# WELCOME TO THE 11TH ANNUAL HACKING CONFERENCE

The Institute of Internal Auditors Chicago

ISACA Chicago Chapter

# WELCOME TO THE 11TH ANNUAL HACKING CONFERENCE

Check-In Code: balance

The Institute of Internal Auditors Chicago

ISACA Chicago Chapter

# Making Threat Intelligence Operational

Jason Torres, Associate Director, Security Threat Incident Management, MSKCC

# The Four Stances of Operational Intelligence

*Each pillar moves you from reactive monitoring to operational defense.*

01

## Defining

*Operational Intelligence*

Move from “knowing” to “doing.” Establish a Cyber Threat Profile that focuses defense on what actually threatens you.

02

## Prioritizing

*Data Sources*

Curate over collect. Align feeds and intel sources to your business-critical assets, not vendor catalogs.

03

## Integrating

*the Tool Stack*

Embed intelligence into SIEM, SOAR, EDR, and identity systems so response is automatic — not aspirational.

04

## Measuring

*Effectiveness*

Prove the program. MTTD, MTTR, dwell time, false-positive reduction, and breach-cost avoidance — not tool dashboards.

# Polling Questions (to set the Stage)

**Do you have a Threat Intelligence Program in your organization?**

A. Yes
B. No

**Do you In-Source or Out-Source your Threat Intelligence Program?**

A. So In
B. Very Out


**Which of the following best describes your organization's approach to selecting threat intelligence data sources?**

A. Strategic
B. Vendor-Driven
C. What AI Told Me

**To what extent is your threat intelligence integrated with your security tools (SIEM, EDR, firewalls, etc.)?**

A. Full Integration
B. Partial
C. What Integration?

# Defining Operational Intelligence



> *"First Learn Stand, Then Learn Fly" – Mr. Miyagi (The Karate Kid)*

THREAT INTELLIGENCE

## Knowing

**Awareness that something might threaten us. Reports, feeds, indicators, signals — valuable, but inert without action.**

OPERATIONAL INTELLIGENCE

## Doing

**Intelligence that drives immediate defense — wired into SIEM, SOAR, EDR, identity, and IR playbooks. The fight, not the briefing.**

**CYBER THREAT PROFILE** = the guardrails + the compass -> which fights are yours — which to ignore.

> *"Inner peace. Focus. Balance. These are just some of the skills that you will master when you join Miyagi-do Karate." — Daniel LaRusso, Season 2 Episode 3*

# Where the Industry Stands on Operational TI

*Threat intelligence is no longer a luxury — it's standard practice. The maturity gap, however, is real.*

**83%**

Of organizations now run full-time threat intelligence teams; 89% pay at least one TI vendor.

*Recorded Future 2025 State of TI*

**49%**

Rate their TI maturity as advanced — but 87% expect significant progress in the next 2 years.

*Recorded Future 2025 State of TI*

**65%**

Say TI directly drives security technology purchasing; 58% say it guides business-initiative risk assessment.

*Recorded Future 2025 State of TI*

**86%**

Express high trust in AI-generated TI outputs; most expect GenAI to cut analyst workloads >25%.

*Recorded Future 2025 State of AI in TI*

**91%**

Plan to invest more in threat intelligence in 2026; 81% plan to consolidate TI vendors.

*Recorded Future 2025 State of TI*

**1 in 6**

Breaches now involves attackers using AI — most often for phishing (37%) and deepfake impersonation (35%).

*IBM Cost of a Data Breach 2025*

***"No one can take honor from you. Only you can take honor from yourself." — Chozen to Tory, Season 5 Episode 2***

*Sources: Recorded Future 2025 State of Threat Intelligence Report; Recorded Future 2025 State of AI and Automation in Threat Intelligence; IBM Cost of a Data Breach 2025.*

# Choosing Your Data Sources: 3 Truths

*The questions every TI program must answer — and what 2025 data tells us about the right answers.*

## 1 Match data to YOUR threat profile, not vendor catalogs

Half of TI teams cite difficulty determining accuracy and credibility of reports (50%); 46% say feeds lack context tailored to their environment. The default response is to add more vendors. The right one is to start from your Cyber Threat Profile and let it tell you what to subscribe to — and what to cut.

