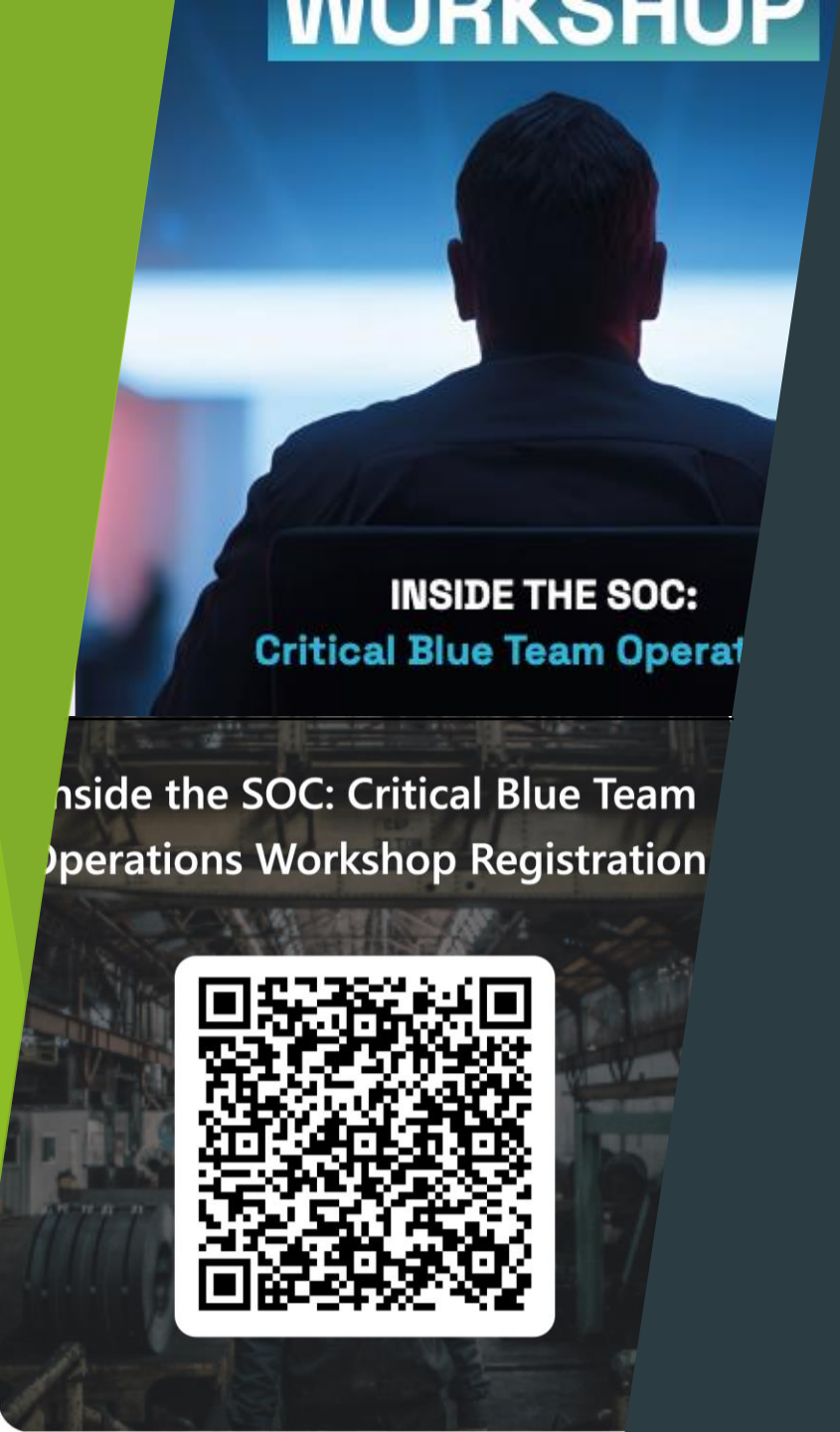

- Thank you, SecureCyber!
- New newsletter format
- TechCred expected to open July 1
- FBI: Cyberattacks up 245% since beginning of military operations in Iran
- People's Republic of China five year plan: Target healthcare
- Cyber Resilience Healthcare Conference – Oct.14th

gocyber COLLECTIVE


# Incident Response

- Tuesday/Wednesday July 28-29
- 9 AM – 3:30 PM
- This is not a document. This is not a template. This is a game plan. YOU LEAVE WITH A PLAYBOOK!
- $3,000 (Credentialed by TechCred)
- Group rates available

gocyber COLLECTIVE




# Inside the SOC: Critical Blue Team Operations

- Wednesday July 8th
- 9 AM – 3:30 PM
- Identify: How attacker gained access, moved through environment, explored systems
- $999

gocyber COLLECTIVE

Cyber for Local Government Executive Leadership - One-Day Workshop Registration

# Cyber for Local Government Executive Leadership

- Tuesday July 21st
- 8:00 AM – 4:30 PM
- Take Aways:

