How NOT to Be Your Adversary's Best Friend

Doing what matters... — FIRST CTI 2026, Munich

FIRSTCTI MUNICH

BRIAN HEIN

JAMES SHANK

We Have a Focus Problem

"Actionable" became the entire personality of threat intelligence.

And it's killing us.

Raise Your Hand

> "What did we actually get for this CTI investment?"

If your honest answer was a fancy dashboard and a shrug — you're not alone. That's the whole industry.

Today's Roadmap

1

The Action Trap

Motion confused for progress

2

What Impact Looks Like

Outcomes that matter

3

Community as a Weapon

The 1000× force multiplier

SECTION 2

The Action Trap

Confusing motion for progress

You Built a Factory

- IOCs Ingested
- Feeds Consumed
- Reports Produced
- Tickets Closed

You're measuring how fast the conveyor belt moves. Not whether anything useful comes off the end.

The Question Nobody Wants to Answer

> "If your entire CTI program vanished overnight — would the adversary even notice?"

If the answer is no — or you're not sure — we have a problem.

The False Success of "Actioned" Intelligence

50,000 IOCs Processed

SOC team celebrates. Management applauds.

Same Org Gets Breached

Attack was *in* those IOCs. Actioned. Just not in any way that mattered.

The Adversary

Was not impressed.

Intelligence Theater

> "Action for action's sake is intelligence theatre. We're performing security instead of producing it."

The adversary is in the audience. Laughing.

What Impact Actually Looks Like

Outcomes the business will value. Outcomes the adversary can't survive.

The Reframe That Changes Everything

❌ Old Question

"Is this intel actionable?"

✅ New Question

"So what? What happens if we act? What happens if we *don't*?"

CTI that influences **decisions** is worth 100× CTI that populates dashboards.

CTI That Moves Business

Ransomware Tactics Intel

Doesn't just fire a YARA rule — it justifies a $2M investment in immutable backups and shifts the board's risk appetite.

Threat Landscape Analysis

Doesn't just fill a quarterly report — it kills a bad M&A deal, changes a vendor relationship, reprices cyber insurance.

The Uncomfortable Truth

If your CTI team can't get a meeting with the CFO — you're doing data entry with a security clearance.

Metrics That Make Executives Lean Forward

$4.2M	18mo	0
Fraud Loss Prevented	Adversary Dev Time Torched	Reports Nobody Asked For
Real dollar impact, not feed counts	Infrastructure seizures that hurt	Stop counting. Start mattering.

Not feed counts. Not report counts.

Money. Decisions. Risk reduced in terms the business already tracks.

Attackers Run Businesses

They have costs, timelines, infrastructure investments, and expected returns. A P&L — even if it's on a Telegram channel.

Your job isn't just to defend. Your job is to **wreck their economics.**

Wreck Their Economics

1

Rapid Sharing Burns Their Tools

Hours instead of months. Their R&D costs skyrocket.

2

Sector-Wide Defense

Every target is expensive, not just the hard ones. Revenue-per-attack craters.

3

Proactive Disruption

Takedowns don't stop one campaign — they torch years of infrastructure investment.

The FBI Gets It

> "Impose greater cost and risk to cyber criminals."

That's not a tagline. That's the only strategy that scales.

The metric that should be on every CTI team's wall: **"How much more expensive did we make it to be our adversary today?"**

Before vs. After

What Teams Say Now

"We processed 10,000 IOCs and produced 47 reports this quarter."

Cool. So did the team that got breached last month.

What They Should Say

"Our intelligence prevented $4.2M in fraud, caused Threat Group X to abandon a campaign mid-operation, and contributed to seizures costing the adversary 18 months of development."

The best programs already talk like this. The rest of us are still counting IOCs like frequent flyer miles.