*Recorded Future 2025 State of Threat Intelligence Report*

## 2 Curation beats collection — every time

81% of organizations are consolidating threat intelligence vendors in 2025. Multi-source correlation now replaces hours of manual work per incident. The shift: fewer feeds, better enrichment, automated normalization. Vendor count is no longer a maturity signal — signal-to-noise is.

*Recorded Future 2025 State of Threat Intelligence Report*

## 3 Enrichment must include context, not just IOCs

48% cite poor integration with existing tools as a major blocker; 46% cite information overload. An IOC without business-asset context, MITRE mapping, and confidence scoring is just another row in a SIEM. Operational intel is the IOC plus the so-what — wired into the playbook that acts on it.

*Recorded Future 2025 State of Threat Intelligence Report; Verizon 2025 DBIR*

***"Put good out into the world and good will come back to you." — Kumiko quoting Yukie, Season 3 Episode 5***

# Prioritizing Intelligence Data Sources

> *"Never Put Passion Before Principle. Even if Win, You Lose"– Mr. Miyagi (The Karate Kid II)*

**THE PRACTICE**

Evaluate, select, and prioritize threat feeds and intelligence sources that align with your organization's risk profile, business-critical assets, and operational security requirements — rather than consuming every available data source. Quality of fit beats volume of feeds, every time.

**ALIGN**

Map every feed to a Cyber Threat Profile concern — if it doesn't tie to a business risk, it's noise.

**ENRICH**

Context is non-negotiable: MITRE TTP, asset criticality, confidence score, expiration.

**RETIRE**

Audit feeds quarterly. Drop sources that don't fire on actual investigations.

> *"Winning one championship don't mean squat! A true champion never stops training. You gotta keep moving forward, or else you can get stuck exactly where you are." — Johnny Lawrence, Season 2 Episode 2*

# Reshaping Threat Source Priorities



*Six numbers that should reshape what you collect — and what you stop collecting.*

**95%**

Of breaches are financially motivated — ~19% are espionage. Tune feeds to crimeware ecosystems first.

*Verizon 2025 DBIR*

**44%**

Of breaches involved ransomware — up from 32%. Ransomware ecosystems must be a first-class TI target.

*Verizon 2025 DBIR*

**30%**

Of breaches now involve a third party — doubled from 15% YoY. Vendor and supply-chain TI is mandatory.

*Verizon 2025 DBIR*

**33%**

Mandiant's #1 initial access vector for the 5th consecutive year: vulnerability exploitation. Pair vuln intel with scan data.

*Mandiant M-Trends 2025*

**8x**

Year-over-year jump in breaches via edge devices (firewalls, VPN concentrators, RAS gateways) — 22% of all vuln-exploit breaches.

*Verizon 2025 DBIR*

**9.3%**

Healthcare's share of Mandiant IR investigations — 5th most-targeted industry. Sector-specific feeds matter.

*Mandiant M-Trends 2025*

***"Karate is about discipline. It's about inner strength. It's about confidence. Lessons you can use for the rest of your life." — Miguel Diaz, Season 3 Episode 8***

*Sources: Verizon 2025 DBIR (22,052 incidents / 12,195 breaches); Mandiant M-Trends 2025; CrowdStrike 2025 Global Threat Report; IBM X-Force Threat Intelligence Index 2025.*

# Operationalizing Your Stack: 3 Truths

*Where automation, integration, and identity converge in 2025 — and where defenders are still losing.*

## 1 Identity is your new perimeter — defend it like one

Identity weakness is implicated in ~90% of Unit 42 IR investigations. 97% of identity attacks are password attacks (Microsoft) — phishing-resistant MFA stops over 99% of them. If you only fund one integration this year, fund the one between identity, EDR, and SIEM.