  -Recognize significance of cybersecurity

  -Role of leadership to maintain security

  -Understand/implement cyber hygiene

  -Importance of audits/regular training

  -Comprehensive role of insurance roles

  -Requirements under new state law
- Donuts, coffee, & lunch provided
- $499

gocyber COLLECTIVE

Digital Transformation Center

gocyber COLLECTIVE

# SPOOFING

**May 20, 2026**
**9:45 AM to Noon**

## Signal Domain Threat Role Play

Scenario 1

**Aviation**

*Flight path manipulation*

HIGH RISK

Scenario 2

**Maritime**

*Position deception*

ACTIVE

CRITICAL

**GPS**

*Position Alteration*

Scenario 3

ELEVATED

**Power Grid**

*Infrastructure Targeting*

Scenario 4

**GoCyber Collective 201 Tyler Way Moraine 45439**

# SparkSprints: Spoofing

GEOIntel exercise → Wednesday, May 20th, 2026 → 9:45 AM – 12:00 PM (right after GoCyber meeting)

FREE!!! → Great team-building exercise → Lunch provided

Register today!

gocyber COLLECTIVE

# May GoCyber Collective Keynote Speaker

Netta Squires

-Open District Solutions (ODS)

-President of Gov't Affairs, Cybersecurity, & Resilience

-Exec. Director: Center for Critical Infrastructure Security (CCIS)

OPEN DISTRICT SOLUTIONS

*Cybersecurity | Crisis Management | Resilience*

# THE RESILIENCE DELTA

*Measuring, Naming, and Closing the Resilience Delta in Critical Infrastructure*

**Netta Squires, Esq., CEM, CCRP**

Founder & President, Open District Solutions · Executive Director, CCIS

**GoCyber Collective · Dayton, Ohio · May 20, 2026**

ONE YEAR AGO TODAY

# May 20, 2025

## Kettering Health.

**14**
hospitals

**120+**
outpatient facilities

**941 GB**
stolen data

**3 weeks**
Epic / EHR down

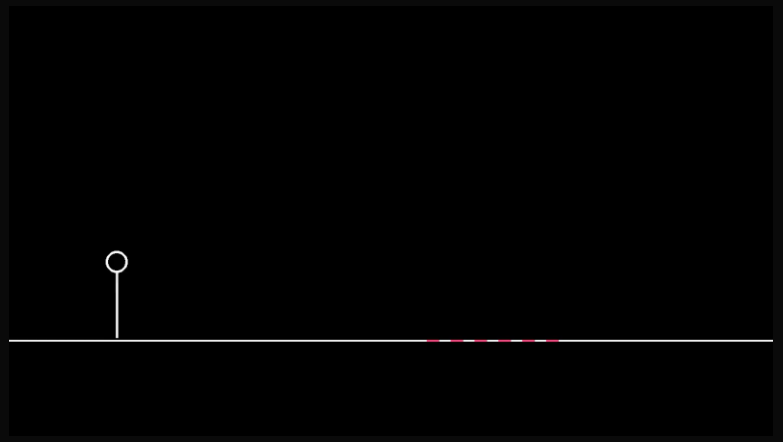
***Not merely a cyber incident. A mass care event that started with malware.***

THE FRAME

**This conversation is no longer about compliance.**

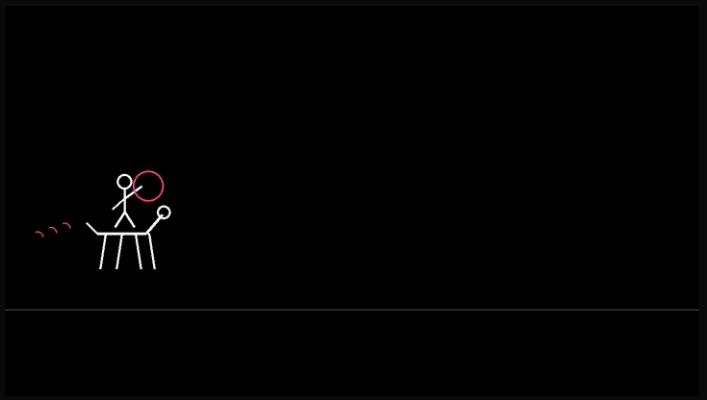
**It is about resilience, continuity, and preparedness.**

