

Threat Intelligence Isn’t a Feed:

Using It to Drive Security Decisions and Calm the Chaos Monkeys

Who am I?



www.linkedin.com/in/coreyhlavacek

Corey Hlavacek

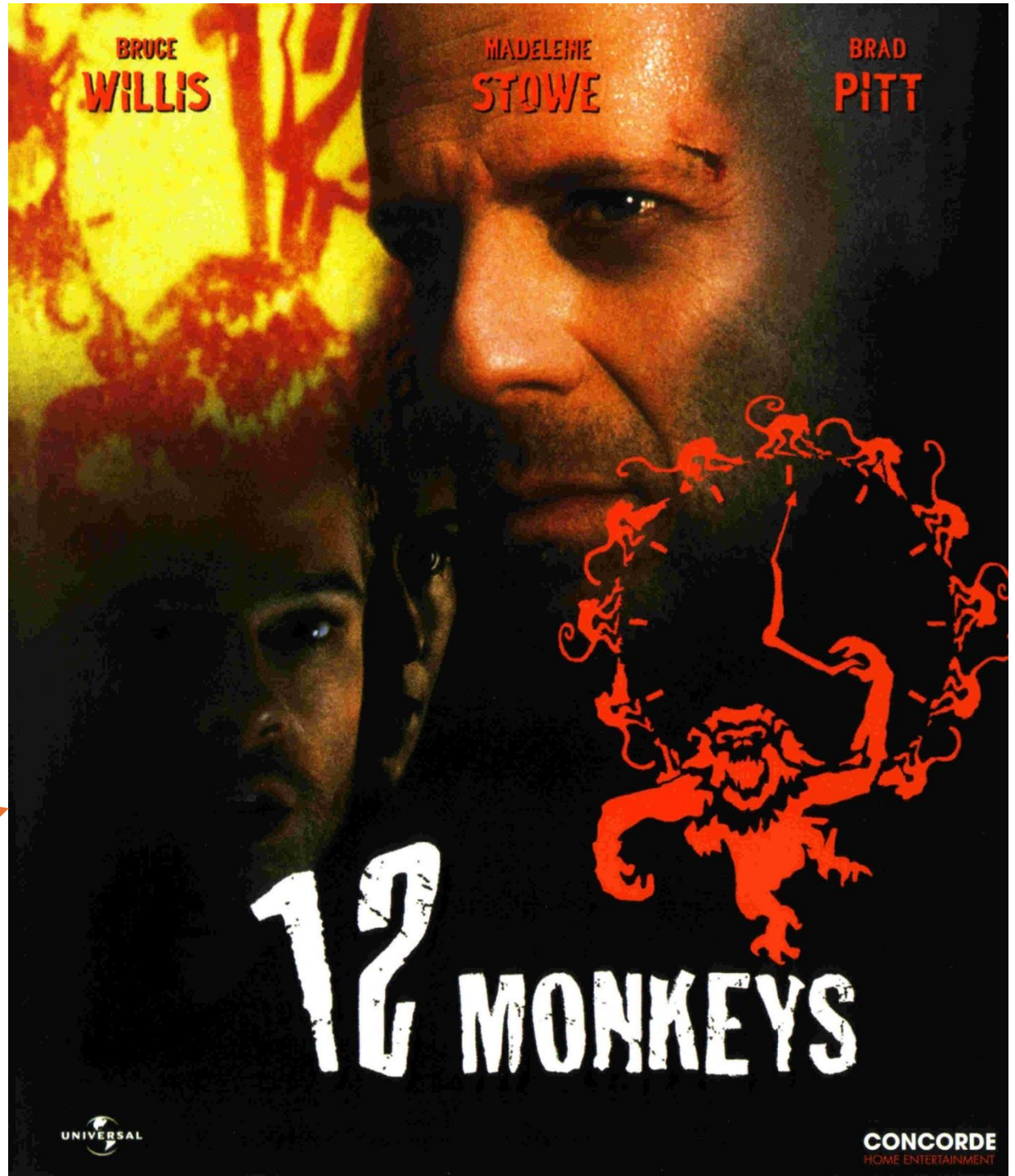
- Senior Director Information Security and Head of Security
  - enVista
    - Indianapolis-area supply chain consulting and technology firm
  - Responsible for all aspects of information security
- Prior Experience
  - Delta Air Lines, Texas Instruments, BNSF Railway
- Education and Certs
  - CMU CISO Executive Leadership Certificate
  - M.S. Information Systems Security
  - NACD.DC; NACD Certificate in Cyber-Risk Oversight
  - CISSP, CISM, ISSMP, C|CISO, CISA, and more…
- Conference Presentations
  - BSides Fort Wayne 2025 & 2026, CornCon 2025, Hacker Halted 2025, and the AI Agent & Copilot Summit North America 2025

The Obligatory Disclaimer…

This presentation is intended for educational purposes only and does not replace independent professional judgment. The content and statements of facts and opinions expressed and presented herein are my own and do not represent the views or opinions of enVista, LLC, CornCon, the Docent Institute, or sponsors.