SECTION 4

Community as a Weapon

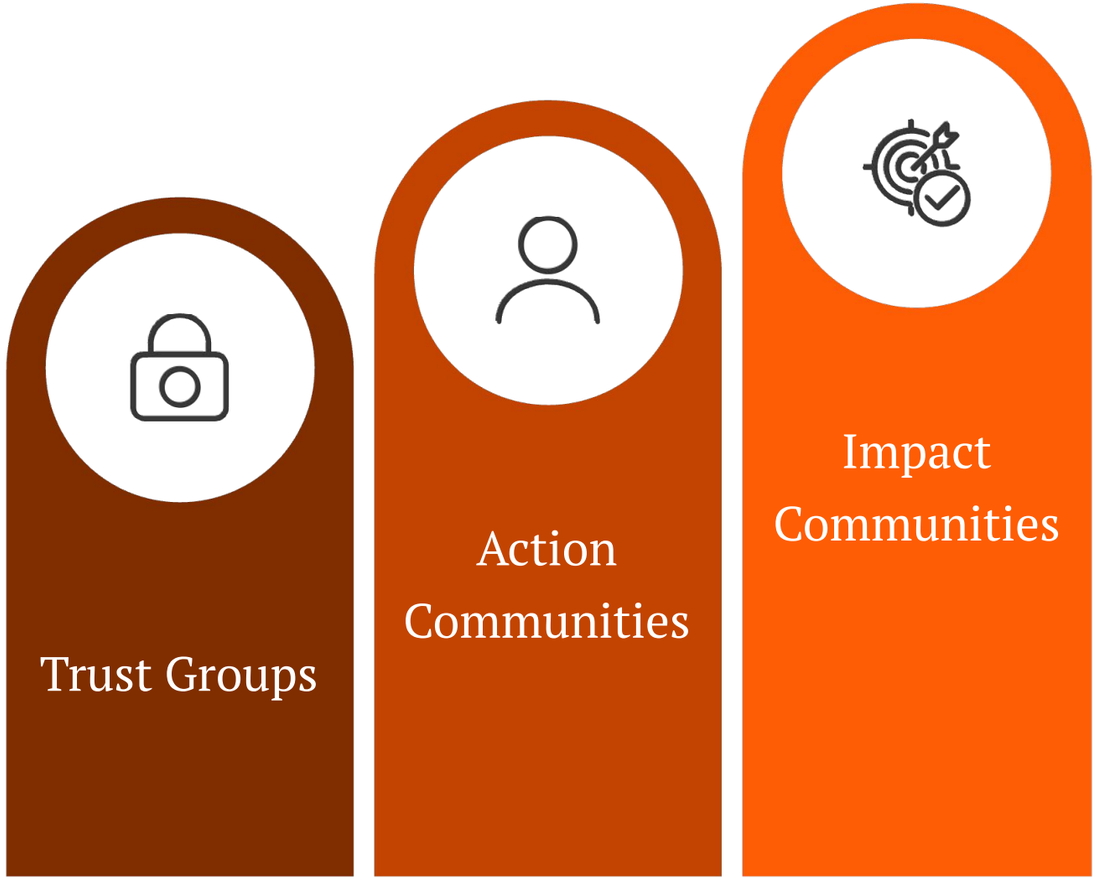
Alone, you defend. Together, you impose cost at scale.

TLP is a Weapon — Aimed at Whom?

1	TLP:CLEAR	Your enemy's enemy — share widely, impose cost broadly
2	TLP:GREEN	Your enemy's distant enemy — limited but still useful
3	TLP:AMBER	Your enemy's friend — sharing is restricted, impact shrinks
4	TLP:AMBER+STRICT	Your enemy's close friend — nearly useless for collective defense
5	TLP:RED	Your **enemy's best friend** — hoarded intel protects no one

Over-classification is an adversary shield. The more you hoard, the less you fight.

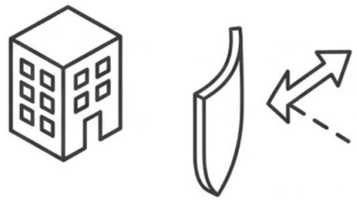
The Evolution of Collaboration



The adversary can survive one of you. They can't survive all of US at once.

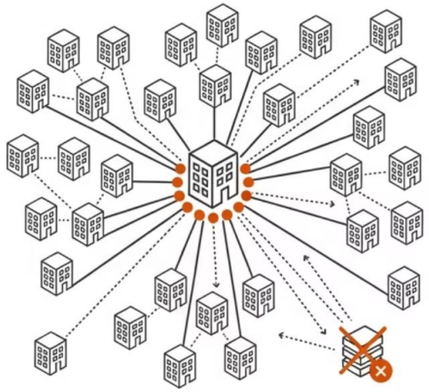
The 1000× Force Multiplier

Solo Defender



Solo Organization

Coordinated Community



The Math is Brutal

One org blocking an attack saves one target.

A community sharing indicators burns the attacker's infrastructure across thousands of targets simultaneously.

Adversary spends a dollar. Gets nothing but pain across an entire sector.

Rapid Response

> No bylaws. No NDAs. No attribution debates. Just: "Here's what we know. Here's what works. Go."