*— GoCyber Collective, May 2026*



THE STAKES

# The cavalry isn't coming.



NATION-STATE THREAT

**Volt Typhoon (PRC)**
Pre-positioning in US water, energy, transportation — not stealing, staking out.

**CyberAv3ngers (Iran/IRGC)**
Aliquippa PA water authority, Nov 2023. Six IRGC officials sanctioned by Treasury.

**DHS NTAS, June 2025**
Warning of Iranian retaliatory cyber after US strikes on Iranian nuclear sites.

FEDERAL RETRENCHMENT

**MS-ISAC**
Federal funding cut — the backbone for state and local threat sharing.

**SLCGP**
Reauthorized through 2033 — but no appropriations. Paper promise.

**CISA + Jan 2025 EO**
Narrowed posture. Cyber preparedness shifted explicitly to the states.

PART ONE

# Three cases.
# One pattern.

Suffolk County, NY

Kidd v. Springhill

SEC v. SolarWinds

CASE 1 · SUFFOLK COUNTY, NY · SEPT 2022

# Failure of leadership.

*Now a published phrase.*

> ***"In sum, the damage sustained by Suffolk County was largely attributable to a failure of leadership."***
>
> *— Suffolk County Legislature Special Cyber Intrusion Investigation Committee, Final Report (Sept. 12, 2024), at 2*

**$25M+** in remediation · **1.5M** residents · **8 months** in-network before launch

WHAT THEY KNEW — AND WHEN

# Suffolk County didn't fail to predict the future.

# They failed to act on what was already in their own files.

**2019**

After-Action Report: "There are currently no formal plans to respond to a cybersecurity incident."

**FEB 2022**

External assessment: every domain rated risk level 100. "Rare for an organization the size of the county to lack this degree of strategic cybersecurity leadership."

**JUN 21 2022**

FBI calls DoIT: ransomware actors operating in your environment. Deputy Commissioner does not escalate. "That's not our governance."

**SEP 7 2022**

5:14 PM email: "Brian. we need to deal with this asap. 3rd cortex today. with the last two being malicious." → Ransomware launches hours later.

CASE 2 · KIDD v. SPRINGHILL MEMORIAL HOSPITAL · AL, 2019

# When the planning gap costs a life.

THE COMPLAINT

*"Springhill planned, orchestrated, and implemented a scheme by hospital management and ownership in which they conspiratorially hid, suppressed, and failed to disclose critical patient safety-related information."*

THE TEXT (DISCOVERY)

***"I need u to help me understand why I was not notified. I know bad things happen and sometimes you can't control it but this was preventable."***

*— Dr. Parnell to nurse manager, post-delivery (court exhibit)*

***First US case alleging a patient death caused by a hospital ransomware attack. Settled April 2024.***

CASE 3 · SEC v. SOLARWINDS & TIMOTHY G. BROWN · S.D.N.Y. 2024

# What you say in public is the standard.

*First time a CISO faced personal liability for cybersecurity disclosures.*

> ***"Brown approved, disseminated, and promoted the Security Statement despite knowing of the ample evidence contradicting the Statement's rosy account of SolarWinds' cybersecurity practices. Thus, his dissemination and promotion of the Security Statement as an accurate depiction of SolarWinds' cybersecurity practice was reckless and an extreme departure from standards of ordinary care."***
>
> *— SEC v. SolarWinds, July 18, 2024 (Engelmayer, J.)*

***The evidence that survived dismissal was SolarWinds' own internal NIST CSF assessment.***

THREE CASES. ONE GAP.

# Same pattern. Different scale.

**SUFFOLK**

SAID: *We have cybersecurity. We have plans.*

DID: End-of-life firewalls. No CISO. Alerts ignored. "Failure of leadership."

**SPRINGHILL**

SAID: *We are caring for patients safely.*

DID: Fetal monitor on paper at bedside. Nurses' station blind. Nicko died.