*Unit 42 2026 IR Report; Microsoft Digital Defense Report 2025*

## 2 Automate the obvious

Free analysts for the ambiguous. 79% of CrowdStrike detections in 2024 were malware-free — the fight has moved to behavioral, identity, and cloud telemetry, where humans can't scale. 86% of TI teams already trust AI-generated outputs. Extensive use of AI/automation saves an average $1.9M per breach and cuts 80 days from the lifecycle.

*CrowdStrike 2025 Global Threat Report; Recorded Future 2025; IBM 2025*

## 3 The edge you forgot is the edge they're hitting

22% of all vulnerability exploitation breaches now target edge infrastructure — firewalls, VPN concentrators, remote access gateways. Median time to remediate: 32 days. Median time from disclosure to mass exploitation for these CVEs: zero days. Asset inventory + vuln intel + EDR coverage on edge gear is non-negotiable.

*Verizon 2025 DBIR*

***"This is what we have that Cobra Kai does not. Their movement mile wide, but only inch deep." — Chozen, Season 5 Episode 4***

# Security Tool Stack Integration

03

**Integrating**

*the Tool Stack*

> *"It's Ok to Lose to Opponent. It's Never Okay to Lose to Fear“ – Mr. Miyagi (The Karate Kid: Part 3)*

THE PRACTICE

Embed threat intelligence directly into SIEM, SOAR, EDR, identity systems, and orchestration platforms so detection, blocking, enrichment, and intelligent alerting happen automatically. Reflexive defense beats heroic analysis.

**DETECT**

Push curated IOCs and behavioral signatures into SIEM, EDR, and DNS/proxy in real time — no manual ticket-to-rule lifecycle.

**RESPOND**

SOAR playbooks pre-wired for the top 10 incident types. Phishing reports, MFA bypass, infostealer hits, ransomware precursors.

**ENRICH**

Asset, identity, vuln, and TI context auto-applied to every alert. The analyst sees the why before they see the what.

> *"Alone We Are Nothing. But If We Work Together, We Have A Shot.“— Samantha LaRusso, Season 4, Episode 7*

# Where Integration Pays Off

*The data shows where attackers operate — and where your stack must integrate to keep up.*

## ~90%

Of Unit 42 incidents involve identity weakness; 65% of initial access is identity-based.

*Unit 42 2026 IR Report*

## 97%

Of identity attacks are password attacks. Microsoft now blocks 7,000 password attacks per second.

*Microsoft Digital Defense Report 2025*

## +84%

Increase in infostealers delivered via phishing in 2024; early 2025 weekly volume up 180% vs. 2023.

*IBM X-Force Threat Intelligence Index 2025*

## +442%

Vishing growth from H1 to H2 2024. By H1 2025, vishing already exceeded all of 2024.

*CrowdStrike 2025 Global Threat Report & Threat Hunting Report*

## +136%

Cloud intrusions up YoY — valid-account abuse drives 35% of cloud incidents.

*CrowdStrike 2025 Global Threat Report & Threat Hunting Report*

## 30%

Of compromised systems in infostealer logs were enterprise-licensed devices — BYOD bleeds credentials in.

*Verizon 2025 DBIR*

***"Fear does not exist in this dojo, does it? Pain does not exist in this dojo, does it? Defeat does not exist in this dojo, does it?" — Johnny Lawrence, Season 1 Episode 6***

*Sources: Unit 42 2025/2026 IR Reports; Microsoft Digital Defense Report 2025; IBM X-Force 2025; CrowdStrike 2025 Global Threat & Threat Hunting Reports; Verizon 2025 DBIR.*

# Measuring What Matters: 3 Truths



*How operationalized TI shows up in the metrics that boards and CISOs actually care about.*

### 1 Score adversaries by what they DO, not what they ARE

70% of incidents now exploit three or more attack surfaces; 87% unfold across multiple surfaces. Static actor scoring is obsolete. Use behavioral risk: tactic + asset criticality + active exploitation. The same threat actor profile means different things on a domain controller vs. a kiosk.

*Unit 42 2025 IR Report*

### 2 MTTD and MTTR aren't dashboards — they're savings

Organizations using AI and automation extensively save an average $1.9M per breach and cut 80 days from the breach lifecycle. Threat intel sharing alone reduces breach cost by an average $211,906. Faster identification (<200 days) saves $1.88M vs. >200 days. Time-to-detect is a P&L line.

