Digital Innovation Hub Trakia

Co-funded by the European Union

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

OSCRAT Open-Source Cyber Resilience Act Tools

From Chaos to Control

Strategic Cyber Incident Management in a Complex Digital Environment.

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. – Project: 101190180.

Your Guide Through the Regulatory Maze.

Auditor & Standardizer

Lead Auditor for Management Systems (ISMS, ITSMS, BCMS).
Deputy CEO of the Bulgarian Union of Standardizers.

Academic Leader

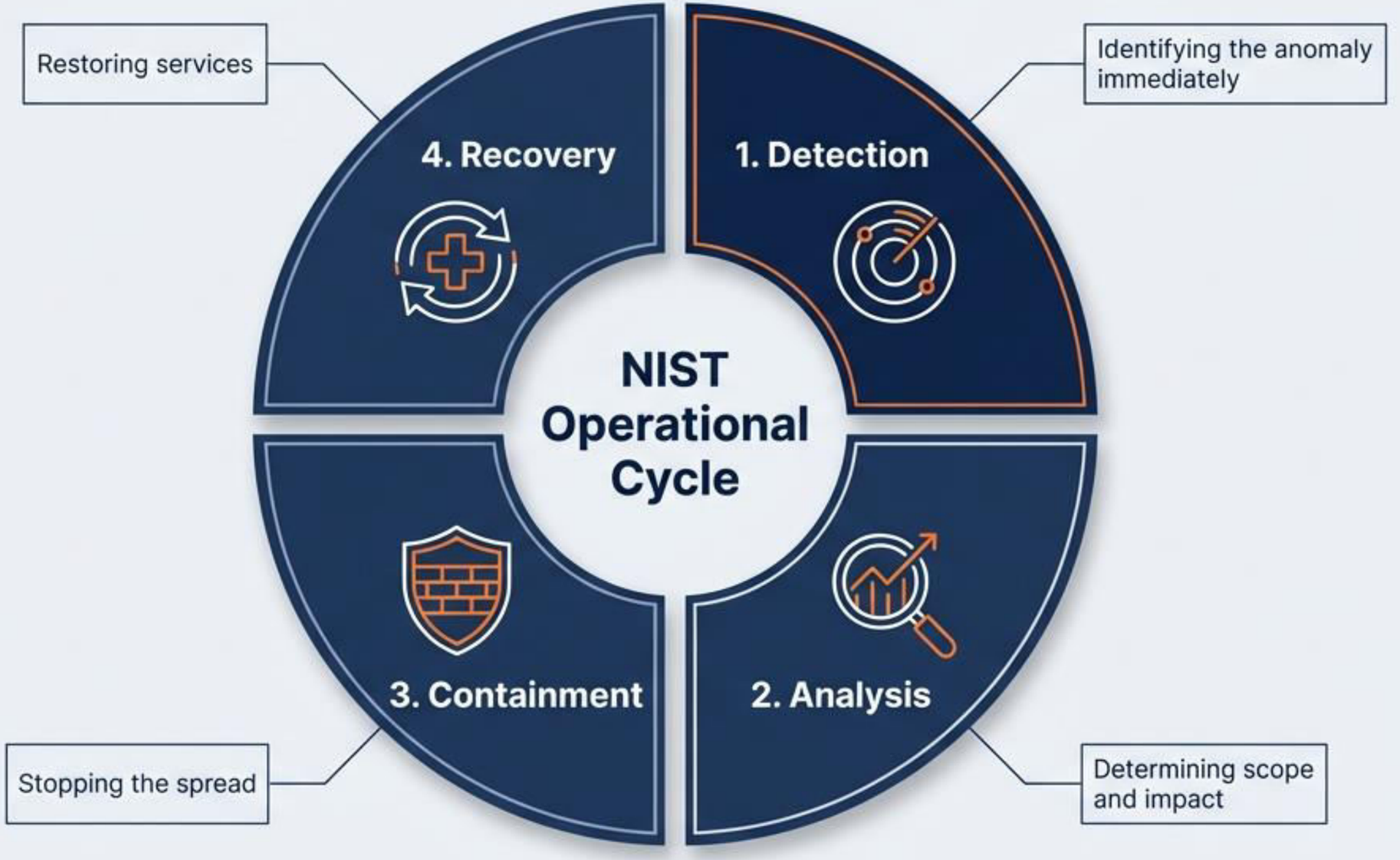
Chairman of the Institute for Artificial Intelligence.
Assistant Professor at UniLIT.

Subject Matter Expert

Specializing in Cybersecurity Standards, Incident Response, Cryptography, and Zero Trust Architectures.

Active participant in numerous European and national cybersecurity projects.

Tactical Response: The Practical NIST Model



From Detection to Recovery: This cycle turns the abstract CRA requirement into a daily operational workflow.

Structural Resilience: ISO 27035

Ad-hoc Approach

- Chaos
- Hero-dependent
- Unrepeatable

TRANSFORMATION

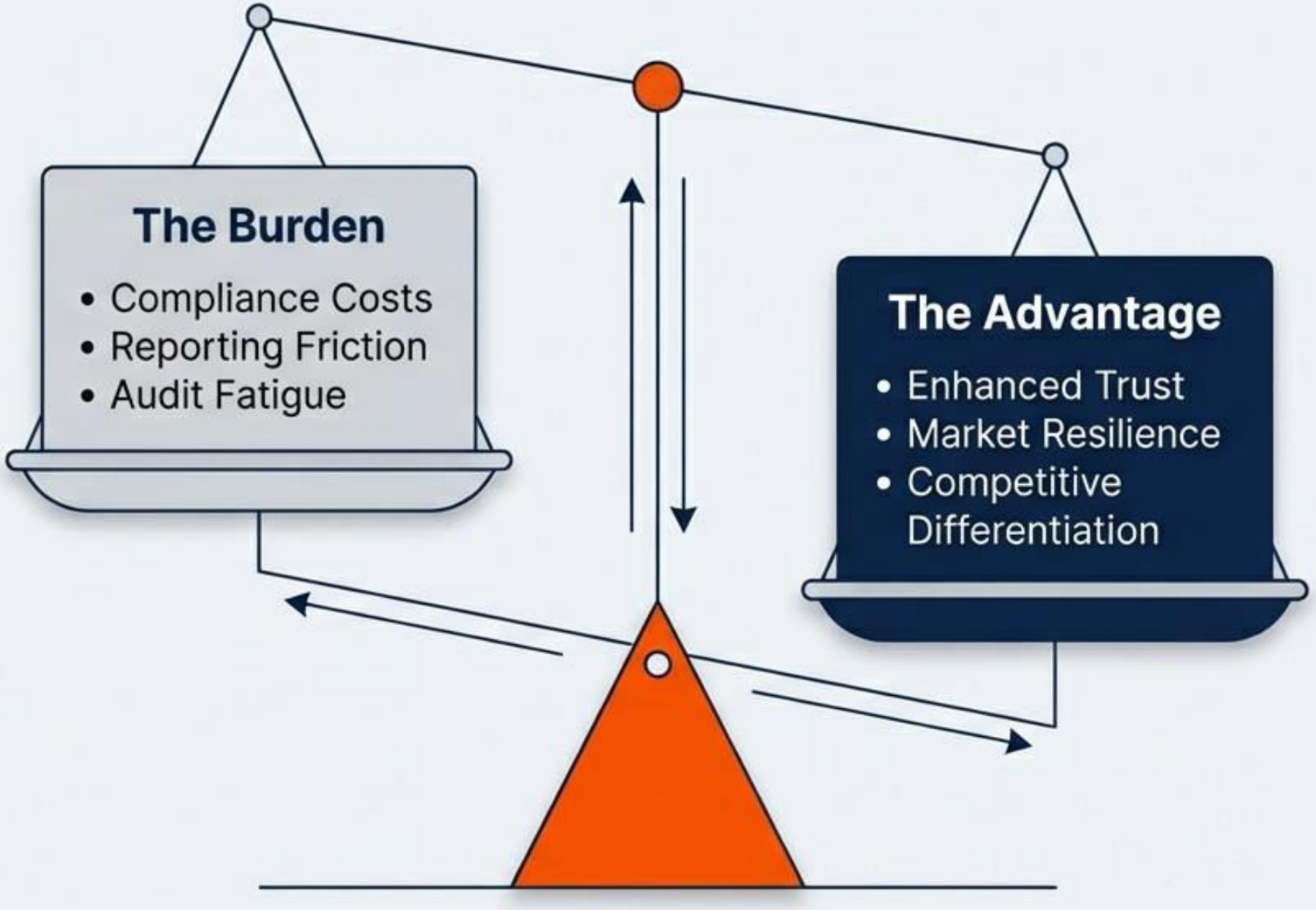
ISO 27035 Approach

1. Preparation
2. Detection & Reporting
3. Assessment & Decision
4. Responses
5. Lessons Learned

- Documented
- Process-driven
- Auditable

The Architecture of Resilience. ISO 27035 provides the management container in which the NIST tactics operate, ensuring consistency across the organization.

The Strategic Shift: Regulation as Advantage.

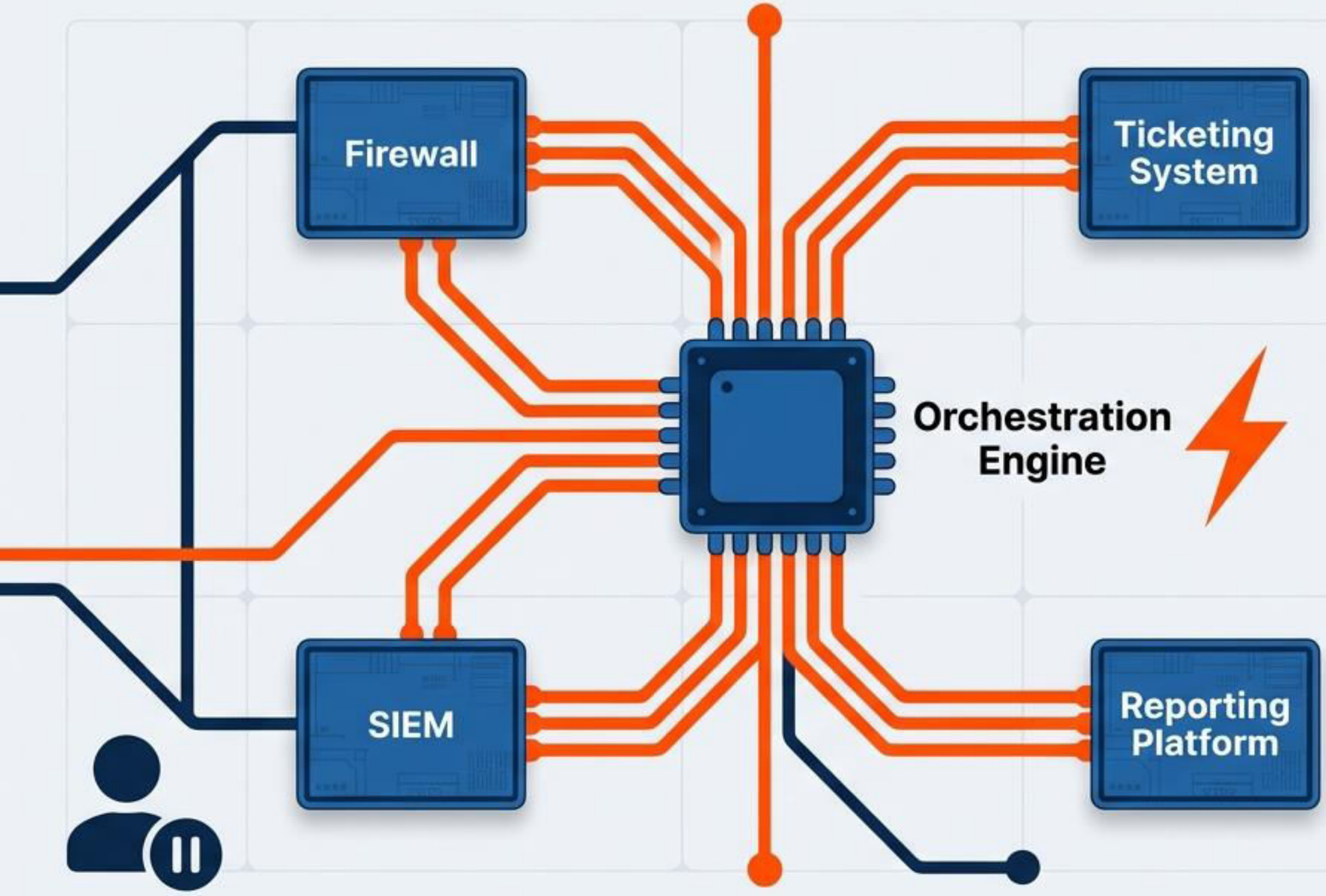


Turning Regulatory Challenges into Competitive Advantages.

Organizations that master the Single Reporting Platform and ISO standards prove to their customers that they are safe partners in a high-risk digital ecosystem.

Compliance is not just a cost center; it is a trust badge.

Beyond Response: The Automated Ecosystem



To meet CRA deadlines, we must move at machine speed.