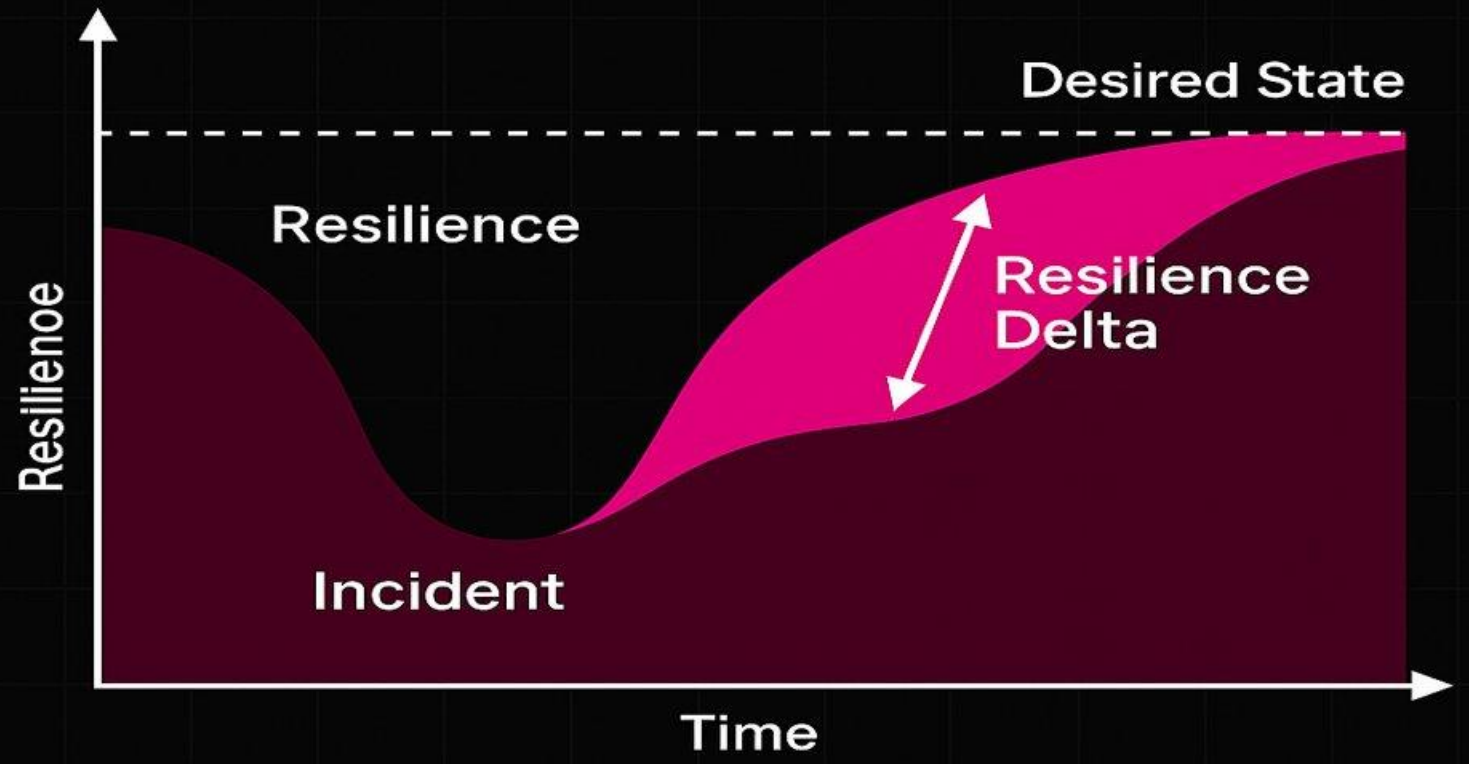
**SOLARWINDS**

SAID: *Our password practices are muscular.*

DID: Internal NIST CSF assessment said otherwise. CISO charged personally.

***The gap between what they said and what they could execute under pressure → that gap has a name.***

# RESILIENCE DELTA




**Your gap has a name.**

THE REALITY OF LEADERSHIP

# Your official role is cyber.

# Your real role entails thinking like every C in the building.

## CISO

*because the technical risk is real*

## CEO

*because the mission depends on it*

## CFO

*because resilience is an operating cost*

## CDO

*because data and trust are inseparable*

## COO

*because operations live or die by the network*

## CCO

*because public trust gets tested in hour one*

***Closing the Delta is organizational leadership through a cyber lens.***

THE DELTA IS NOT THEORETICAL

# Your sector. Your Delta.

*Here's what "can't execute under pressure" looks like across critical infrastructure.*

## HEALTHCARE

- EHR / Epic offline — diagnostic delays, manual charting
- Telemetry & fetal monitoring blind
- ER on diversion, regional load shift

## WATER & WASTEWATER

- SCADA / PLCs compromised — pressure, chemical dosing manual
- Customer billing offline — revenue halt
- Treatment continuity = public health risk

## LOCAL GOVERNMENT

- 911 / CAD down — dispatch on paper
- Court records exposed or encrypted
- Vendor payments halted — services stop

## ENERGY & UTILITIES

- OT disruption — distribution blind
- Billing / meter data offline
- SCADA monitoring = operational fog

## PUBLIC SAFETY / PSAPs

- Dispatch CAD down — radio fallback
- RMS records inaccessible
- Inter-agency comms degraded

## K-12 EDUCATION

- SIS, payroll, financial aid frozen
- Transportation routing failed
- Instructional network down

***Different sectors. Different failure modes. Same Delta to measure, name, and close.***

MEASURING THE DELTA

# Four questions.

1. At what point does an incident exceed our capacity?
2. When do we run out of people, tooling, money, attention?
3. What critical systems are still not recovered at 24 hours? 48? 72?
4. Who do we call — and how fast can we coordinate?