*IBM Cost of a Data Breach 2025*

### 3 Show business outcomes, not tool outputs

65% of TI customers report it directly drives security technology purchasing; 58% say it informs business-initiative risk assessment. Reports for the SOC look like alerts saved. Reports for the board look like risk reduced and dollars avoided. Translate, or don't expect funding.

*Recorded Future 2025 State of Threat Intelligence Report*

***Daniel: "He's way off balance. I'm not sure Miyagi-Do is going to help!"***
***Chozen: "Then try something else. You know how his mind works, Daniel-san. You are his sensei! Wolf wants to obliterate him! You must do something!"***
***Season 6 Episode 8***

# Measuring Effectiveness



> *"Man Who Catch Fly with Chopstick, Accomplish Anything" – Mr. Miyagi (The Karate Kid)*

**THE PRACTICE**

Establish KPIs that prove operational impact and business value: detection accuracy, MTTD/MTTR, false-positive rates, dwell time, breach-cost avoidance, and ROI on operationalized TI — not feed counts and dashboard activity.

**OPERATIONAL**

MTTD, MTTR, dwell time, false-positive rate, alert volume per analyst, automated containment rate.

**PROGRAMMATIC**

Detection coverage by MITRE technique, feed utilization, playbook execution success, intelligence-to-action conversion.

**BUSINESS**

Breach-cost avoidance, risk reduction by asset class, ROI vs. tooling spend, board-level risk posture trend.

> *“"I fought with honor. If that lands me in second place, there's worse places to be."*
> *— Robby Keene, Season 6 Episode 13*

# What “Effective” Looks Like



*Six numbers that define the bar — and the savings — for operationalized TI today.*

## 11 days

Global median dwell time. Internally discovered: 10 days. Externally notified: 26 days. Adversary-notified: 5.

*Mandiant M-Trends 2025*

## <5 hrs

Time to data exfiltration in 25% of incidents — and under 1 hour in 1 of 5 cases.

*Unit 42 2025 IR Report*

## $4.44M

Global average breach cost — first decline in 5 years. U.S. average a record $10.22M.

*IBM Cost of a Data Breach 2025*

## -$1.9M

Per-breach savings for organizations using AI/automation extensively — plus 80 fewer days in lifecycle.

*IBM Cost of a Data Breach 2025*

## -$212K

Per-breach savings attributed specifically to threat intelligence sharing.

*IBM Cost of a Data Breach 2025*

## 351%

Documented total annual ROI from operationalized TI — ~100 hrs/week saved per program.

*Recorded Future 2025 ROI Report (UserEvidence)*

***"In Miyagi-Do, when an opponent comes swinging at you, you always respond in a circular motion. Moving in the opposite direction of what your opponent expects. Life's like that too." – Daniel LaRusso, Season 4 Episode 1***

*Sources: Mandiant M-Trends 2025; Unit 42 2025 Global IR Report; IBM Cost of a Data Breach 2025; Recorded Future 2025 ROI Report.*

# From Intelligence to Action

*Operational threat intelligence is a discipline, not a deployment. Continuously train these movements.*

01

## Define

*Your Profile*

Develop your org's Cyber Threat Profile.

Name your adversaries.

Name your crown-jewel assets.

Every other decision flows from these two.

02

## Curate

*Your Feeds*

Drop one source that doesn't map to your threat profile.

Replace it with one that does.

Signal-to-noise is the new maturity metric.

03

## Wire

*Your Stack*

Pick your top 3 incident types.

Pre-wire automation playbooks for each.

Intelligence that doesn't auto-respond is just a report.