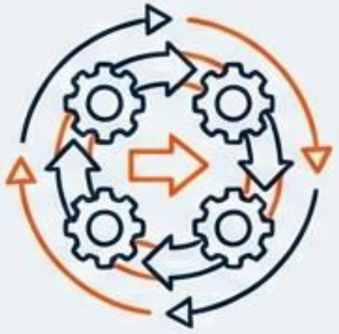
1. **Automation:** Handling repetitive detection tasks instantly.
2. **Orchestration:** Coordinating tools into a single workflow.
3. **Integration:** Moving beyond isolated tools to a unified defense mesh.

From Chaos to Control.

The Mandate

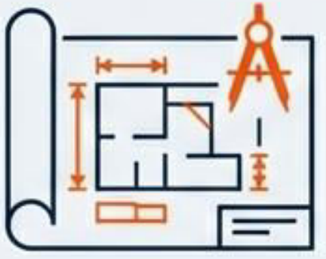
Cyber Resilience Act &
Single Reporting Platform

The Method



NIST Operational Cycle
(Detect - Recover)

The Structure



ISO 27035
Management Standards

The tools are defined. The regulation is active.
The path to resilience is clear.

Co-funded by the European Union. Project: 101190180

Incident Response & Cyber Risk Management

Navigating the Paradigm Shift in NIST SP 800-61r3

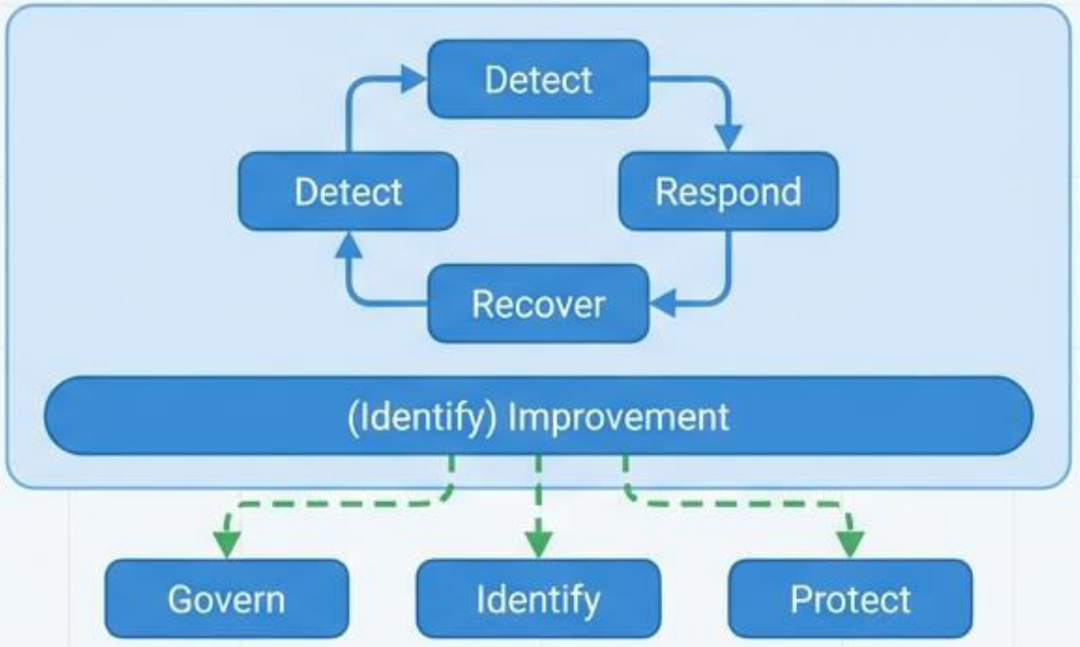
A CSF 2.0 Community Profile | Strategic Overview

The Evolution: From Isolated Triage to Integrated Risk

The Past (SP 800-61r2)

- Rare incidents
- Siloed teams
- Check-the-box compliance

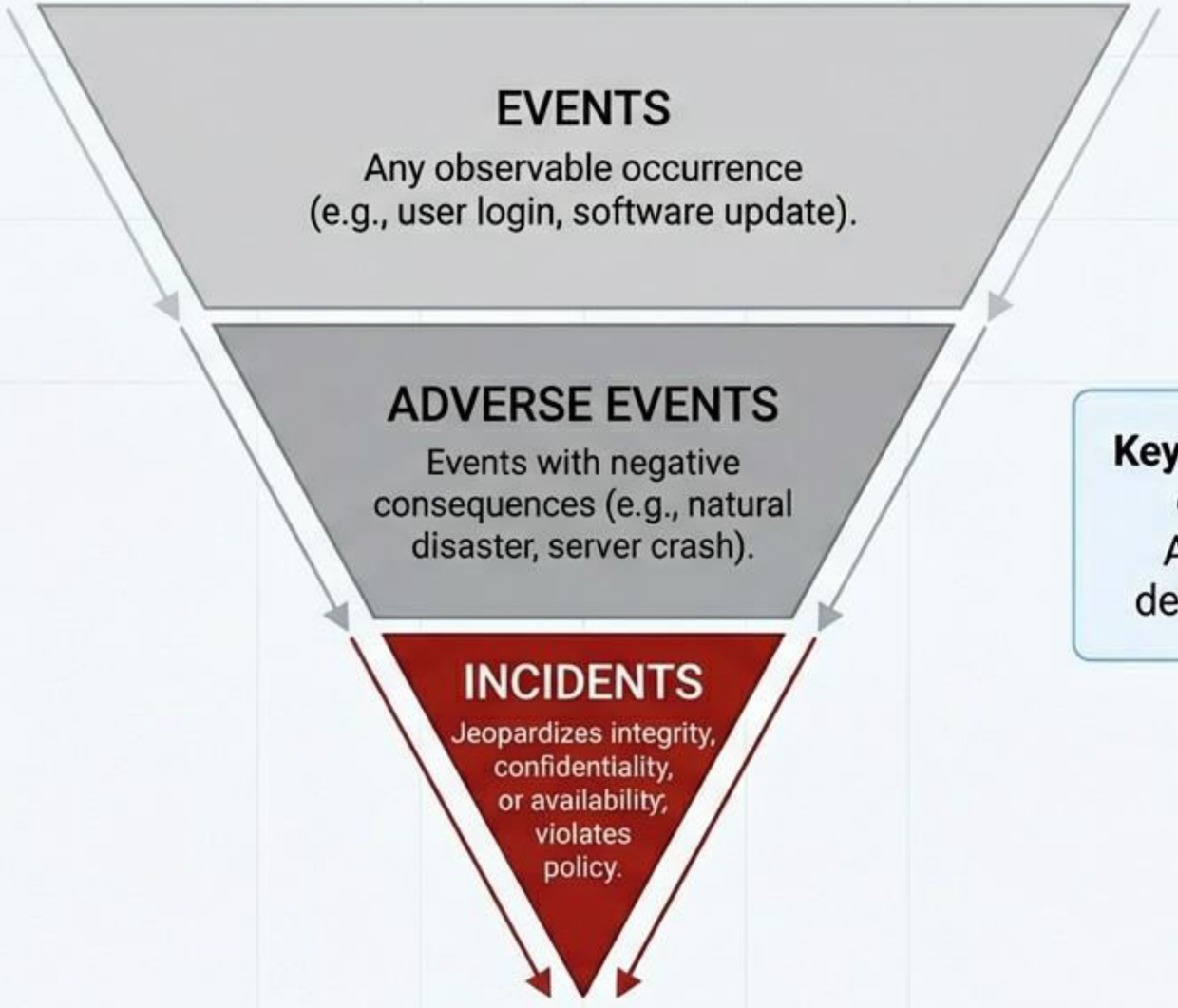
The Future (SP 800-61r3)



- Continuous improvement
- ERM integration
- CSF 2.0 Mapping

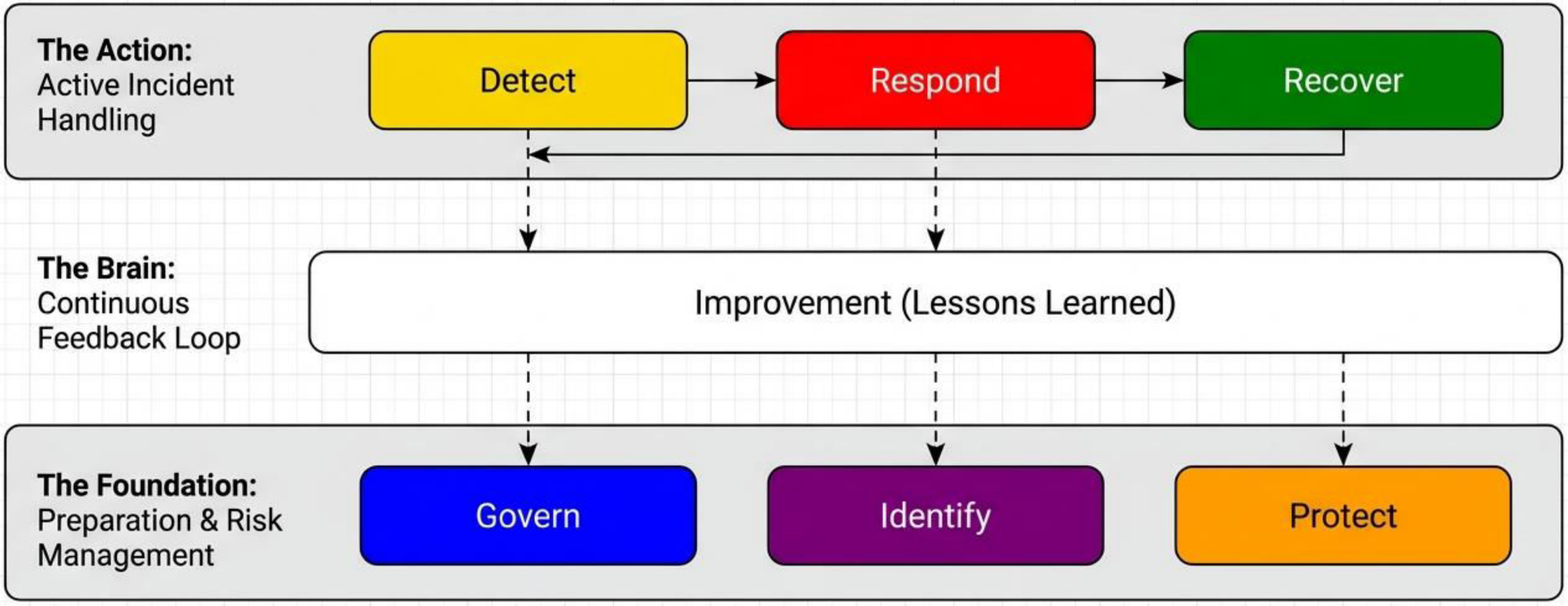
Incident Response is no longer a standalone technical activity.
It is a critical component of Enterprise Risk Management.

Defining the Scope: Filtering the Noise



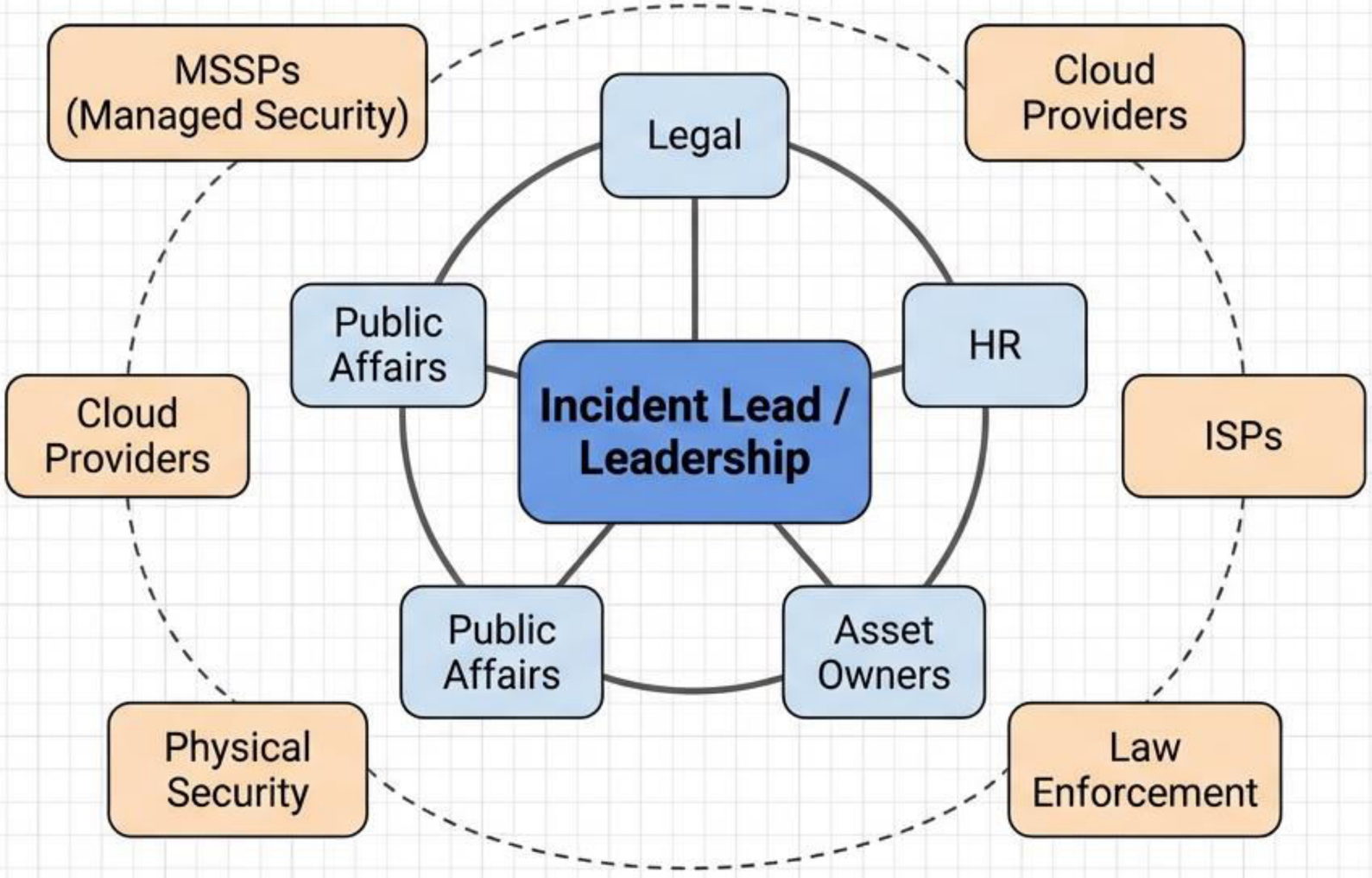
Key Insight: Not all adverse events are incidents. Analysis is required to determine the difference.