*These are the metrics of resilience that matter when it's not theory. When it's crisis.*

THE PIVOT

# Documentation is what makes the Delta visible.

---

***And invisible Deltas can't be closed.***

*Not paperwork. Not compliance. Not lawsuit defense. Those are byproducts.*

FOUR JOBS DOCUMENTATION DOES

# Not paperwork. Leverage.

## MEASURE *the Delta*

Technical verification. Can you actually do what your plans and assessments say? MFA, backups, patch SLAs, EOL equipment.

## NAME *the Delta*

Out loud, in writing, upward. The leadership artifact. The Suffolk Clerk's "sleepless nights" email survived because it was written down.

## SURVIVE *the Delta*

While you're still closing it. Ohio R.C. 1354 affirmative defense. The file IS the defense — burden of proof on you.

## BUILD *the architecture*

The plan itself. The alternative is what Suffolk wrote about itself: "ad-hoc and based on trusted relationships."

THE HARD TRUTH

# You don't have time for this.

## *I know.*

### The hamster wheel is the trap.

*The Delta work is the way off the wheel. Not because the tickets stop — they won't. Because it turns the chaos of "the next thing" into the structure of "the program."*

PART TWO

# Five moves to close the Delta.

*None require you to do this alone.*

MOVE 1

# Join — or start — a community.

*Trusted partners, vetted volunteers, academic partners, fractional pros. Free or low-cost. They build the plan with you.*

**GoCyber Collective**
Community you know and can trust.

**Ohio Cyber Reserve**
Ohio Homeland Security Watch Desk, 614-799-3733.

**Berkeley CLTC + New America**
National cyber clinic consortium and cyber civil defense network.

**Think Like a CISO Academy (CCIS)**
Under-resourced critical infrastructure operators, Cyber and AI Clinic (Funded by a Maryland DoL Grant).

YOU'RE HERE!

MOVE 2

# Share resources.

*You are not the only small entity trying to figure this out. The peers are in this room.*

## 1 Fractional CISO

One CISO across 3–5 small entities. Whole-of-state programs, MSPs, or nonprofit models.

## 2 Cyber mutual aid

Modeled on EMAC. Your county has mutual aid for police, fire, and EMS. Add cyber. Reach out to your OEM.

## 3 Joint purchasing

Three counties on one MDR contract. Same for insurance. Same for tabletops.

MOVE 3

# Don't start from a blank page.

*Use templates. Shareable. Adjustable.*

- Consequence Management Plan skeleton · IR + DR + COOP + PIO + ESF-5 in one document
- NIST CSF Evidence Checklist · the folder structure you build Monday morning
- First-Four-Hours Runbook · role by role, hour by hour, ready to fill contact list
- Resource Inventory & Gap Worksheet · measure your Delta on one page

MOVE 4. PREPAREDNESS

# One plan. Six annexes.

*Stop multiplying plans. Integrate them. Structure after FEMA & CISA resources.*

## 1 Technical IR

Detection, containment, eradication. The cyber response track.

## 2 Technical DR

System and data restoration. Backups, failover, integrity validation.

## 3 Crisis Comms

Internal staff, external stakeholders, regulator notification, JIC if activated.

## 4 COOP

Mission-essential functions through extended degradation. Workarounds, dependencies, manual operations.

## 5 EOP

Activation, command, and control. Or your sector equivalent — HICS, ERP, Crisis Plan.

## 6 ESF-5 / ESF-20

County EM, state, federal partners. Mutual aid. Recovery and cost capture.

MOVE 5 · THE STRATEGIC ONE

# Document maturity. Risk. And your gaps.

*Three columns on one page. The document that travels upward.*

## MATURITY

*Where are you today?*

NIST CSF tier. CIS Controls IG level. Sector-specific scoring (HICP, AWWA).

## RISK

*What does it cost?*

Top 5 scenarios with quantified impact. A bad number is better than no number.

## GAPS & ASKS

*What do you need?*

What you have. What you don't. What you asked for. What closing the gap costs.