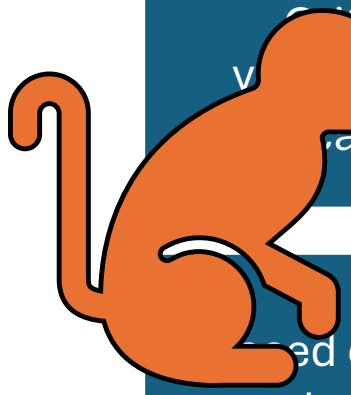
The Monkeys of Cybersecurity Chaos Are Already Inside Your Program

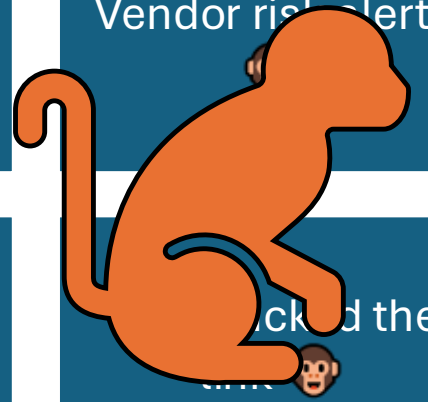
No, Not Those 12 Monkeys



The Monkeys of Cybersecurity Chaos Are Already Inside Your Program







Critical v…bility …cation

AI-enabled hack attempt

New threat-actor campaign

…ed credential alert

Executive concern after peer company's breach

Vendor ris… alerts

Active security incident

End-of-life operating system

…ck…d the …

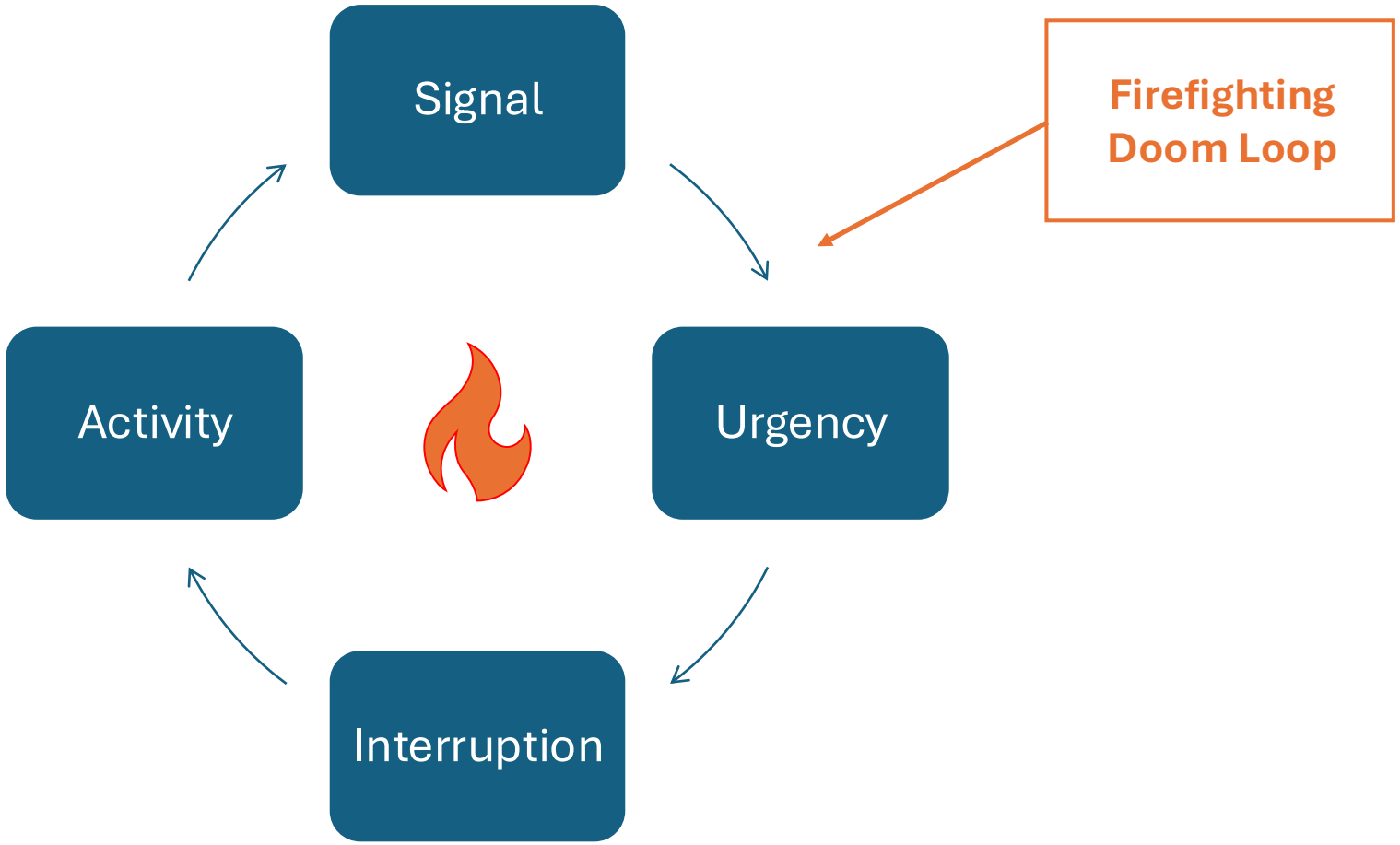
Brand impersonation attempt

Cloud misconfiguration

Operational and project commitments

Everything is urgent. Nothing is prioritized

The Latest Signal Controls the Agenda



Activity Is Not Control

Reactive Activity	Intelligence-led Control
Processing every alert	Establishing relevance
Circulating reports	Identifying a decision owner
Patching by severity score	Prioritizing actual exposure
Escalating the newest issue	Acting according to risk
Measuring activity volume	Measuring what changed

Threat intelligence shifts the program from processing inputs to improving decisions