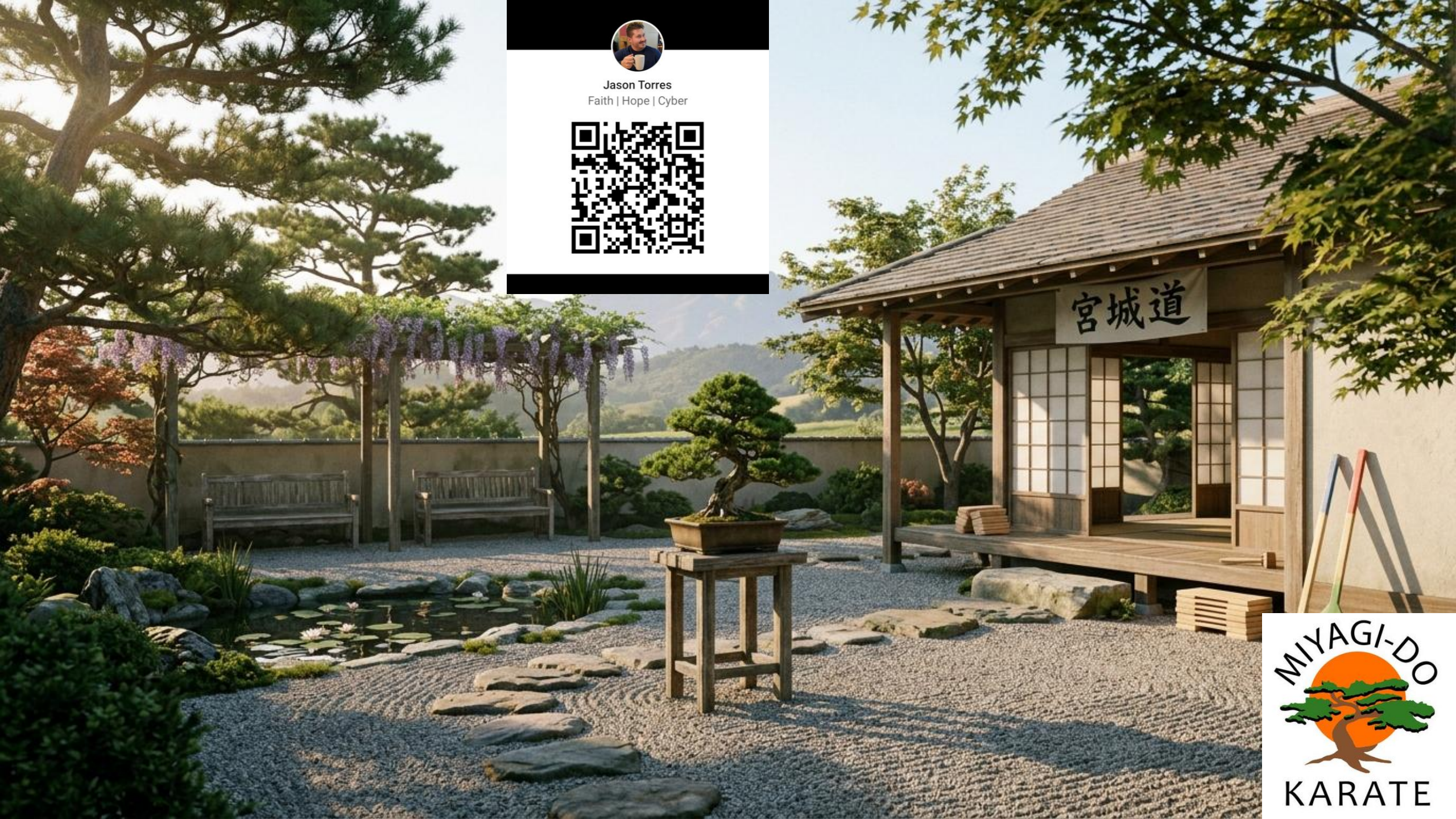
04

## Measure

*What Matters*

Translate your TI metrics into business language: breach-cost avoidance, risk posture trend, and ROI vs. spend—supported by MTTD, MTTR, true and false positive rate, incident reduction, blocked versus unblocked indicators, and time to containment.

*"Every Experience Holds The Potential Key To The Enlightenment You Seek." — To Ei Do [Way of the Sword & Shadow] Guiding Principle*


Jason Torres
Faith | Hope | Cyber
宮城道
MIYAGI-DO
KARATE