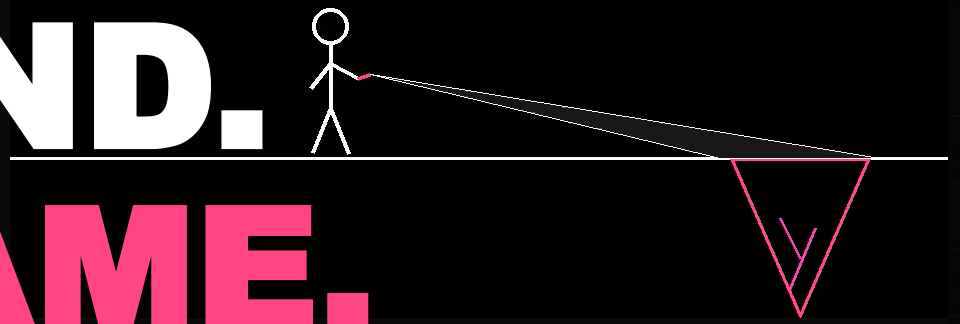
## Why it matters at FOUR levels:

**YOU** (evidence file) → **YOUR ORG** (budget justification) → **YOUR COUNTY/STATE** (rolled-up picture) → **YOUR SECTOR** (funding case)

***Build it for yourself. It becomes the document that gets funded.***

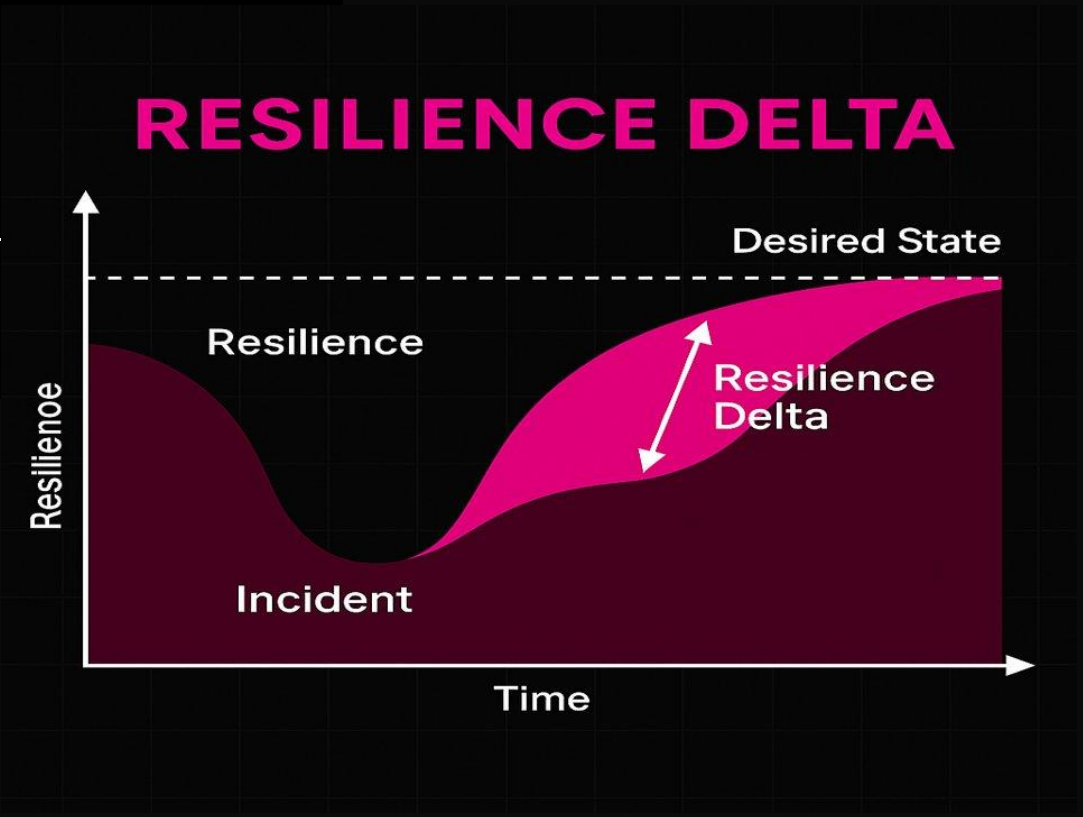
# THE RESILIENCE DELTA

FIND.



NAME.

CLOSE.



THREE-PART FRAMEWORK

# Find. Name. Close.

## FIND

*the Delta*

Measure it. The four questions: where does capacity break, when do we run out, what isn't recovered at 24/48/72 hours, who do we call. Write it down. Make it visible.

## NAME

*the Delta*

Out loud. In writing. To your council, your board, your county EM, your state cyber office, your federal partners. The CISO with a Delta map gets funded.

## CLOSE

*the Delta*

Through the work — the plan, the tabletop, the mutual aid, the vendor exercise, the clinic, the fractional CISO, the call to OhCR. Every move shrinks the gap.

***Tracked over time, your Delta closure IS your growth trail. Your advocacy story. Your case for funding.***

# Thank you.

## *Questions?*

*Find the Delta. Name the Delta. Close the Delta.*

**Netta Squires**

Open District Solutions · CCIS

*Nsquires@OpenDistrictSolutions.com*
*OpenDistrictSolutions.com*
*TheCCIS.org*

# May Threat Briefing

- Joe Tinney
  - -SecureCyber
  - -VP of Cyber Ops

SECURECYBER™

Proven. Proactive. Personalized.