Don’t Add Monkey Number Thirteen

Another feed gives the team

- Another alert
- Another report
- Another indicator
- Another interruption

Intelligence gives the organization

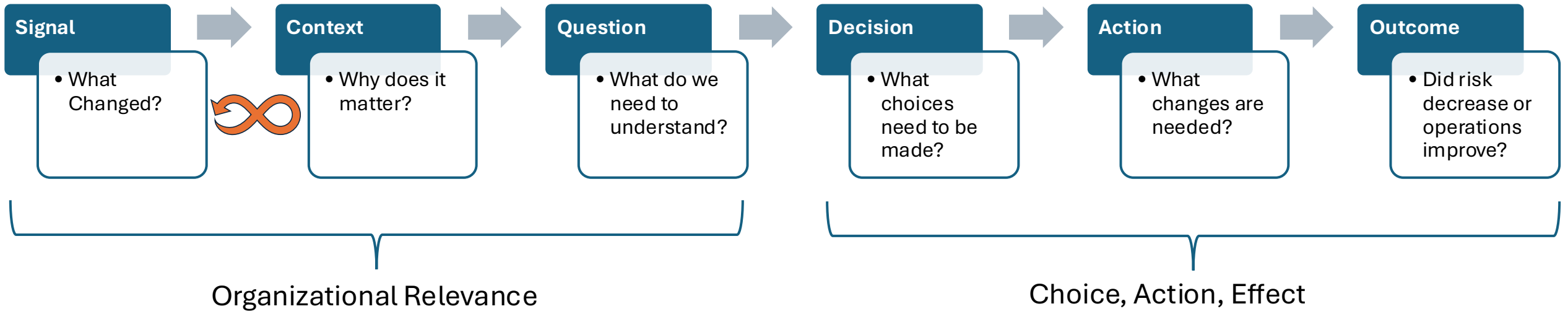
- Relevance
- Implications
- Options
- Ownership

Threat Intelligence is a Decision-Support Function

Threat intelligence helps the organization decide:

- What matters now
- What can safely wait
- Where exposure is changing
- Which control should change
- When normal operations should be interrupted
- When risk should be accepted deliberately

From Noise to Outcome



What Do We Actually Need to Know?

Three weak versus strong question pairs

Weak: What are the latest ransomware threats?

Better: Which current ransomware behaviors should change our controls or response readiness?

Weak: Which critical vulnerabilities were published?

Better: Which vulnerabilities create material exposure to our critical operations?

Weak: Are employee credentials for sale?

Better: Which exposed identities create a risk that justifies an immediate control change?

Priority Intelligence Requirements (PIRs): Keeping the Function Focused

A useful PIR should be:

- Tied to a material risk or operational concern
- Capable of influencing a decision
- Assigned to a decision owner
- Answerable with available or obtainable information
- Reviewed on a defined cadence
- Retired when it no longer produces value

Intelligence Without Ownership Becomes Commentary

Intelligence question	Decision owner	Possible decision
Which exposures require immediate remediation?	Infrastructure or application owner	Interrupt, mitigate, schedule, accept
Which identity risks require stronger controls?	IAM function or business owner	Restrict, challenge, rotate, monitor
Does this incident require broader containment?	Incident commander	Isolate, escalate, activate continuity
Does vendor risk require intervention?	Business sponsor or risk owner	Restrict, disconnect, invoke contingency

The Model Works Against Real Problems

Four application areas:

- Vulnerability prioritization
- Incident response
- Identity controls
- Enterprise and third-party risk

Same chain. Different signal. Different owner. Different decision.

A Severity Score is Not a Business Priority



Vulnerability Prioritization: A Severity Score is Not a Business Priority

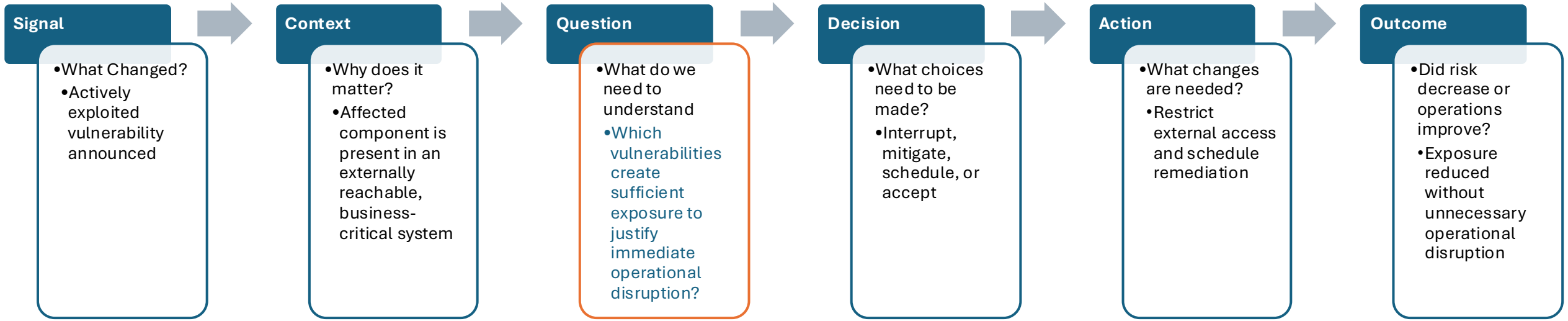
Typical "Emergency" Vulnerability Remediation Process Flow



Impacts and Effects

- Backlog volume becomes the dominant measure
- Headline vulnerabilities interrupt planned work
- Asset importance and reachability arrive late
- Operations and security argue without shared context
- Diminished security reputation and influence
  - Chicken Little

Vulnerability Prioritization: From Noise to Outcome



A Short Detour:

