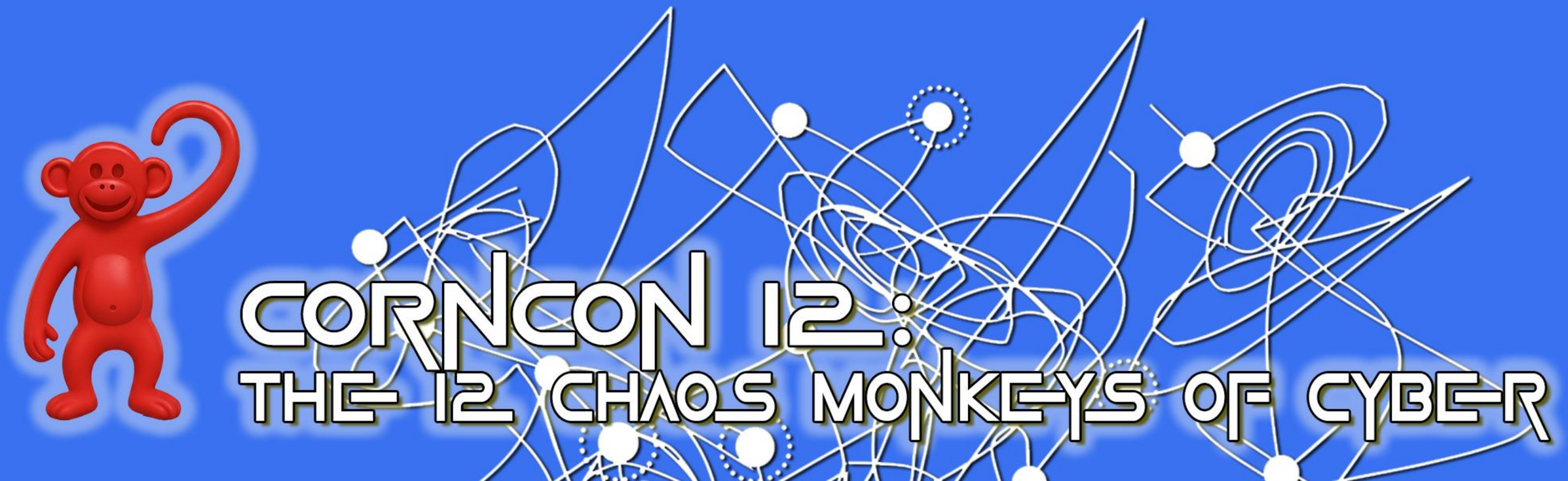
FIRESIDE CHAT

Threat Actors Love Your Security Stack

Chris (CJ) Johnson • Zach Kromkowski



YOUR SPEAKERS

Chris and Zach



Chris (CJ) Johnson

DIRECTOR OF CYBERSECURITY PROGRAMS & EXECUTIVE DIRECTOR OF GTIA ISAO

GTIA

Global Technology Industry Association



Zach Kromkowski

CHIEF RESOURCE OFFICER

SENTEON

2026 CORNCON CYBERSECURITY CONFERENCE

CENTRAL MESSAGE

Attackers do not need organizations to lack security tools



Misconfigured



Ungoverned



Disconnected



Unverified



Possession is not maturity.



Activity is not effectiveness.



You cannot out-secure your operational maturity.



Every tool creates another opportunity for

ASSUMPTIONS

GAPS

EXCEPTIONS

DRIFT

Staying secure in an increasingly complex and chaotic world

THE UNCOMFORTABLE TRUTH

Four Views of the Same Stack

ORGANIZATIONS

Buy the tools

EXECUTIVES

Assume it’s handled

SECURITY TEAMS

Assume activity is progress

ATTACKERS

Look between the tools

2026 CORNCON CYBERSECURITY CONFERENCE



CHRIS TO ZACH

Where does a strong stack still leave the biggest exposure?

Staying secure in an increasingly complex and chaotic world



01

More Tools, Not More Security

Staying secure in an increasingly complex and chaotic world

ZACH · TECHNICAL PERSPECTIVE

Where Exposure Persists

01
Permissive defaults

02
Drift after deployment

03
Inconsistent baselines

04
Permanent exceptions

05
Alerts without correction

06
Hardened once, never validated

The Governance Questions

- Who approved the baseline?
- Who owns the exception?
- How long can it stay open?
- Who weighs disruption against risk?
- How does leadership know it works?
- Who owns the decision?



“A technical gap becomes a business risk when nobody owns the decision around it.”



02

The Gaps Between the Tools

Staying secure in an increasingly complex and chaotic world

THE GAPS BETWEEN THE TOOLS

Three Gaps

1

Assumed coverage

The tool is owned. Its coverage can’t be shown.

2

Fragmented ownership

Every team has a dashboard. Nobody owns the risk.

3

Operational friction

The control is present. Pressure gets it bypassed.

2026 CORNCON CYBERSECURITY CONFERENCE



FIRESIDE EXCHANGE

CHRIS TO ZACH

Disrupt the business, or disable the control?

ZACH TO CHRIS

Who makes the business-risk call?

Staying secure in an increasingly complex and chaotic world



Governance is not documentation.

It is a decision system that works under pressure.

2026 CORNCON CYBERSECURITY CONFERENCE

$$\frac{(L+S+C)}{\square} = CME$$

Governance is not documentation. “It’s a decision system that operates under pressure.”



03

What Mature Organizations Do Differently

Staying secure in an increasingly complex and chaotic world

WHAT MATURE ORGANIZATIONS DO

People, Process, Technology

PEOPLE

Named control owners

Clear escalation paths

Business leaders in risk decisions

PROCESS

Approved baselines

Reviewed exceptions

Tested outside audit season

TECHNOLOGY

Configured to risk outcomes

Drift monitored

Evidence feeds governance



Maturity is not how many controls you have.

It is how consistently you make, implement, verify, and improve security decisions.



04

A Practical Roadmap

Staying secure in an increasingly complex and chaotic world

A PRACTICAL ROADMAP

Four Steps

1

GOVERN

Assign an owner and decision rights

2

HARDEN

Apply a defensible baseline consistently

3

VERIFY

Confirm scope and monitor drift

4

IMPROVE

Fix process before buying tools



Pick one control. Can you name its:

- OWNER
- BASELINE
- EXCEPTIONS
- LAST VERIFIED

Staying secure in an increasingly complex and chaotic world

BEFORE BUYING ANOTHER SECURITY TOOL

Five Questions

01 **What risk can’t we manage today?**

02 **Is the gap technology, or ownership and process?**

03 **Who will operate and improve it?**

04 **How will we know it still works in six months?**

05 **What does it replace?**



“The next tool may expand the stack without improving security.”

KEY AUDIENCE TAKEAWAYS

Takeaways

- Tool ownership is not control effectiveness
- Configuration drift is a governance problem
- People, process, and technology reinforce one another
- Measure repeatability, not activity
- Find the real gap before buying
- Every control needs an owner, baseline, exception process, and evidence
- Make the existing stack effective



ZACH

Hardening is not a one-time project.

CHRIS

Maturity comes from good decisions made repeatedly, especially inconvenient ones.

Replace assumptions with

OWNERSHIP

REPEATABILITY

EVIDENCE



CORNCON 12:
THE 12 CHAOS MONKEYS OF CYBER



Questions?



Chris (CJ) Johnson
email@gtia.org
linkedin.com/in/…



Zach Kromkowski
email@senteon.co
linkedin.com/in/…

Staying secure in an increasingly complex and chaotic world