# Threat Trends

What to fix first when everything looks urgent

The pattern is not just more CVEs. It is faster exploitation of the same weak spots: exposed management planes, software supply chain control points, and old security debt.

# Three themes tie the month together

The same failure patterns keep showing up across very different products.

1

## Management planes are the front door

Cisco SD-WAN, Ivanti EPMM, Quest KACE, cPanel/WHM, SonicWall and similar systems concentrate privilege and sit close to the internet.

2

## Build systems are production systems

GitHub Enterprise, TeamCity and AI-enabled CI tooling can expose source, secrets, signing keys and deployment paths.

3

## Old bugs still pay rent

Nine-year-old PHPUnit exploitation, abandoned plugins, dev dependencies in prod and stale credentials remain routine attack paths.

**Practical takeaway: prioritize by exploitability and blast radius, not just CVSS.**

# Where the heat is: exposed control points

These are not just vulnerable apps; they are places where control, trust, and credentials converge.

| Control point | Examples this period | Why defenders should care |
| --- | --- | --- |
| **Internet edge / hosting** | NGINX 9.2, cPanel/WHM 9.8, SonicWall SMA scanning | Remote exposure; rapid exploitation; high external attack surface |
| **Network management** | Cisco SD-WAN 10.0, Catalyst SD-WAN Manager, Ivanti EPMM, Quest KACE | Authentication bypass, admin access, recoverable credentials |
| **Build and dev platforms** | GitHub Enterprise Server RCE, TeamCity traversal, Gemini CLI RCE | Source, secrets, signing keys, deployment tokens |
| **Collaboration / data apps** | PaperCut, Zimbra, Kentico Xperience | Initial access, credential theft, lateral movement |

**Action filter: inventory exposed admin surfaces - patch KEV/actively exploited first - segment access paths.**

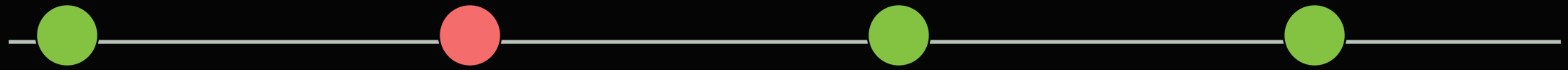
# Exploit windows are collapsing

The operational problem: defenders are not racing disclosure; they are racing automation.

**The old model: wait, test, patch on the normal cycle.**

**The current model: pre-stage emergency change paths before the CVE drops.**

- Asset owner on call
- Known rollback plan
- Firewall / WAF containment option
- Detection query ready



**Disclosure**

Public signal

**13 hours**

LMDeploy exploited

**Days**

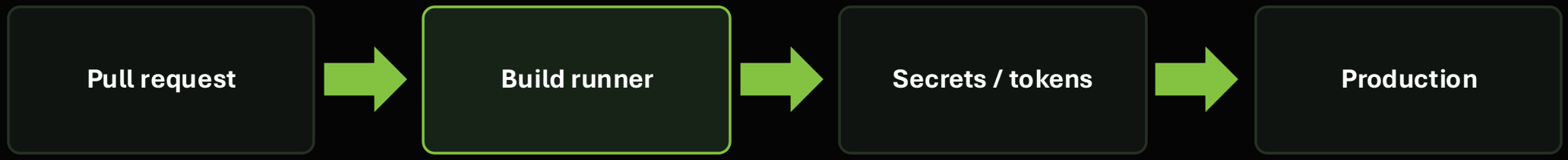
KEV / mass scanning

**Weeks**

Credential reuse and persistence

# Software supply chain is a privilege boundary

CI/CD, source control, and AI tooling now sit in the path between code and production.




**Recent examples:**

- GitHub Enterprise Server RCE through git push injection can lead to code, artifacts, signing keys and stored secrets.
- TeamCity path traversal has been used to reach sensitive configuration and credentials.
- Gemini CLI RCE shows AI tooling can be abused through malicious pull requests into CI/CD.

## Defensive moves

Treat build runners like production. Remove standing credentials. Rotate tokens after compromise windows. Constrain AI tools by repo and command, not by trust in the workspace.

# Security regressions attackers still monetize

The uncomfortable part: many of the wins are not novel. They are neglected basics at scale.

| | |
|---|---|
| **Ancient CVEs** | CVE-2017-9841 saw 80,000+ attempts in 30 days; botnets still carry it in playbooks. |
| **Abandoned plugins** | Closed or unmaintained WordPress payment/event plugins remain exposed. |
| **Dev dependencies in prod** | Vendor directories and eval-stdin.php remain web-accessible when --no-dev is skipped. |
| **Credential hygiene** | Credential rotation materially reduced Ivanti EPMM risk; stale admin creds turn auth-only into practical compromise. |
| **Patching without eradication** | Persistence can survive patching, as seen with FIRESTARTER-style malware after known guidance. |

**Practical read: cleaning up old exposure often removes more attack surface than chasing every new headline.**

# What to do this week

A short action list for reducing real-world exploitation risk.