The New Architecture: IR Mapped to CSF 2.0



Preparation is no longer a single phase. It is the cumulative output of Governance, Identification, and Protection.

Roles, Responsibilities, & The Extended Network



The Shared Responsibility Model

- Third parties play critical roles in detection and response.

- **Crucial Distinction:** You can transfer tasks, but you cannot transfer accountability.

- SLAs must clearly define information flows and decision authority.

GOVERN (GV)

Setting the Strategy, Policy, and Expectations.

High-Value Actions:

1. **Policy (GV.PO)**: Policies must explicitly **cover Incident Response**, not just general security.
2. **Supply Chain (GV.SC):** Contracts with suppliers must mandate incident reporting and vulnerability disclosure.
3. **Risk Integration (GV.RM):** Incident decision-making must be informed by broader enterprise risks (reputational, legal), not just technical factors.

IDENTIFY (ID)

Knowing What We Defend & The Threats We Face.

High-Value Actions:

1. **Asset Management (ID.AM):** Maintain automated inventories. You need to know asset criticality **before** the incident occurs.
2. **Threat Intelligence (ID.RA):** Ingest CTI from sharing forums (ISACs). Use it to model threats and understand TTPs.
3. **Vulnerability Mgmt (ID.RA-01):** Record and validate vulnerabilities to inform risk decisions during an active crisis.

PROTECT (PR)

Reducing Impact & Enabling Investigation.

High-Value Actions:

1. Logging (PR.PS-04):
Logs are vital. Without logs, detection and recovery are impossible.

2. Backups (PR.DS-11):
The safety net for Recovery. Backups must be tested and isolated (immutable) to survive ransomware.

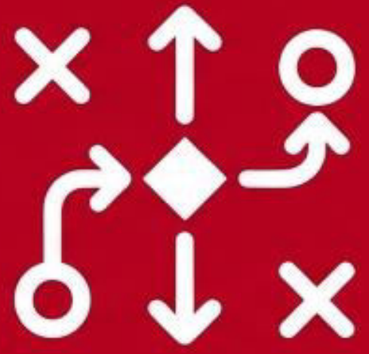
3. Training (PR.AT):
Conduct role-based training. General awareness is not enough; specific roles need specific IR scenarios.

DETECT (DE)

Continuous Monitoring & Finding the Signal

High-Value Actions:

1. **Continuous Monitoring (DE.CM):** Monitor networks, physical environment, and personnel activity.
2. **Analysis (DE.AE):** Use SIEM/SOAR to correlate logs, reduce noise, and integrate CTI.
3. **The Pivot Point (DE.AE-08):** Declare the incident. Apply strict criteria to adverse events to officially trigger the Response phase.



RESPOND (RS)

Managing the Chaos & Prioritizing Action.

High-Value Actions:

1. **Management (RS.MA):**
   Critical Rule: Incidents should not be handled on a first-come, first-served basis. Prioritize based on functional and information impact.

2. **Forensics (RS.AN):**
   Establish root cause and preserve chain of custody for evidence.

3. **Magnitude (RS.AN-08):**
   Estimate the scope. Is this a single endpoint or a systemic compromise?

Active Response: Mitigation & Communication

Zone 1: Mitigation (RS.MI)

Containment: Stop the expansion (e.g., isolate the VLAN).

Eradication: Remove the threat (e.g., delete malware, disable accounts).

Zone 2: Communication (RS.CO)

Internal: Update leadership and legal.

External: Notify regulators, law enforcement, and customers as required by law.

Information Sharing: Share TTPs with ISACs/peers (voluntary sharing increases collective immunity).

RECOVER (RC)

Restoring Operations & Verifying Integrity.

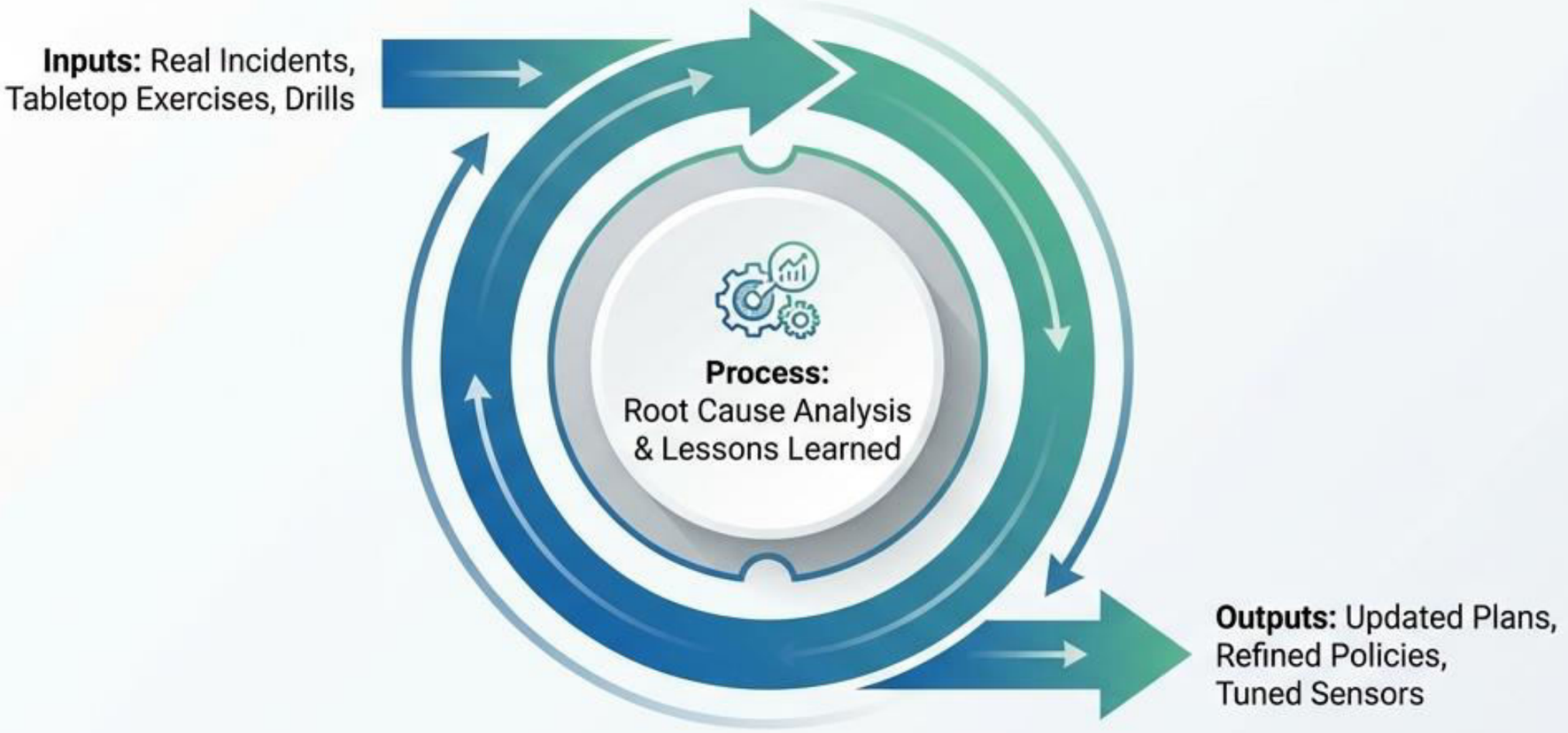
High-Value Actions:

1. **Plan Execution (RC.RP):**
   Prioritize restoration based on mission criticality.

2. **Integrity Check (RC.RP-03):**
   Do not restore the vulnerability. Verify backups are clean before reloading them.

3. **Validation (RC.RP-05):**
   Monitor restored assets closely. The attacker may still have a foothold.

The Engine of Resilience: Continuous Improvement



Philosophy: Improvement happens continuously, not just post-incident. (ID.IM-03)

The Executive Checklist

1. Integrate IR with ERM:
Move IR out of the technical silo and into Enterprise Risk Management.

2. Define Shared Responsibility:
Clearly document roles for MSSPs, Cloud Providers, and internal teams.

3. Prioritize by Impact:
Abandon 'first-come, first-served.' Triage based on mission criticality.

4. Operationalize CTI:
Don't just collect threat intel; use it to tune detection and risk models.

5. Test the Loop:
Regular tabletop exercises are non-negotiable for identifying improvements.

References & Resources

NIST SP 800-61r3

Full Text
(DOI link)

NIST CPRT

Cybersecurity & Privacy
Reference Tool
(Online mappings)

Project Page

NIST Incident Response
Project
(For updates)

Contact

800-61-comments@nist.gov

Based on NIST SP 800-61r3 (April 2025).


ISO/IEC 27035-1:2016
Principles of Information Security Incident Management
A Structured Approach to Building Organizational Resilience
ISO/IEC
JTC 1/SC 27
NotebookLM

Structural Resilience: ISO 27035

Ad-hoc Approach

- Chaos
- Hero-dependent
- Unrepeatable

TRANSFORMATION

ISO 27035 Approach

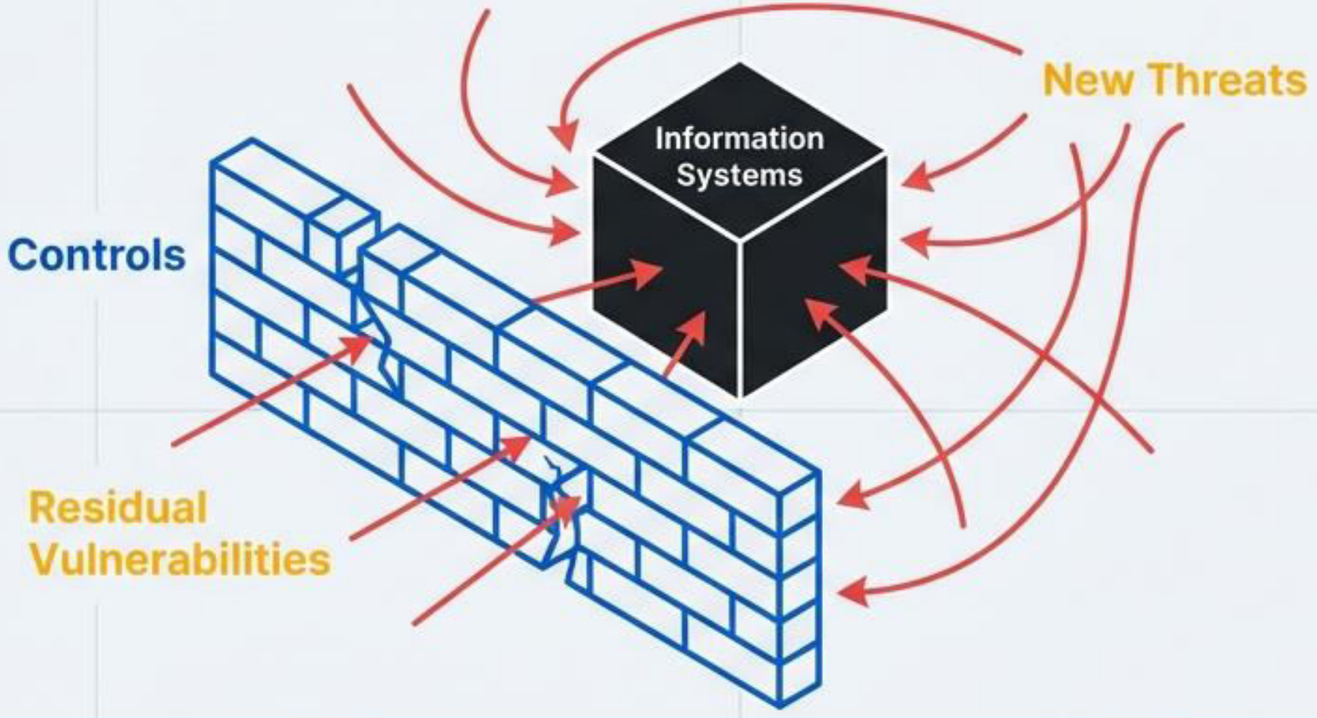
1. Preparation
2. Detection & Reporting
3. Assessment & Decision
4. Responses
5. Lessons Learned

- Documented
- Process-driven
- Auditable

The Architecture of Resilience. ISO 27035 provides the management container in which the NIST tactics operate, ensuring consistency across the organization.