When Community Goes Nuclear

Fast Sharing

Intelligence snowballs across organizations

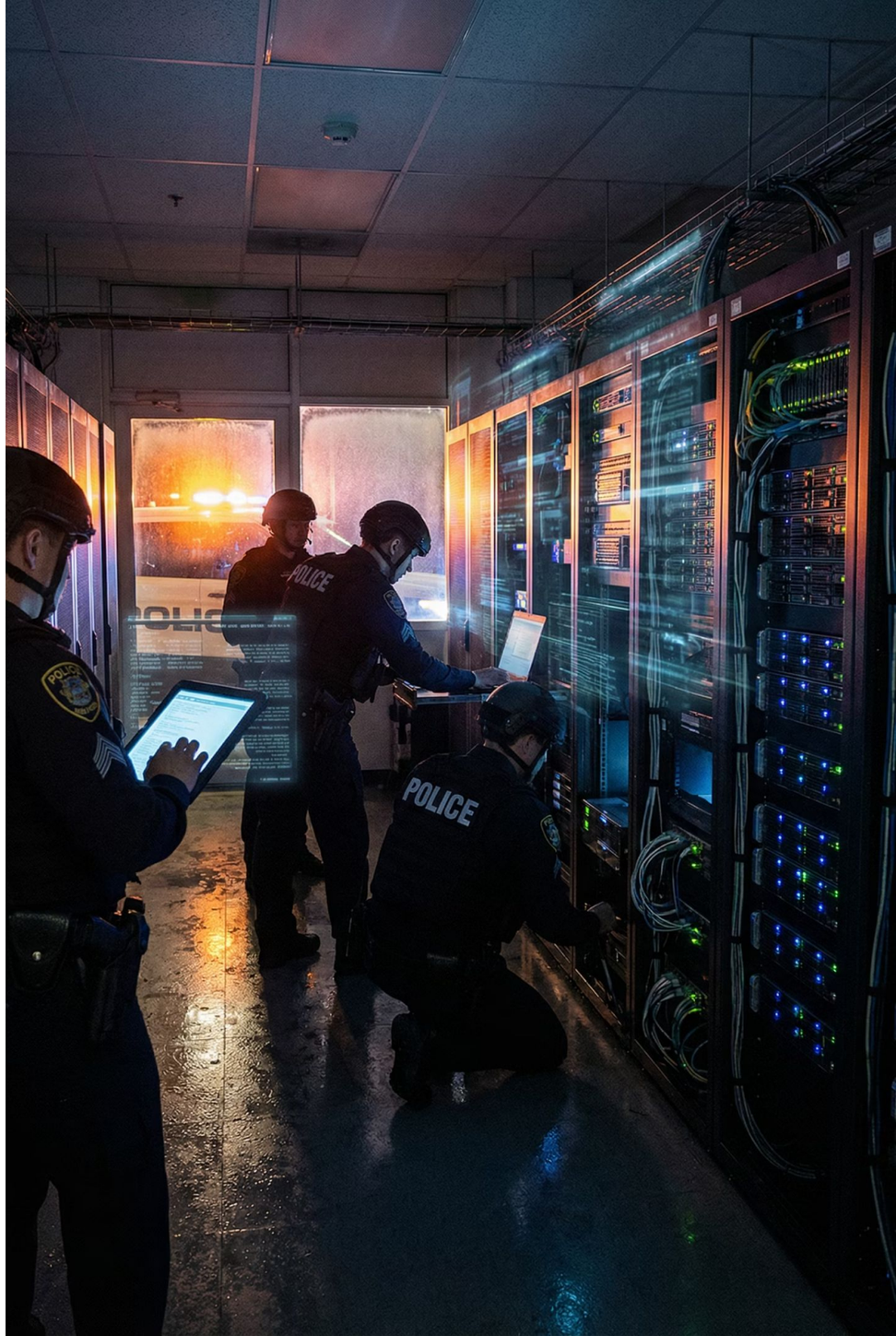
Do all the things!

Private sector + law enforcement act independent

Infrastructure Disabled

Globally. Permanently.

Operation destroyed. Years of investment incinerated. Forced to rebuild from zero. **That's not "actioning" intelligence. That's weaponizing it.**



No Single Hero

> "No single organization, no single government, no single vendor did this. The community did this.
>
> And the adversary felt it in their wallet."

The Gauntlet

Three things. No fluff.

Three Things. Starting Now.

Kill Your Vanity Metrics

Replace "reports produced" with something that makes your CFO or your adversary flinch.

Become Their Cost Center

Stop defending. Start making their business model fail.

Build Your Network Today

All practitioners. One group chat.

One rule: share fast, act together.

That's a force multiplier.

The Parting Shot

> "Actionable intelligence is table stakes. Every vendor on the expo floor will sell you 'actionable.' What they can't sell you is *impact* — because impact requires you to actually care about outcomes, not outputs."

Let's Fix That

When defenders wreck adversary economics, protect what the business *actually* values, and fight as a community — adversaries don't just notice.

Revenue per attack craters.

> "Turn your intelligence into outcomes adversaries can't afford to ignore. Because right now? Most of them can afford to ignore us."