SECURECYBER

## 1 Inventory exposed control planes

VPN, SD-WAN, MDM, KACE, Git, CI, cPanel, printers and admin portals.

## 2 Patch by active exploitation

KEV and confirmed exploitation first; CVSS second.

## 3 Rotate privileged credentials

Especially where vendors tied risk reduction to credential rotation.

## 4 Separate build from prod

Restrict runner network paths, secrets access and deploy permissions.

## 5 Remove dead weight

Abandoned plugins, dev dependencies, old web-exposed vendor directories.

## 6 Watch for persistence

After patching, hunt for new users, web shells, tasks, tokens and odd outbound traffic.

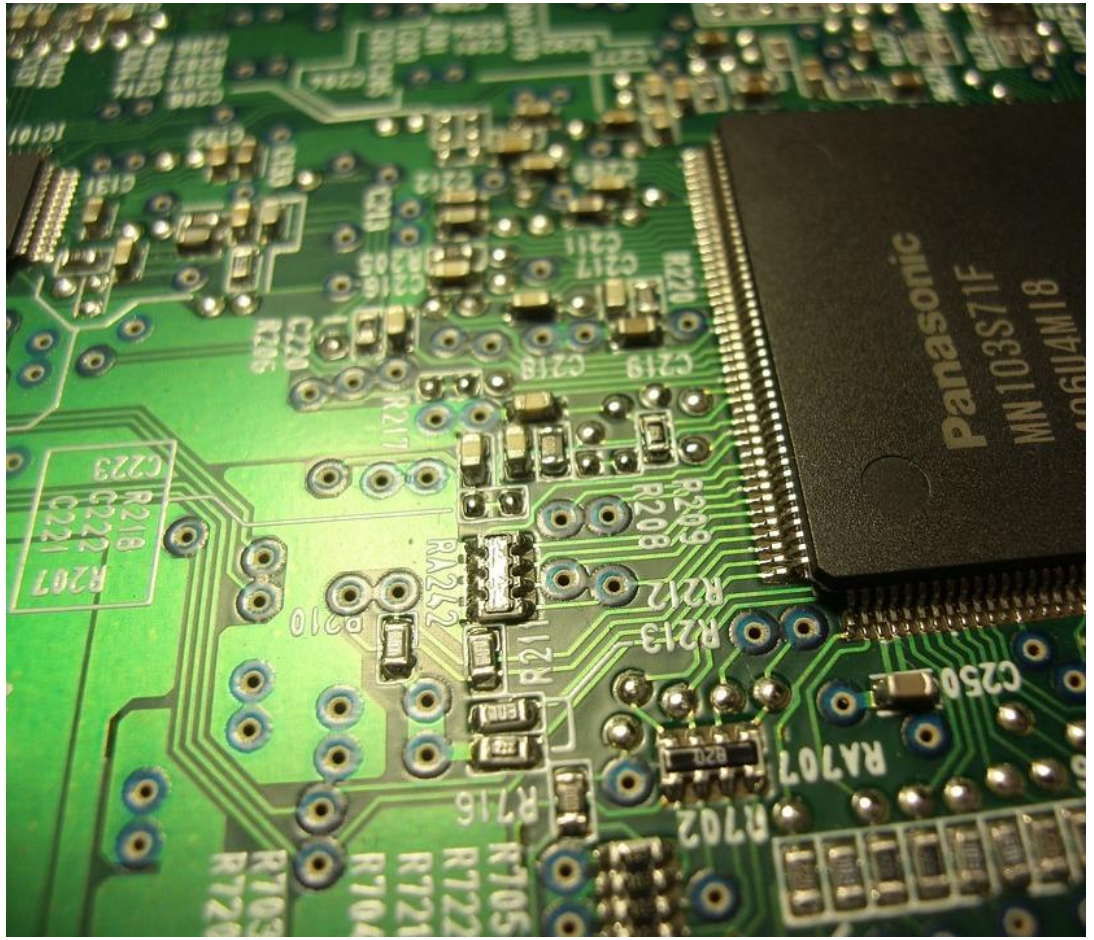
**When in doubt: reduce exposed admin surfaces, then reduce credential blast radius.**

# June Meeting:

- Connie Matthews Reynolds: ReynCon Security
- Founder & CEO: ReynCon Educational Services & Training
- Founding member: EmpoWE-R Women of InfoSec
- Success not determined by luck and circumstance

# May 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




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