Swiss International Tech

Policies Alone Cannot Guarantee Total Protection



The Reality

Even after controls are implemented, residual vulnerabilities remain.

The Risk

New instances of previously unidentified threats are inevitable.

The Consequence

Insufficient preparation increases the degree of potential adverse business impact.

A structured, planned approach is essential to detect, report, and recover from the inevitable.

Distinguishing the Event from the Incident

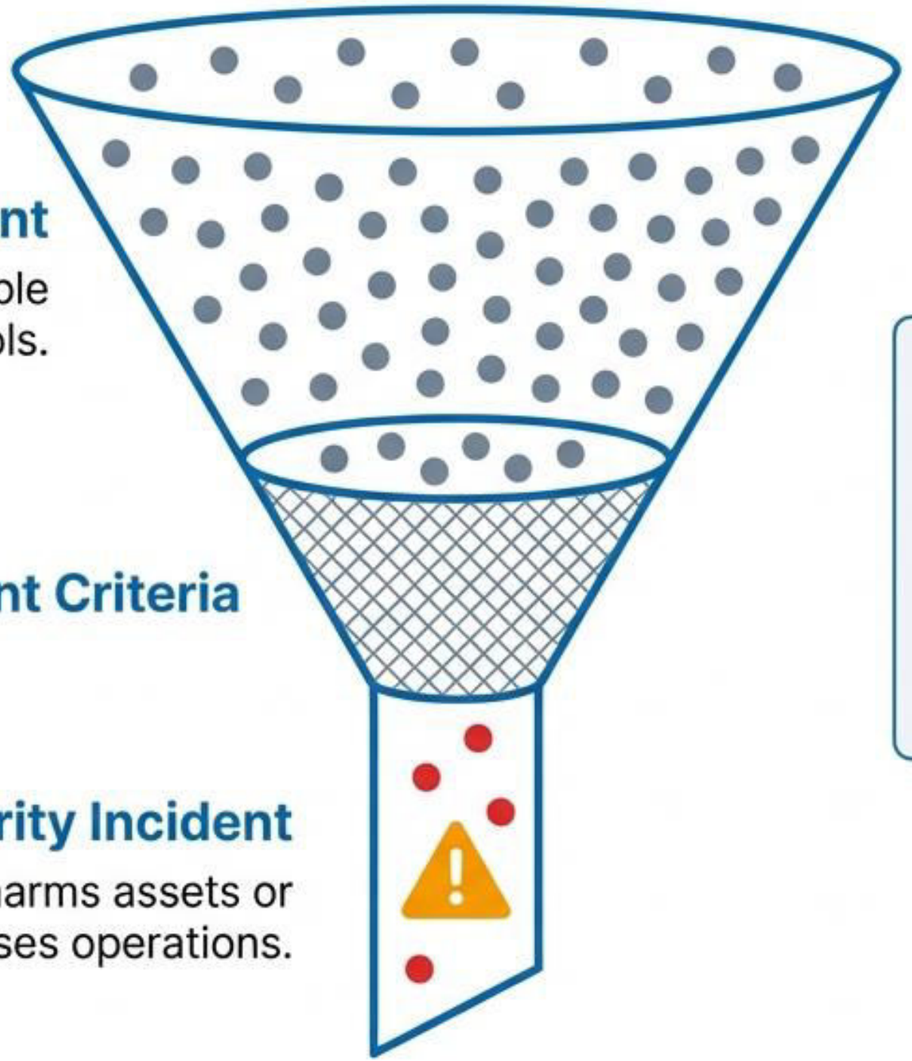
Information Security Event

Occurrence indicating a possible breach of security or failure of controls.

Assessment Criteria

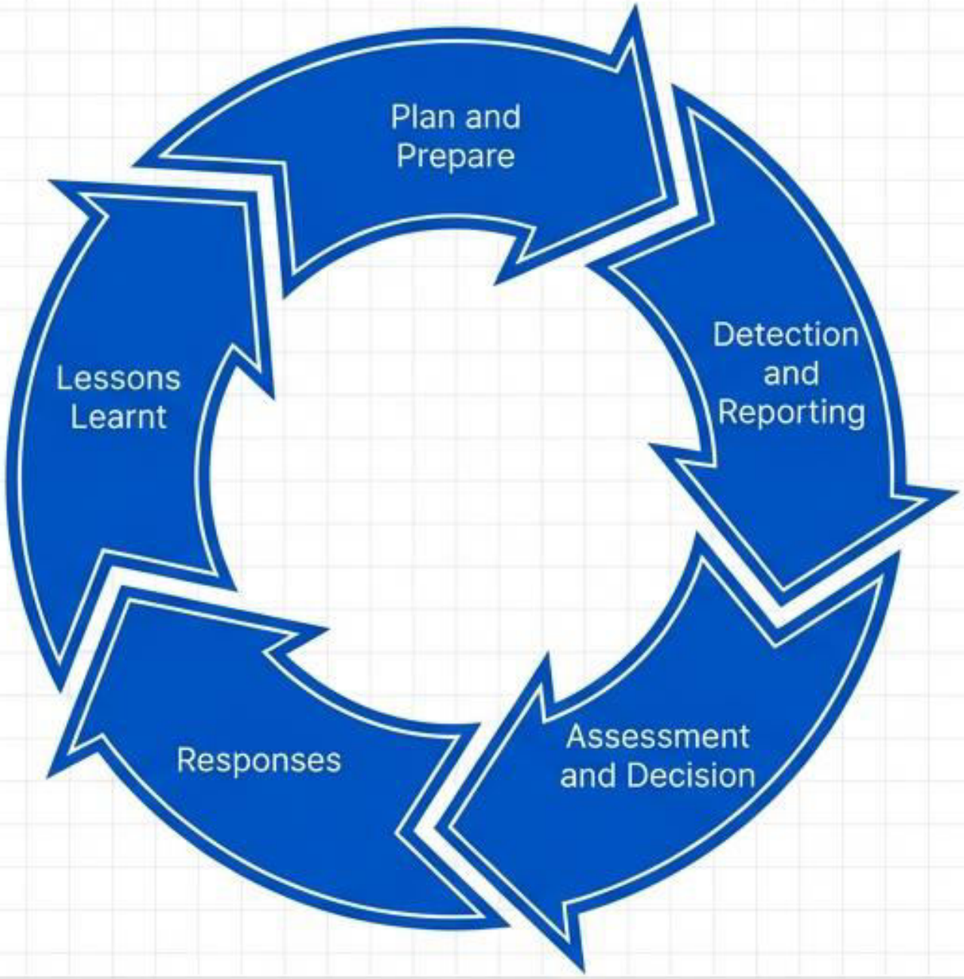
Information Security Incident

Confirmed event that harms assets or compromises operations.



Not all information security events are classified as information security incidents. An event indicates a indicates a possibility; an incident confirms harm.

The Five-Phase Management Model



ISO/IEC 27035-1 covers the principles of all five phases. Part 2 specifically provides guidelines for 'Plan and Prepare' and 'Lessons Learnt'.

Phase 1: Planning is the Foundation of Defense

Policy

Formulate information security incident management policy and gain top management commitment.

Team

Establish the Incident Response Team (IRT) with appropriate training.

Plan

Define and document the detailed management plan, including communication and information disclosure.

Testing

Test the plan through simulations to ensure readiness.

Phase 2: Detection and Data Collection

The objective is to capture data on occurrences (manual or automatic) before they are fully classified.

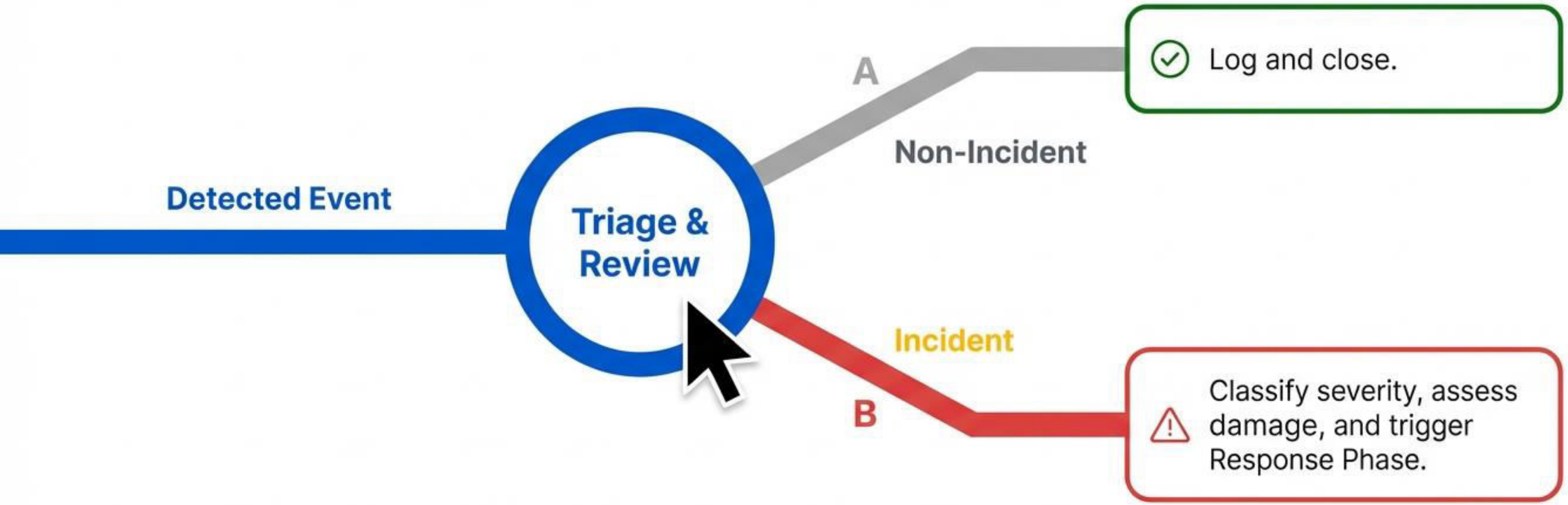
Monitor: Log system and network activity (local traffic, news feeds, attack trends).

Detect: Identify anomalies or control failures.

Collect: Gather evidence securely. Evidence preservation must be monitored for legal prosecution or disciplinary action (Refer to Annex A).

Report: Log all activities into the information security database to support future decisions.

Phase 3: The Assessment Pivot



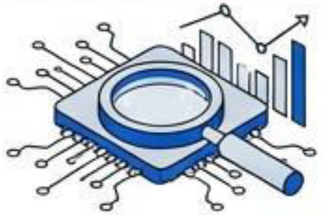
Requirement: All decisions must be thoroughly documented to maintain an audit trail.

Phases 4 & 5: Mitigation and Evolution

RESPONSE (The "Now")

- Activate controls to prevent, reduce, and recover from impacts.
- Protect and restore normal operational conditions.
- Link with Crisis Management and Business Continuity if necessary.

LESSONS LEARNT (The "Future")



- Analyze forensic data to identify patterns and trends.
- Institute preventive controls based on findings.
- Update the overall Information Security Incident Management policy.

The Information Security Event and Incident Flow

Information sharing and coordination with external IRTs helps resolve incidents crossing organizational boundaries.

Strategic Objectives of Incident Management

1.

Efficiency

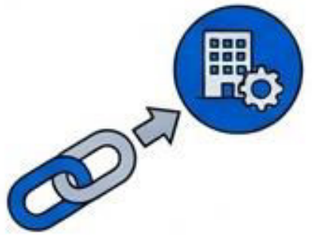
Detect and deal with events quickly.

2.

Mitigation

Minimize direct and indirect damage to operations.

3.



Linkage

Establish escalation paths to Crisis Management & Business Continuity.

4.

Prevention

Assess vulnerabilities to stop future attacks.

5.

Learning

Feedback mechanisms to improve overall security hygiene.

The Business Case for a Structured Approach

Financial

Reduce immediate financial loss and long-term damage to reputation and credibility.

Legal

Ensure evidence collection is sound and legally admissible for prosecution or disciplinary action.