Vulnerability Threat Intelligence: AI Edition

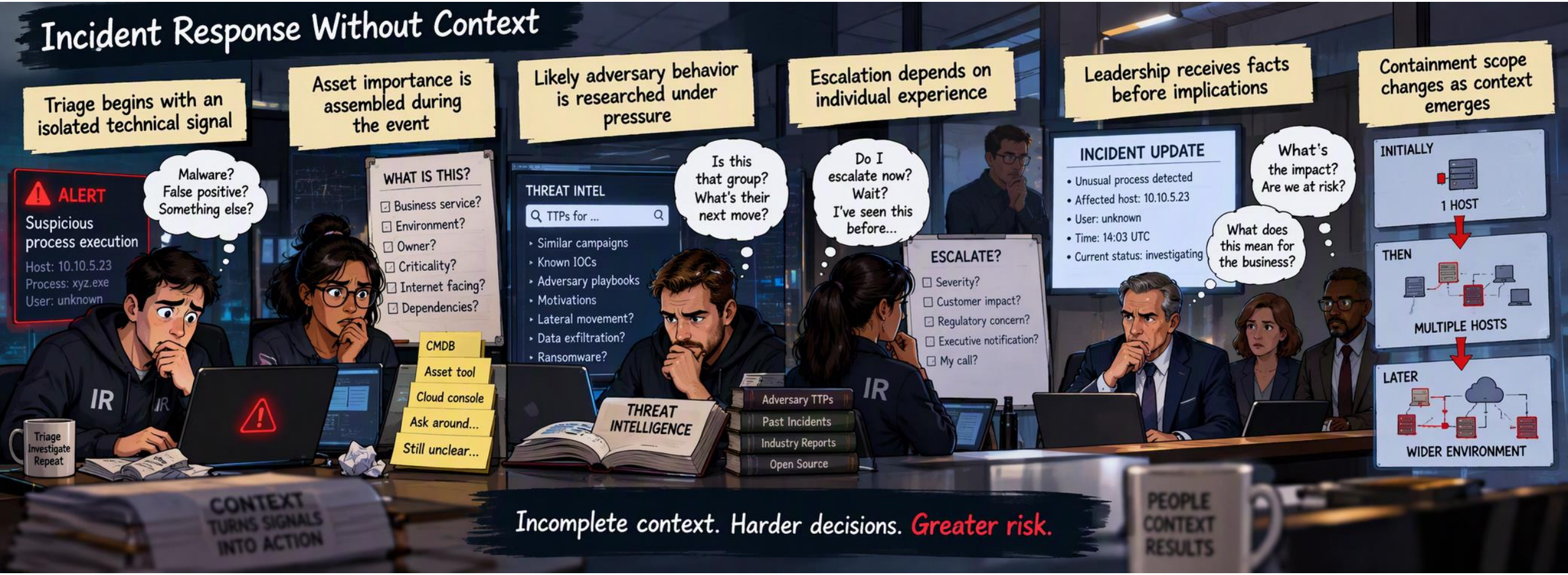
- Probably one of the most important components of threat intel today
- The NVD system is broken
  - *Limited enrichment and scoring*
- AI Vulnpocalypse or AI Vulnageddon
- Timeline compression
  - *Zero Days >> Zero Hours*
- AI exploitation capabilities (and vulnerability chaining?)
  - *Remember those "medium" vulnerabilities?*
- New Risk: Vulnerabilities in AI Systems Themselves
- No longer about how many vulns we patch but what we patch and when
  - *This is going to drive the auditors crazy*

A Short Detour:

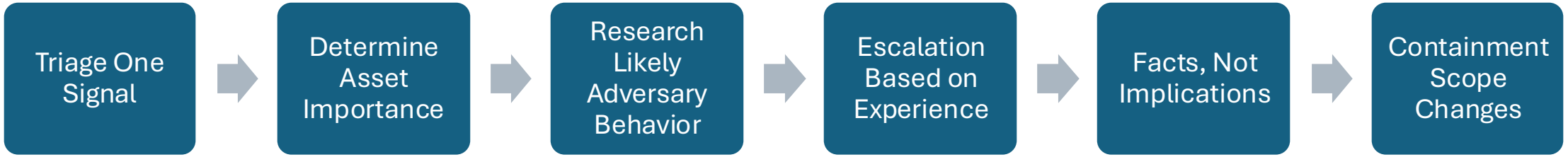
The Vulnpocalypse



Incident Response Without Context



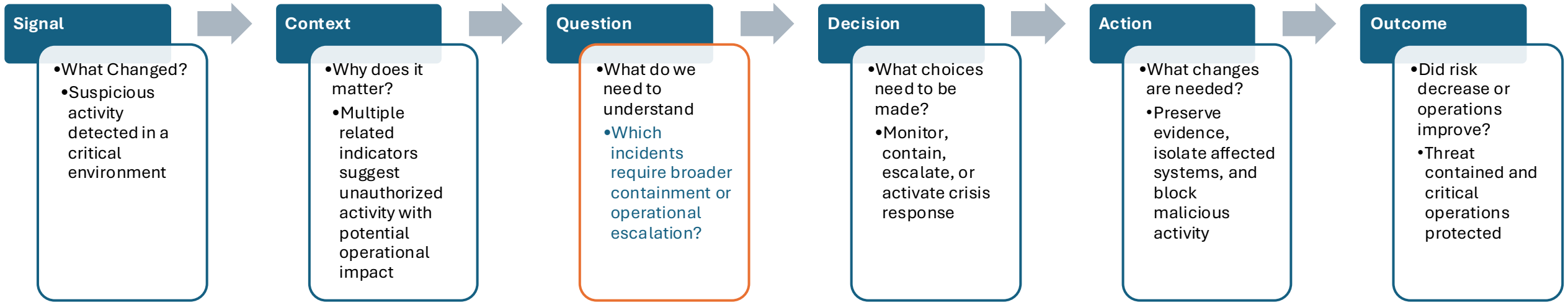
Incident Response Without Context



Incident Response Context Provided by Threat Intelligence

Intelligence contribution	Decision supported
Relevant adversary behavior	Expand or narrow investigation
Likely objectives	Prioritize systems, identities, and evidence
Known attack patterns	Select containment actions
Business and operational context	Escalate to crisis or continuity processes
Confidence and uncertainty	Determine proportional response

Incident Response: From Noise to Outcome



Identity Protection Without Context



Identity Protection Without Context



Trust is removed before exposure, business impact, or dependencies are understood.