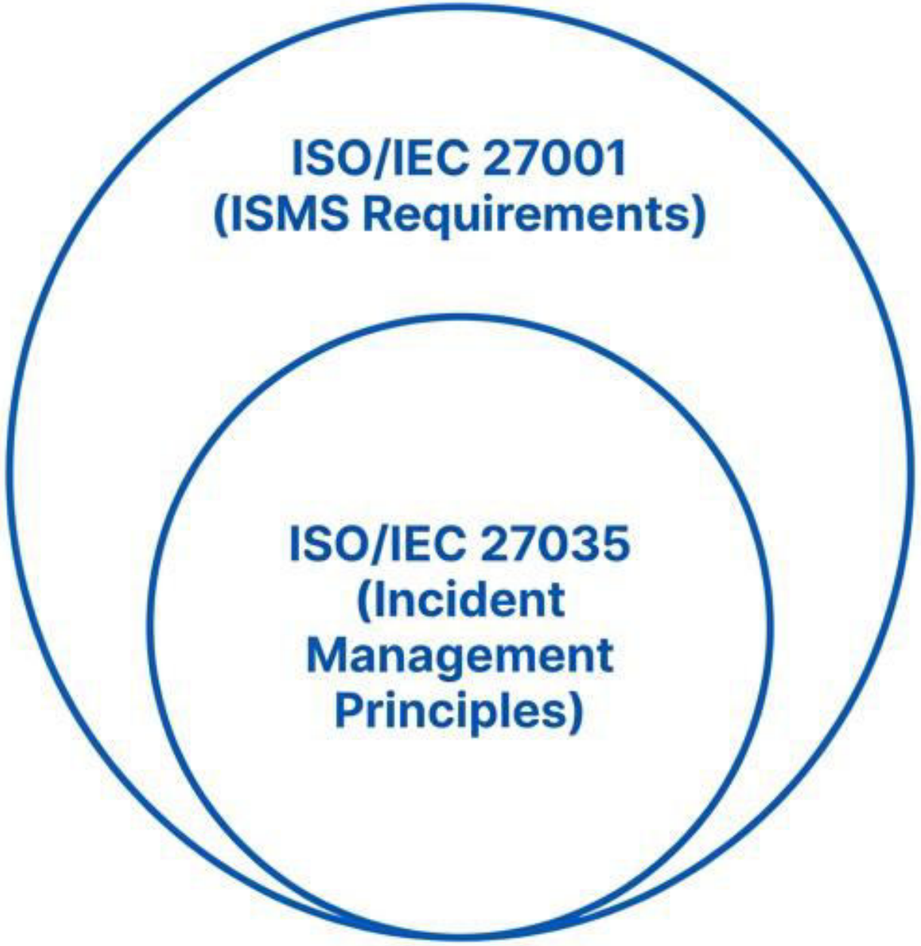
Strategic

Improve risk assessment data and justify budget/resource allocation.

Operational

Strengthen focus on prevention by identifying new threat patterns and prioritizing resources.

Supporting the ISO/IEC 27001 ISMS



ISO/IEC 27035 provides the guidance necessary to meet the specific incident management requirements found in ISO/IEC 27001 (supported by ISO/IEC 27002).

See Annex C for a cross-reference table of 27001 clauses to 27035.

Adaptability and Proportionality

The complexity of the implementation should be proportional to the organization's needs.

“Adopt guidance in a manner that is relevant to the scale and characteristics of the business.”

Operational Readiness Checklist

- [ ] Do we have a designated Incident Response Team (IRT)?
- [ ] Is the distinction between ‘Event’ and ‘Incident’ clearly defined in our policy?
- [ ] Are we logging detections centrally in an information security database?
- [ ] Is there a formal process to escalate incidents to Crisis Management?
- [ ] Do we have a feedback loop to update policies based on lessons learnt?

ISO/IEC 27035-1:2016

Principles of Incident Management

For specific guidelines on the 'Plan and Prepare' and 'Lessons Learnt' phases, refer to ISO/IEC 27035-2.


READY FOR IMPACT
BUILDING A RESILIENT INCIDENT RESPONSE CAPABILITY
GUIDANCE BASED ON ISO/IEC 27035-2:2016
READING DECK FOR IT LEADERS & SECURITY ARCHITECTS
NotebookLM

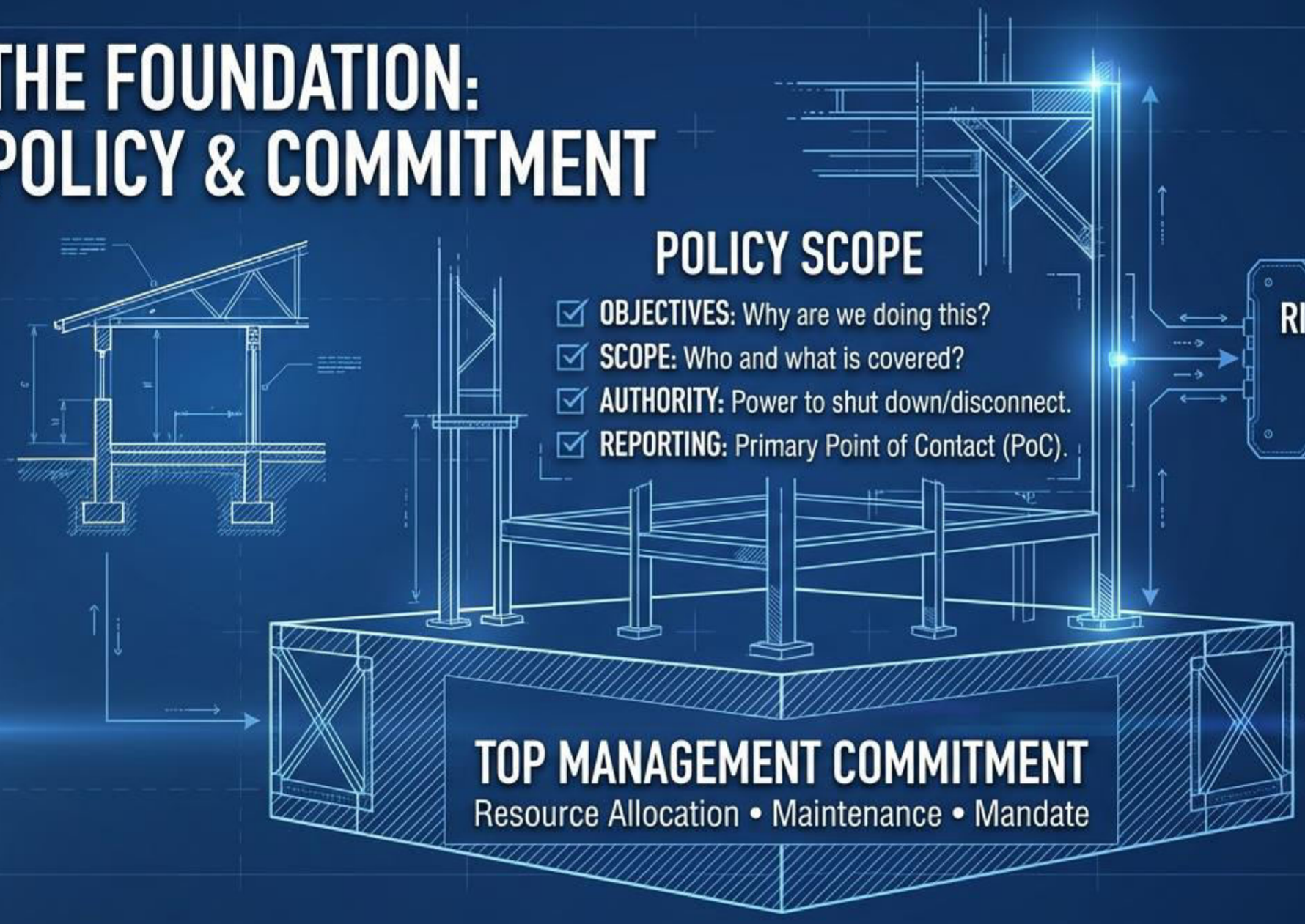
THE ASSUMPTION

THE REALITY

There can be a large gap between an organization's plan for an incident and an organization knowing it is prepared.

CRITICAL SUCCESS FACTOR: INCIDENT MANAGEMENT IS A CSF FOR INFOSEC (ISO/IEC 27000).

THE FOUNDATION: POLICY & COMMITMENT



POLICY SCOPE

- ☑ **OBJECTIVES:** Why are we doing this?
- ☑ **SCOPE:** Who and what is covered?
- ☑ **AUTHORITY:** Power to shut down/disconnect.
- ☑ **REPORTING:** Primary Point of Contact (PoC).

RISK MANAGEMENT INTEGRATION (Clause 5)

TOP MANAGEMENT COMMITMENT

Resource Allocation • Maintenance • Mandate

ENGINEERING SPEC 1.0

BLUEPRINTING THE PLAN

KEY DISTINCTION:
EVENT (Occurrence) vs.
INCIDENT (Adverse Impact)

CONSENSUS: Where policy is silent, the plan must be built on stakeholder consensus to ensure effective operation (Clause 6.2).

STRUCTURING CHAOS: CLASSIFICATION & SCALE

CLASS IV (Very Serious):
Business paralysis, national security threat.

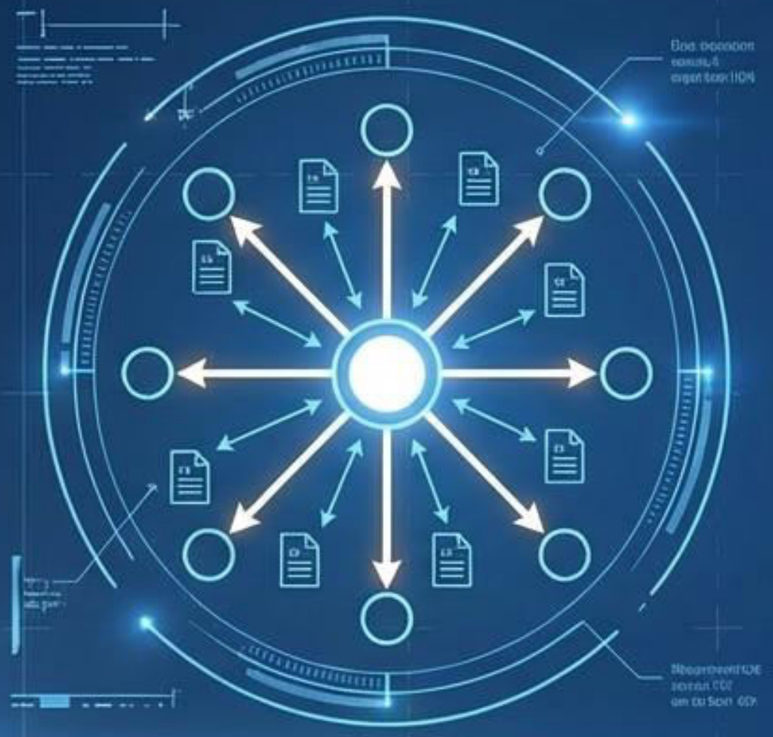
CLASS III (Serious):
Important system affected, serious loss.

CLASS II (Less Serious):
Considerable loss, limited social impact.

CLASS I (Small):
Minor loss, recording only.

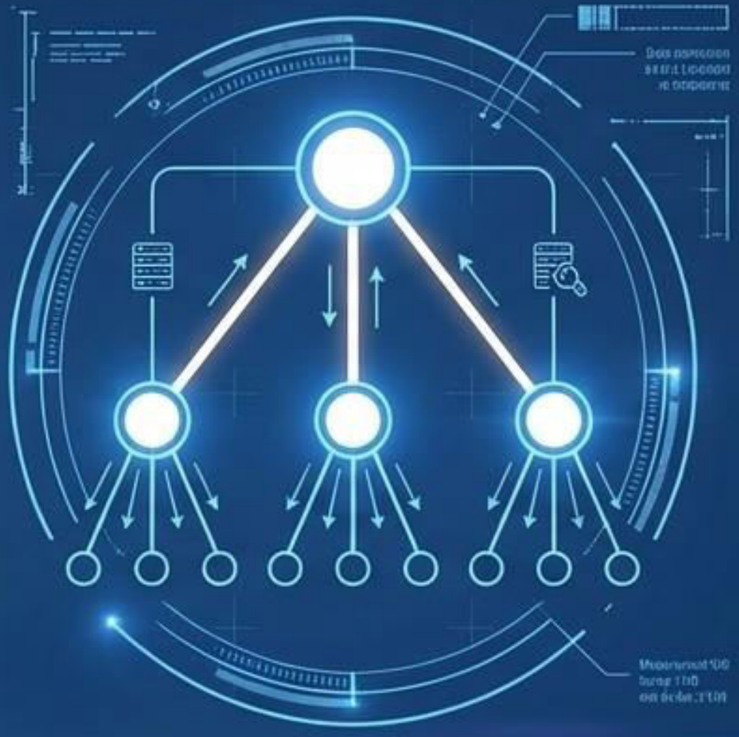
IMPACT FACTOR

ASSEMBLING THE DEFENDERS: IRT MODELS



SINGLE MODEL

Centralized operations for one organization.



HIERARCHICAL MODEL

Central coordination of sector IRTs.

REMOTE MODEL

Outsourced security enterprise.

THE CONSTITUENCY: The specific group, IP range, or domain the IRT is responsible for protecting (Clause 7.2).

THE HUMAN ELEMENT: ROLES & COMPETENCIES

IRT MANAGER
Strategy, leadership, reporting to top management.

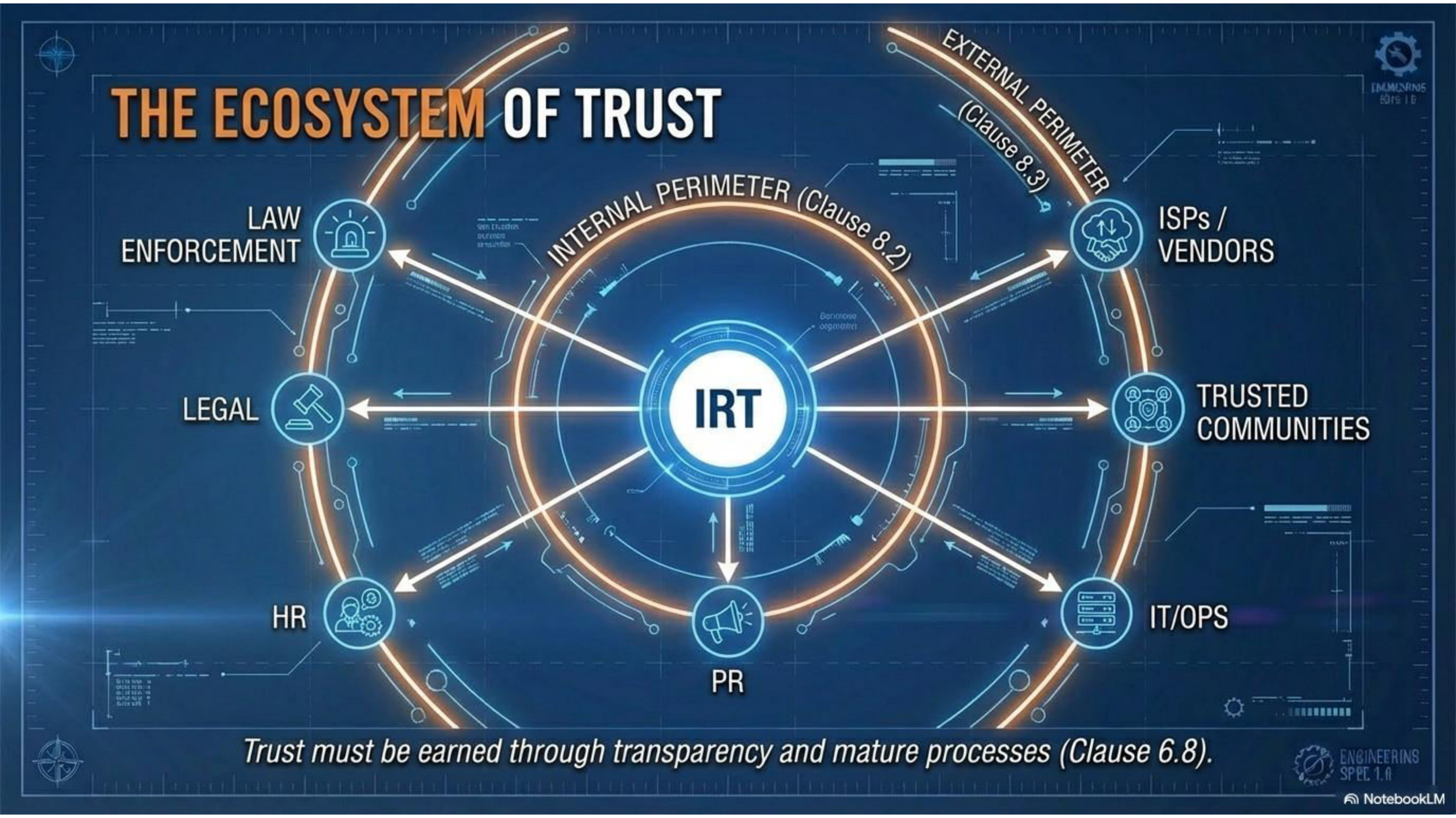
INCIDENT HANDLERS
Triage, analysis, tracking, response coordination.

VULNERABILITY HANDLERS
Patching, research, testing fixes.

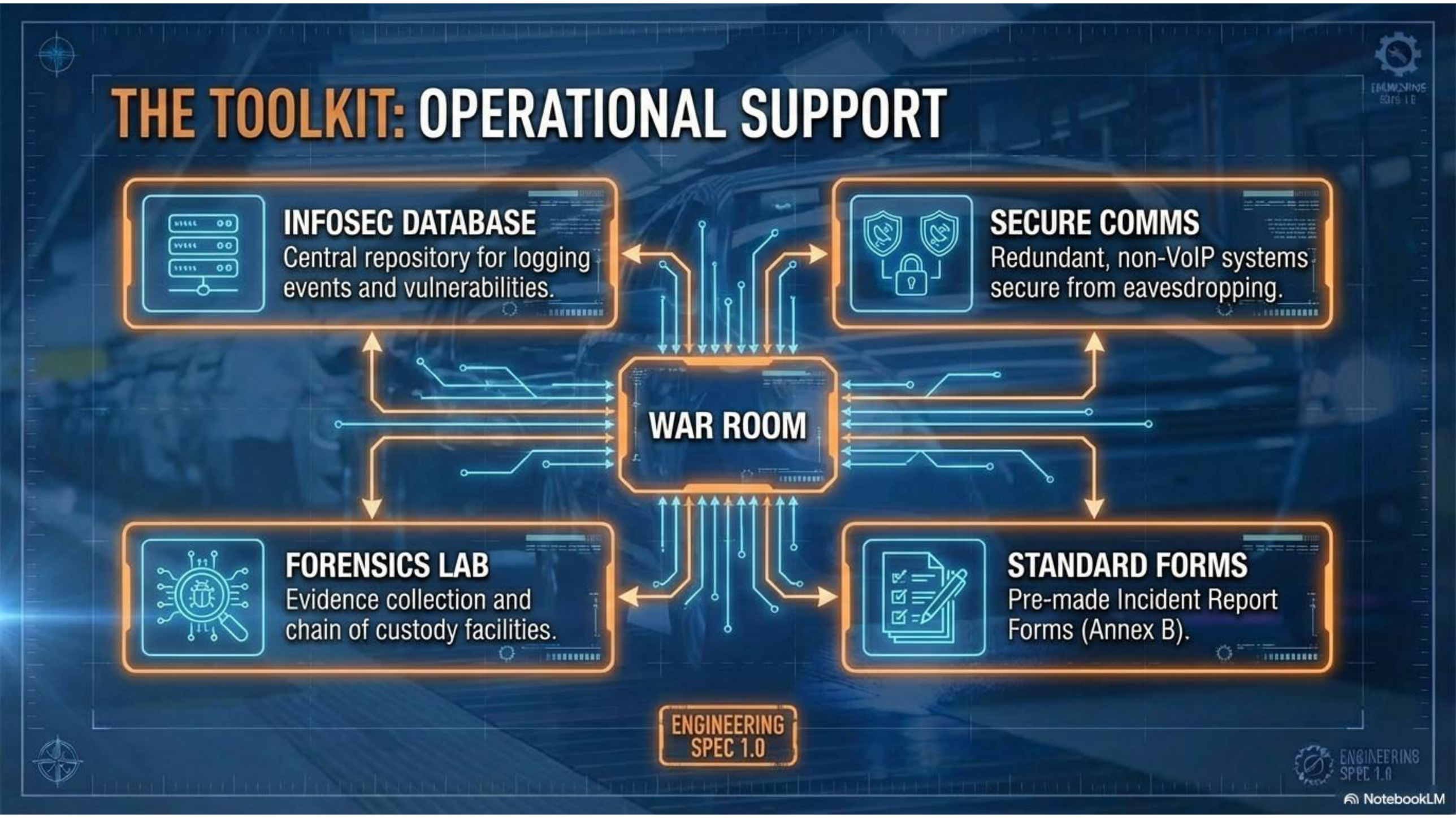
FORENSICS / ANALYSIS
Deep dive investigation, evidence preservation.

TECHNICAL SKILLS
(Logs, Crypto)

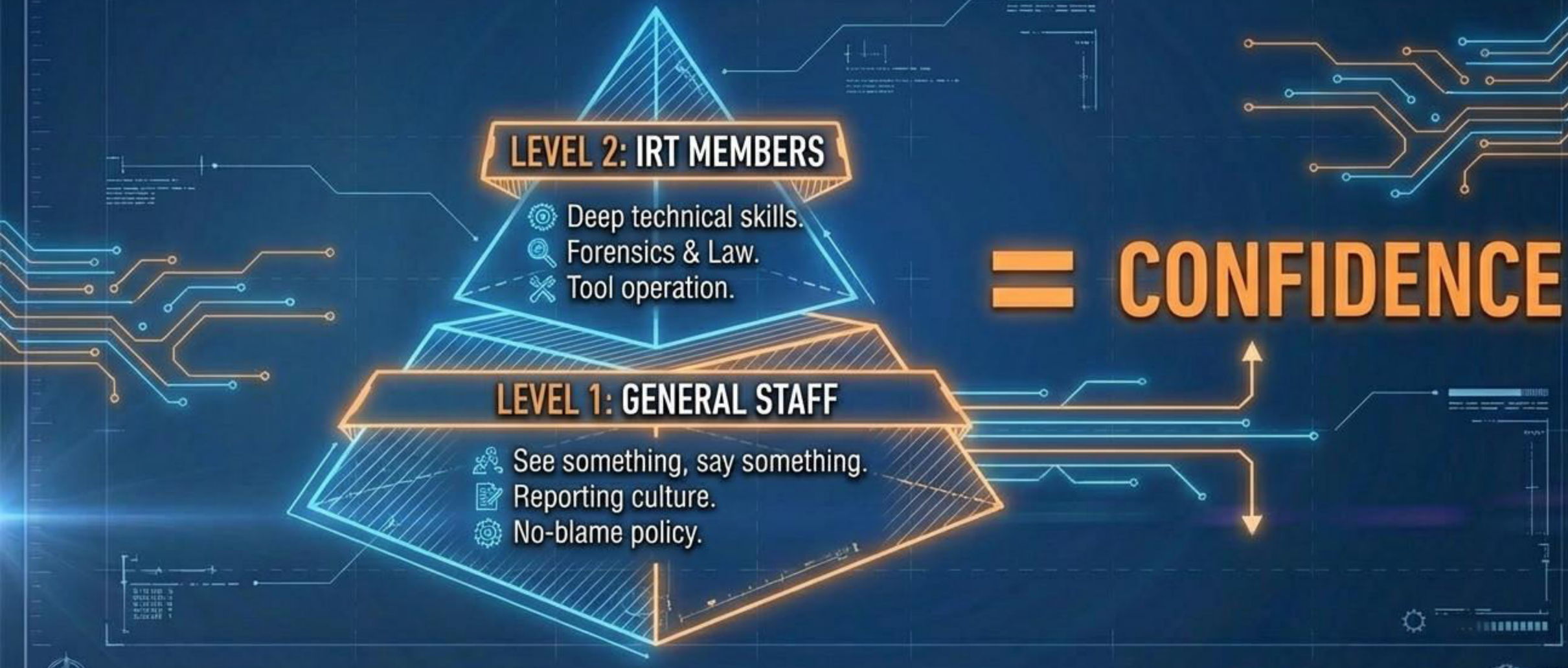
PERSONAL SKILLS
(Communication, Resilience)


THE ECOSYSTEM OF TRUST
EXTERNAL PERIMETER (Clause 8.3)
INTERNAL PERIMETER (Clause 8.2)
IRT
LAW ENFORCEMENT
ISPs / VENDORS
LEGAL
TRUSTED COMMUNITIES
HR
PR
IT/OPS
Trust must be earned through transparency and mature processes (Clause 6.8).

THE TOOLKIT: OPERATIONAL SUPPORT



THE HUMAN FIREWALL: AWARENESS & TRAINING



= CONFIDENCE

STRESS TESTING: VALIDATION & EXERCISES

TABLETOP EXERCISES

Discussion-based walkthroughs.
Focus on decision making.