Identity Intelligence Is Not Only Credential Monitoring

Four identity categories that may require different decisions

- Workforce identity
- Privileged identity
- Customer identity
- Non-human identity

Central question:

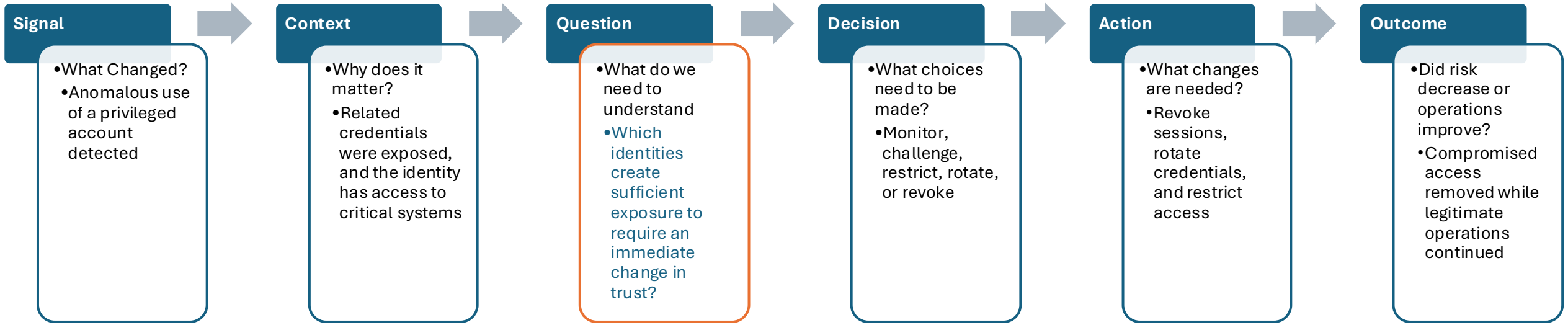
Given what we know, how much should we continue to trust this identity?

Apply Friction Where the Risk Justifies It

Possible intelligence-led actions:

- Require phishing-resistant authentication
- Trigger step-up authentication
- Restrict access or functionality
- Revoke sessions
- Rotate keys, secrets, or tokens
- Increase monitoring for targeted identities
- Notify customers or force credential reset
- Review downstream trust relationships

Identity Protection: From Noise to Outcome



Some Threat-Intelligence Decisions Belong Outside Security

Four Outward-Facing Domains

Third-party Dependency
Restrict, disconnect, or activate an alternative

Customer and Brand Trust
Block, pursue takedown, or communicate

Geographic Operations
Continue, modify, relocate, or exit

People and Facilities
Protect personnel, modify operations, or close

Different Signals, Same Decision Model

Third-Party Compromise

- Question: Which providers create credible paths to our environment?
- Decision: Monitor, restrict, disconnect, or activate an alternative.
- Outcome: Reduced dependency and supply-chain exposure

Brand Impersonation

- Question: Is customer harm likely enough to justify intervention?
- Decision: Block, investigate, pursue takedown, or communicate.
- Outcome: Reduced fraud and customer harm.

Threat Near Facility

- Question: Are people or operations at material risk?
- Decision: Continue, modify, relocate, or suspend operations.
- Outcome: Employees protected and business continuity supported.

Decisions, Not Sources

Wrong Starting Questions

- Which platform should we buy?
- How many feeds should we collect?
- How many reports should we publish?
- What can we automate?



Better Starting Questions

- Which recurring decision is currently poorly informed?
- Who owns that decision?
- What context would improve it?
- What action should a credible answer trigger?

Make the Decision Model Repeatable

1. **Signal:** Detect what changed
2. **Context:** Establish organizational relevance
3. **Question:** Define what must be understood
4. **Decision:** Present choices and tradeoffs
5. **Action:** Assign ownership and timing
6. **Outcome:** Examine what changed and refine the next cycle

Pilot One Decision That Already Causes Pain

Month 1: Define

- Select one recurring decision
- Name the decision owner
- Define one or two questions (PIRs)
- Identify available context and sources
- Establish escalation criteria

Month 2: Operate

- Apply the six-step model
- Produce a concise decision brief
- Record decisions and owners
- Identify context gaps

Month 3: Evaluate

- Review decisions influenced
- Measure time to action
- Identify unnecessary escalations avoided
- Determine whether risk changed
- Continue, revise, or expand

Measure Outcomes, Not Outputs

Measure

- Decisions influenced
- Time from signal to action
- Exposure or blast radius reduced
- Unnecessary escalations avoided
- Control changes completed
- Operational interruption deliberately approved or avoided

De-emphasize

- Reports produced
- Indicators collected
- Feeds connected
- Alerts enriched
- Pages written

Activity explains what the team did. **Outcomes** explain why it mattered.

Minimum Governance for Repeatable Decisions

Minimum governance:

- Three to five active PIRs
- A named decision owner for each PIR
- A standard decision brief
- Defined escalation paths
- A decision log
- A recurring PIR and outcome review
- Revision or retirement of questions that no longer create value

How Can I Apply This?

Today

- Identify one recurring source of security chaos.
- Write down the decision it creates.
- Name the decision owner.
- Define the context that would improve the choice.

Next Week

- Convert the problem into one PIR.
- Build a concise decision brief.
- Test it against a real signal.
- Ask whether the output changed a decision.

This Quarter

- Operate one bounded use case.
- Record the decisions it influences.
- Measure time to action and resulting change.
- Refine or expand based on demonstrated value.

Threat Intelligence Should Help You Decide

Threat intelligence is not about knowing everything happening in the threat landscape. It is about knowing enough to make the next important decision well.

Stop feeding the chaos. Start using intelligence to control it.

Thank You!

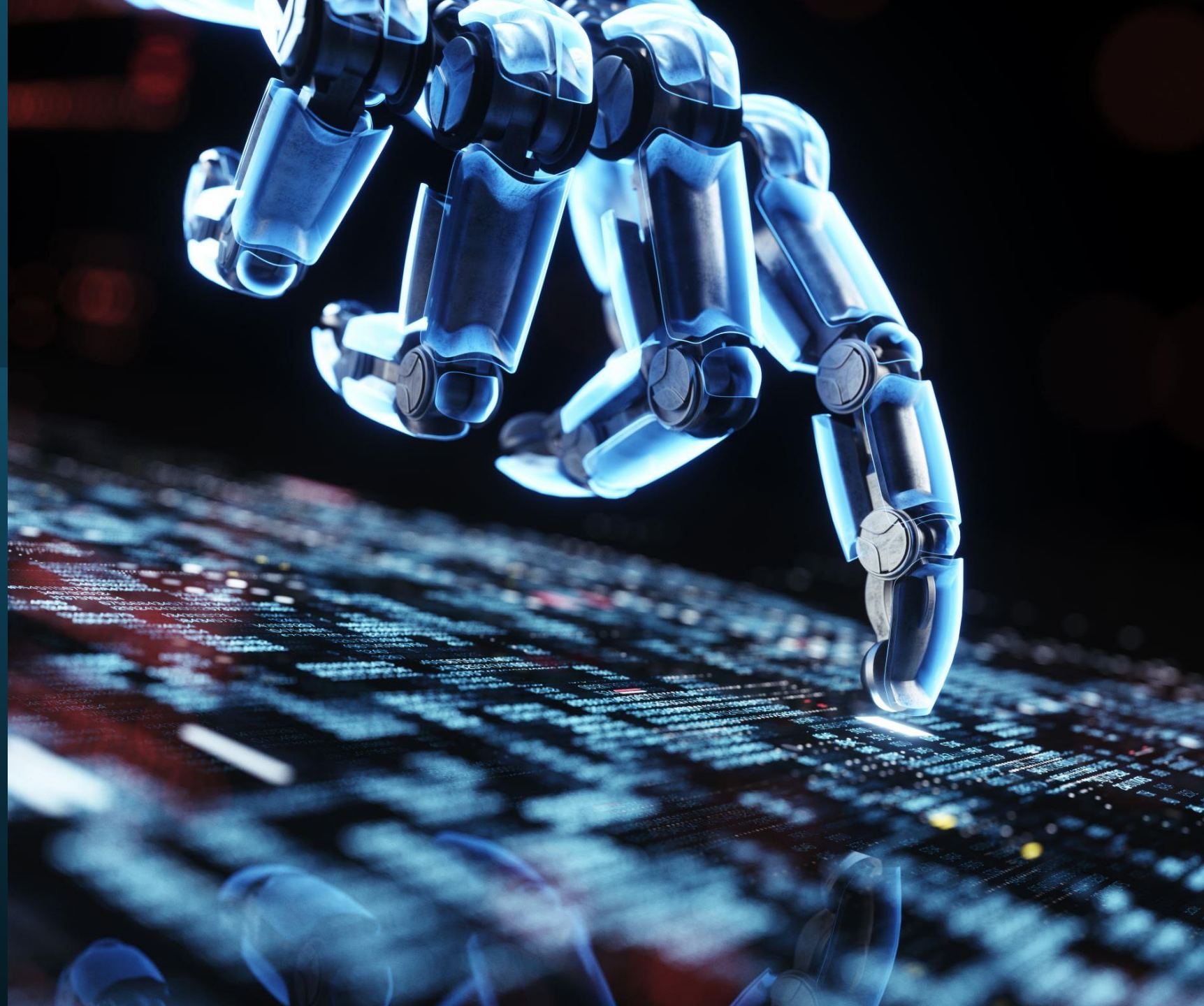
Continue the conversation by connecting with me on LinkedIn



www.linkedin.com/in/coreyhlavacek

Appendix

Cyber Threat Intelligence Today



Communicate the Decision Clearly

Every intelligence brief should answer three questions

WHAT

- What changed?
- What do we know?
- What remains uncertain?

SO WHAT?

- Why does this matter to us?
- What business or operational consequence is plausible?
- How confident are we?

NOW WHAT?

- What decision is required?
- What options are available?
- Who owns the decision?
- When must it be made?