LIVE SIMULATIONS

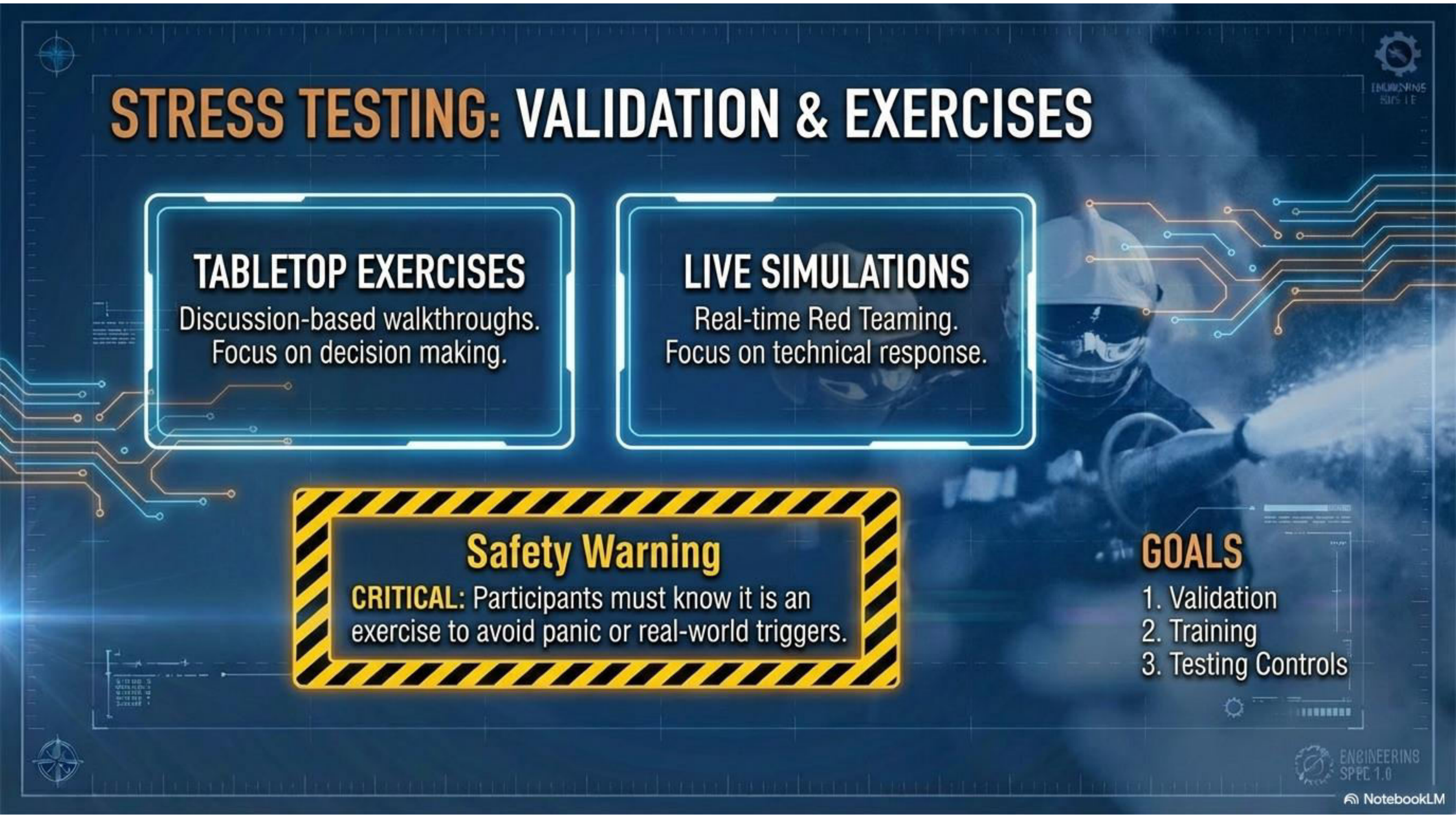
Real-time Red Teaming.
Focus on technical response.

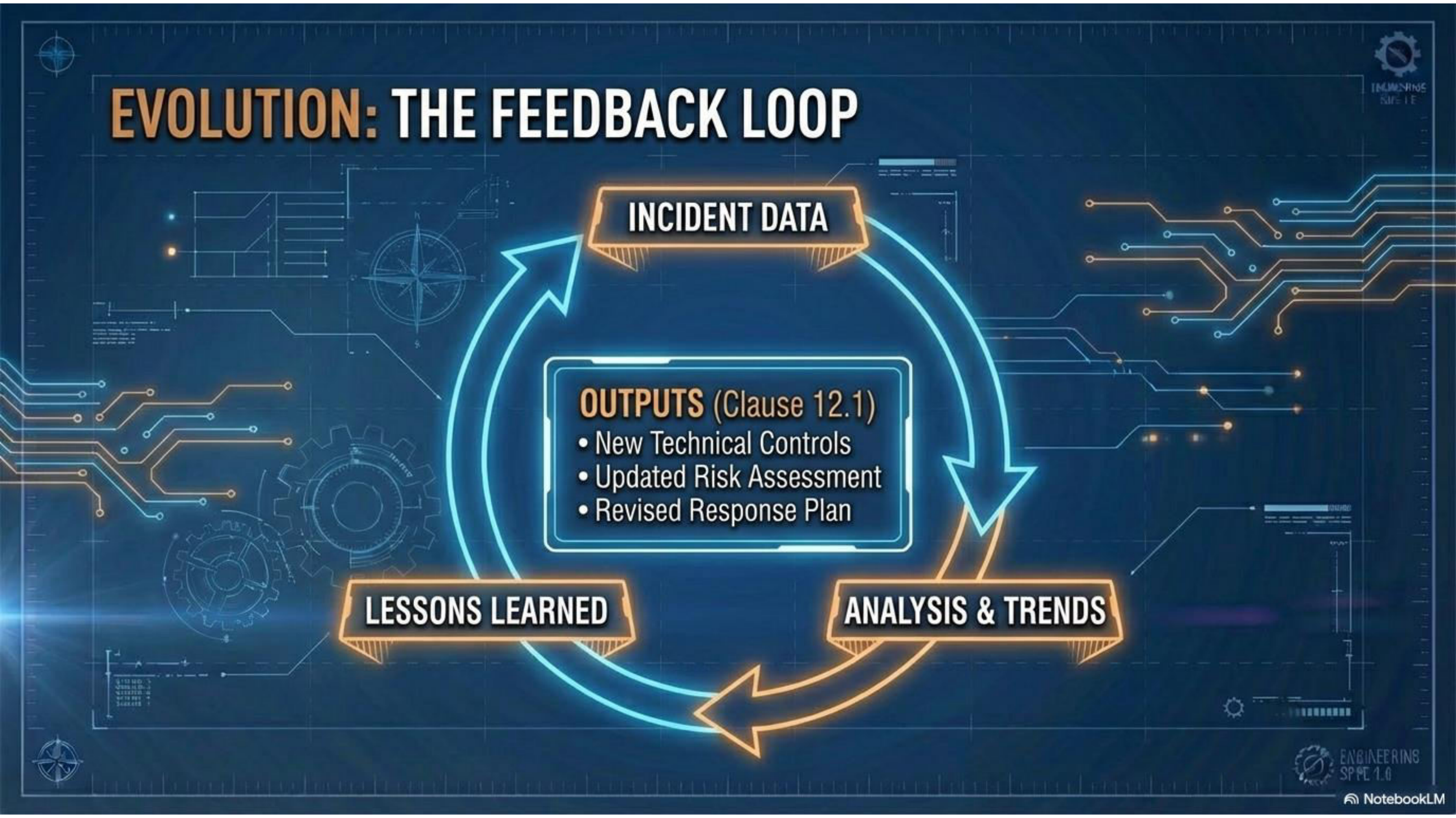
Safety Warning

CRITICAL: Participants must know it is an exercise to avoid panic or real-world triggers.

GOALS

1. Validation
2. Training
3. Testing Controls




EVOLUTION: THE FEEDBACK LOOP
INCIDENT DATA
OUTPUTS (Clause 12.1)
• New Technical Controls
• Updated Risk Assessment
• Revised Response Plan
ANALYSIS & TRENDS
LESSONS LEARNED
NotebookLM

THE SAFETY NET: LEGAL & REGULATORY

PRIVACY

Protection of personal data (GDPR) during investigation.

CHAIN OF CUSTODY

Ensuring evidence is admissible and identical to original.

LIABILITY

Checking validity of disclaimers and external contracts.

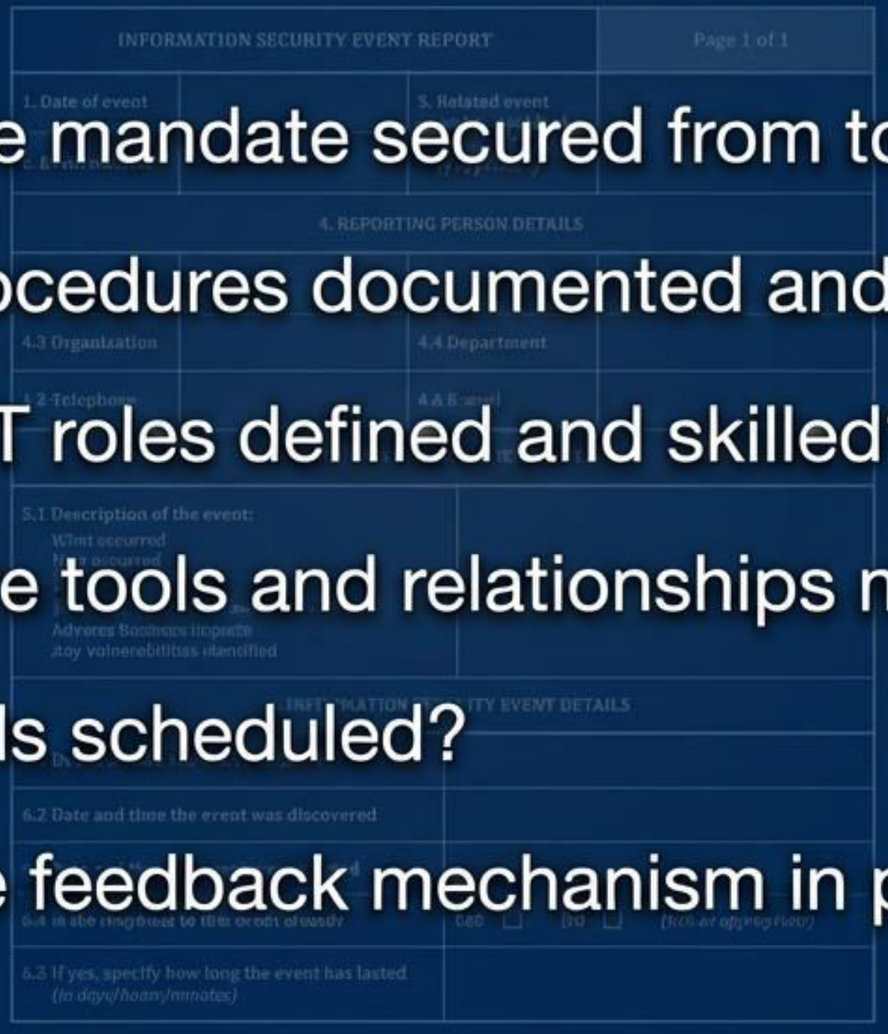
NON-DISCLOSURE

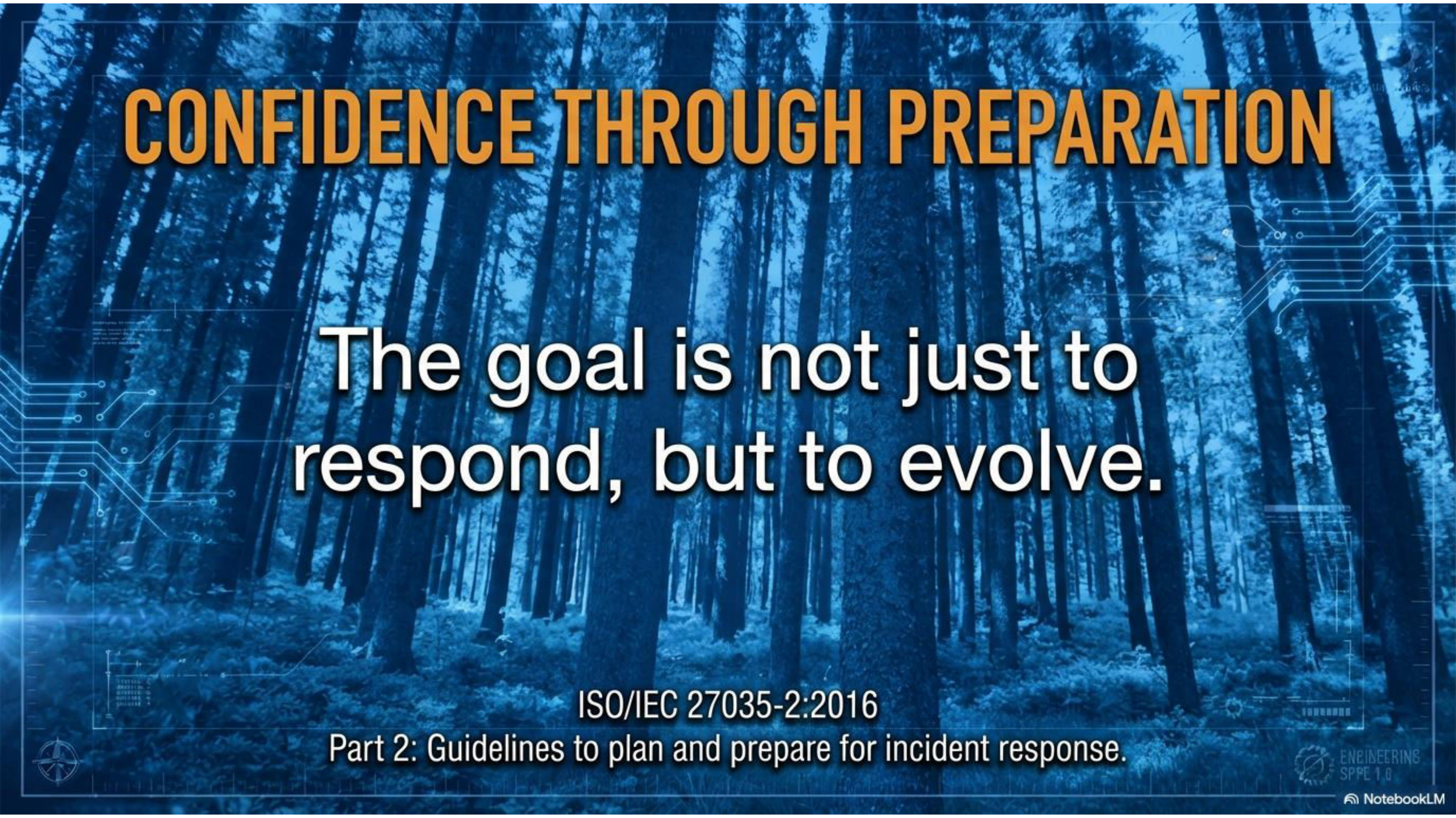
Enforcing NDAs for staff and vendors.