Adapted from the Critical Reflection Model: Terry Borton

Cyber Threat Intelligence Today

- Not limited to Physical or Geopolitical
  - Not just spying on people and places
- Not just the dark web
- Applicable to all organizations
- Democratized
- Many context infused use cases

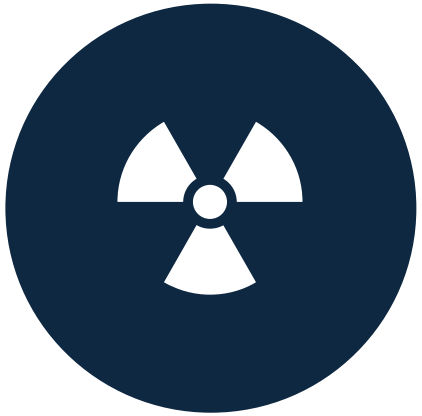
Cyber Threat Intelligence Evolution

- No longer tactical
- Use cases have expanded beyond traditional cyber threat intelligence
- **Cyber threat intelligence has become a decision support capability for critical business decisions**
  - Threat Intelligence provides answers to key business questions

Key Questions Answered by Cyber Threat Intelligence



FINANCIAL

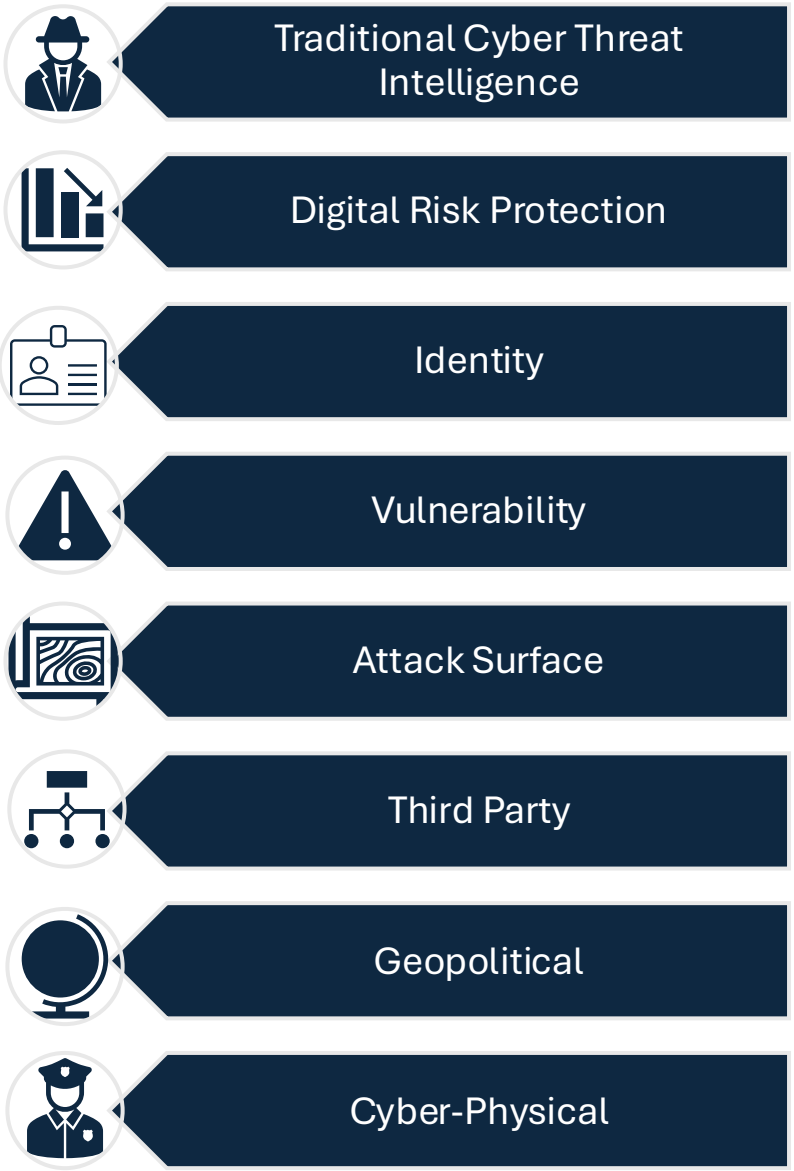


RISK



OPERATIONS

Cyber Threat Intelligence Domains



‘Traditional’ Cyber Threat Intelligence

- Traditional Cyber Threat Use Cases
- What questions does traditional threat intel answer?
  - Financial: What attackers do we face and what controls do we have in place?
    - What technologies do we need to invest in?
      - MFA, EDR, email security
  - Risk: What part of the business is most targeted right now?
  - Operations: What attacks are we getting now and do we need to change how we’re operating today?
    - Enhanced authentication requirements

Digital Risk Protection

- An organization’s external radar feeding decision making
- Visibility into threats before they hit the environment or customers
- Questions answered by Digital Risk Protection?
  - Financial: Which external exposures actually cost us money and where should we invest to reduce that?
  - Risk: Is our brand being abused in ways that could harm customers and our brand reputation?
  - Operations: Which external threats require active intervention (takedown, blocking, escalation)?

Attack Surface

- Identifies what is externally exposed, misconfigured, or reachable and drives decisions about what needs to be reduced, hardened, or controlled.
- Questions answered:
  - Financial: Are we prioritizing investments that actually reduce exposure?
  - Operations: Do we actually know what we own?
  - Risk: Do we know what systems and data are exposed?

Vulnerability Threat

- What to fix, when to fix it, and how quickly to fix it
- Infused by environmental context
- Questions answered by Vulnerability Threat intelligence
  - Financial: Where should we invest in prevention vs remediation? (financial)
  - Risk: Do we have a broader exposure management problem
  - Operations: Do we disrupt the business now to patch?

Identity (Employee / Non-Human Identity)

- A decision function about trust, access, and business risk tied to internal identities
- Questions answered by Identity threat intelligence
  - Financial: Do we need to implement stronger authentication methods?
  - Risk: How much autonomy do we allow machine identities?
  - Operations: Do we need to change identity controls now or later?

Identity (Customer)

- A decision function to reduce fraud (protect revenue) and maintain customer trust
- Questions answered by Identity threat intelligence
  - Financial: Do we need to change how we design customer identity?
  - Risk: Which customer segments are at the highest risk?
  - Operations: Do we need to implement additional friction now?

Side Bar: Intelligence Relationships



Vulnerability Threat Intelligence: AI Edition

- Probably one of the most important components of threat intel today
- The NVD system is broken
  - Limited enrichment and scoring
- AI Vulnpocalypse or AI Vulnageddon
- Timeline compression
  - Zero Days >> Zero Hours
- AI exploitation capabilities and vulnerability chaining
  - Remember those “medium” vulnerabilities?
- New Risk: Vulnerabilities in AI Systems Themselves

- No longer about how many vulns we patch but what we patch and when
  - This is going to drive the auditors crazy

Third Party

- Third-party threat intelligence informs decisions about who we do business with, how much we trust them, and what risk we inherit from them
- Can be context infused
- Questions answered by third party risk intelligence:
  - Financial: Where should we invest in vendor resilience vs internal controls?
  - Risk: Do we focus on a single provider or diversify?
  - Operations: Do we continue operating through a compromised third party?

Geopolitical

- Where is risk changing due to geopolitical conditions and how does that affect our business?
- What questions does Geopolitical Threat Intellgience answer
  - Financial: Do we change how we architect systems across regions?
  - Risk: Which countries and regions introduce elevated cyber risk?
  - Operations: Do we operate, expand, or exit a region?

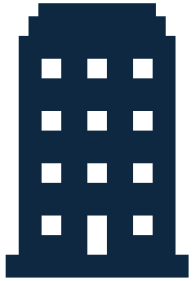
Physical Risk

- “Do real-world threats put our people, facilities, or operations at risk—and how do we respond?”
- Common Capabilities
  - Civil unrest, protests, crime patterns, violence indicators
  - Threats near facilities or offices
  - Targeted threats to executives or key staff
  - Event-specific threats
  - Crowd-related risk indicators
- What questions does cyber-physical intelligence answer?
  - Finance: Do we need to invest in physical security controls
  - Risk: What level of risk are we willing to accept for physical exposure
  - Operations: Do we continue operations at a specific location?

Geopolitical and Physical Risk Intelligence: What's the difference?



VS



Geopolitical Threat Intel

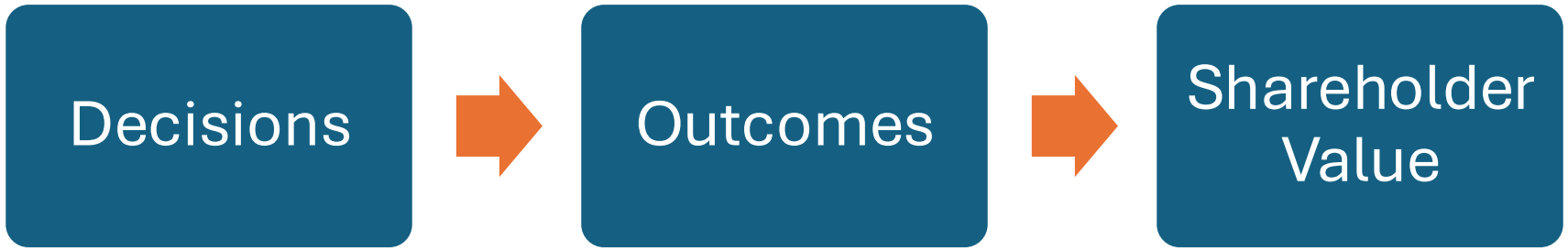
Where should we operate and what macro risk do we accept?

Physical Threat Intel

Are our people and facilities safe right now?

Decisions to Outcomes

- Executives get paid to make decisions, that produce outcomes, that ultimately increase shareholder value
- So, we need to use the same language



Domains → Questions → Decisions → C

Priority Intelligence Requirements

Cyber Threat Intelligence Domain	Example Question	Decisions	Outcomes
'Traditional' Threat Intel	Who is attacking us right now?	Block an attacker	Unclear
Digital Risk Protection	Where is our brand being impersonated externally?	Takedown phishing site	Protect brand trust
Identity (Employee / Non-Human Identity)	Which identity paths are most exposed to takeover?	Restrict functionality	Prevent data breach
Identity (Customer)	Where are we seeing active credential abuse impacting customers?	Increase customer friction	Reduced fraud loss
Vulnerability	Which vulnerabilities are actively exploited in our environment?	Schedule downtime	Operational Uptime
Attack Surface Intelligence	Where can we actually be attacked right now—and how bad is it if we are?	Retire unmanaged assets	Cost Reduction
Third-party	Which vendors are showing signs of compromise or degradation?	Disconnect from vendor	Reduced supply chain risk
Geopolitical	Which regions are becoming higher risk for our operations?	Exit region	Avoid regulatory risk
Cyber-Physical	Which facilities face elevated safety risk tomorrow?	Close facility	Protect employees

Measurement and Proving CTI Impact

- **We can take it a step farther and define measures for outcomes**
- **Not going to the metrics rabbit hole but some broad categories and approaches…**

Decisions Influenced

- Measures how intelligence changed prioritization, resource allocation, or control implementations within the organization

Time to Action

- Track the speed from threat identification to response, showcasing efficiency of intelligence operations.

Risk Impact

- Evaluates reduction in exposure, lowered incidents likelihood, and mitigation of business disruptions.

Qualitative Case Studies

- Use real examples demonstrating how intelligence reports led to concrete security improvements and outcomes.