Source: Aelvetica Now Regular

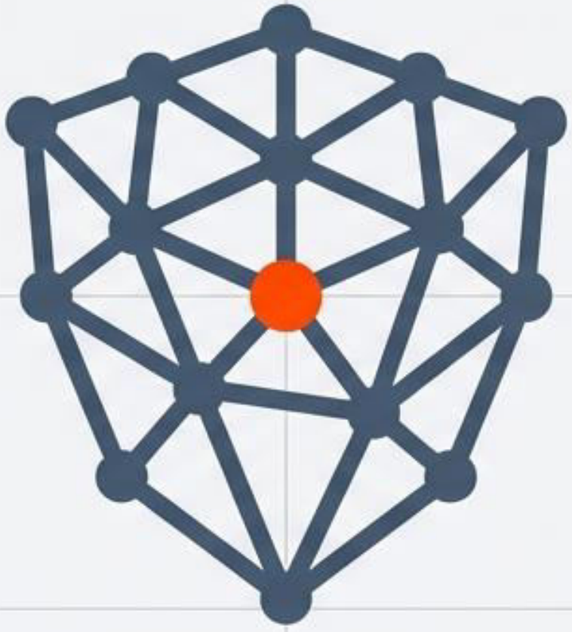
READINESS CHECKLIST

- [ ] **POLICY:** Is the mandate secured from top management?
- [ ] **PLAN:** Are procedures documented and consensus built?
- [ ] **TEAM:** Are IRT roles defined and skilled?
- [ ] **SUPPORT:** Are tools and relationships mapped?
- [ ] **TEST:** Are drills scheduled?
- [ ] **LEARN:** Is the feedback mechanism in place?




CONFIDENCE THROUGH PREPARATION
The goal is not just to respond, but to evolve.
ISO/IEC 27035-2:2016
Part 2: Guidelines to plan and prepare for incident response.
ENGINEERING SPRE 1.0
NotebookLM

ISO/IEC 27035-3



Guidelines for ICT Incident Response Operations

The Operational Field Guide to Incident Lifecycle Management

1. Detect
2. Notify
3. Triage
4. Analyze
5. Respond
6. Report

From Policy to Practice

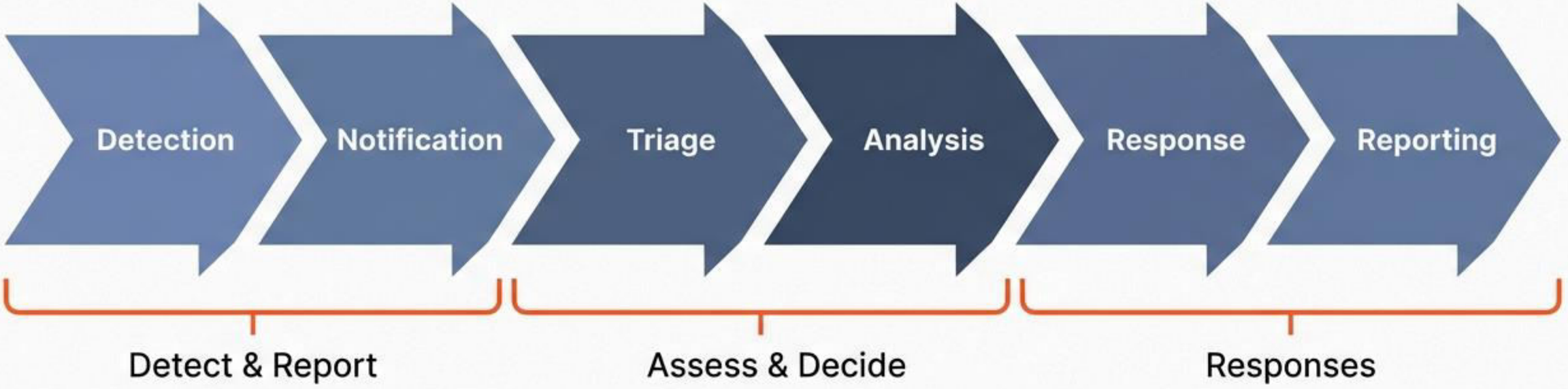
This document functions as the “Runbook” for the Computer Security Incident Response Team (CSIRT), focusing strictly on ICT-related execution.

KEY DISTINCTIONS

- **FOCUS:** ICT-related incidents only.
- **EXCLUDES:** Non-ICT events (paper/ physical security).
- **GOAL:** Identification, Containment, Eradication, Recovery.

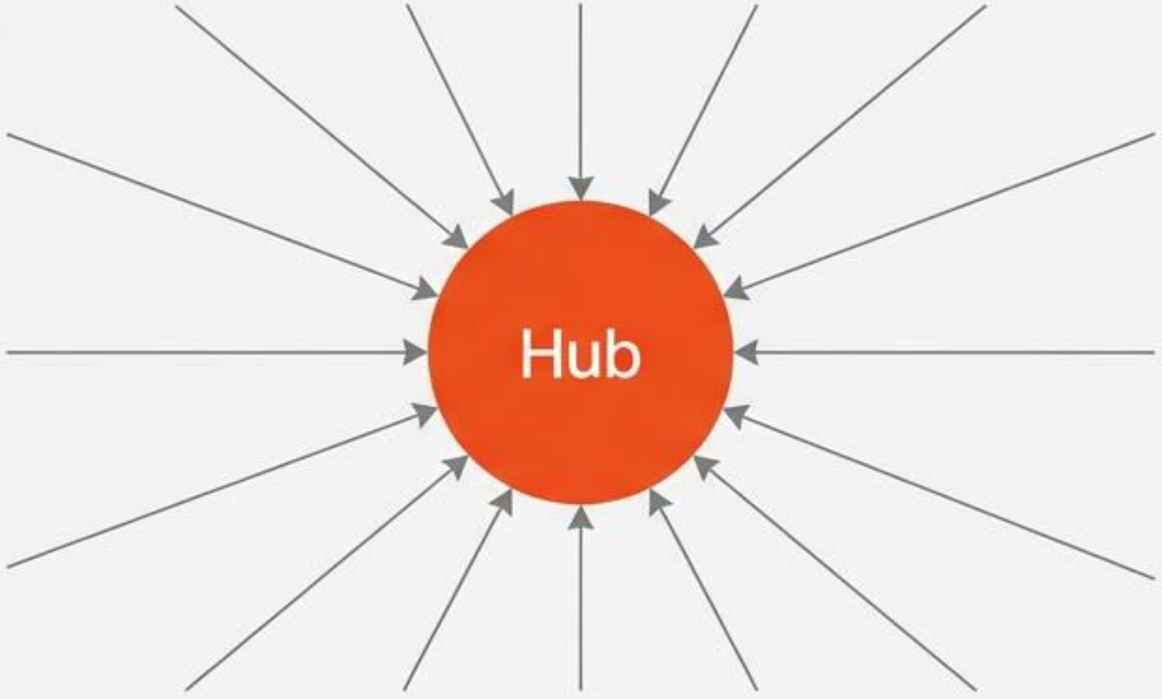
The Incident Lifecycle

A linear progression from chaos to order



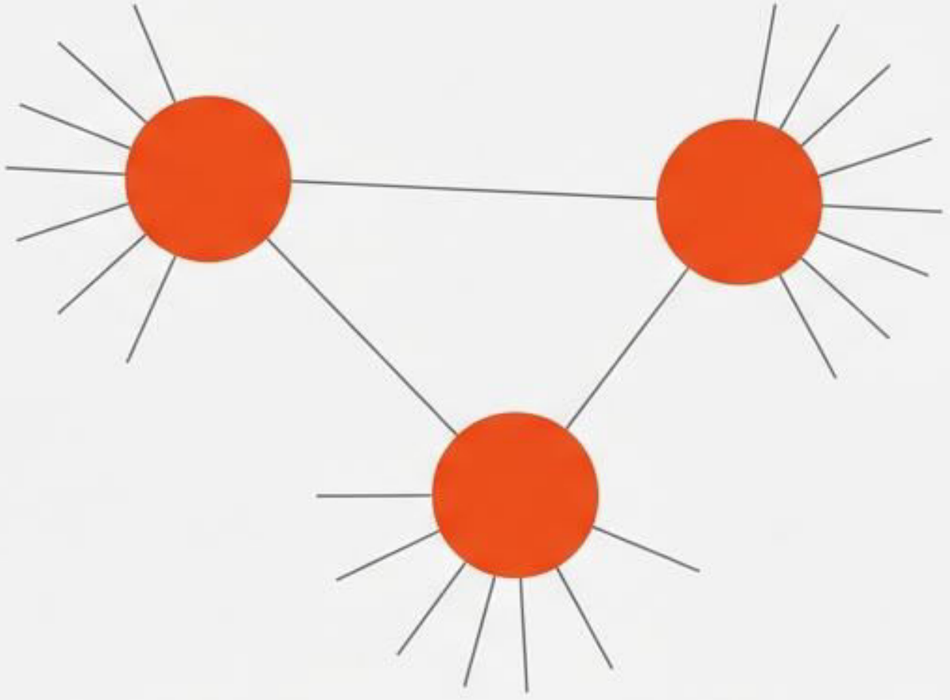
Pre-Requisite: Point of Contact (PoC)

Single PoC Structure



PROS: Centralized control, High availability.
REQ: Must filter Health & Safety / Non-ICT events.

Multiple PoC Structure



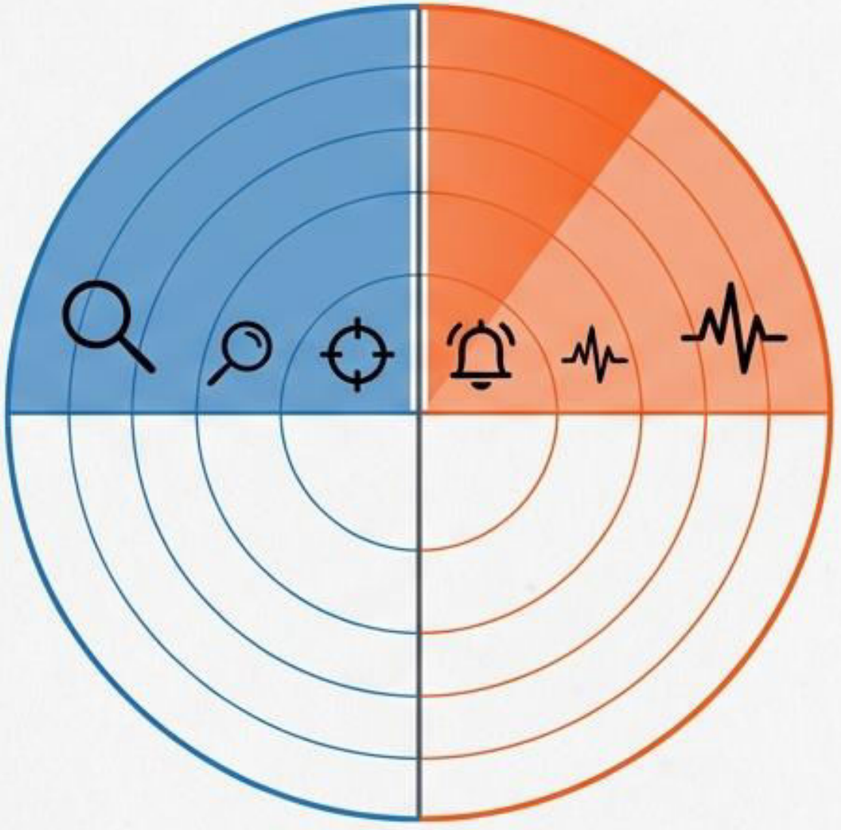
PROS: Specialized handling (Geo/Unit based).
RISKS: Information silos, misrouting.

CRITICAL SUCCESS FACTOR: The PoC must possess the skills to distinguish a generic 'Event' from an 'Incident'.

Phase 1: Detection Operations

PROACTIVE
(The Hunt)

- Vulnerability Scanning
- Penetration Testing
- Threat Intel Feeds
- Log Correlation



REACTIVE
(The Signal)

- IDS/IPS Alerts
- User Reports
- Help Desk Tickets
- Anti-Virus Notifications

"Detection is important because it starts the incident response operations."

DETECTION	NOTIFICATION	TRIAGE	ANALYSIS	RESPONSE	REPORTING

Phase 2: Notification

Critical Intake Data

Indicators of Compromise (IoC)
(Subtext: IP Addresses, URLs)

Integrity Data
MD5: e5d... != a2f...

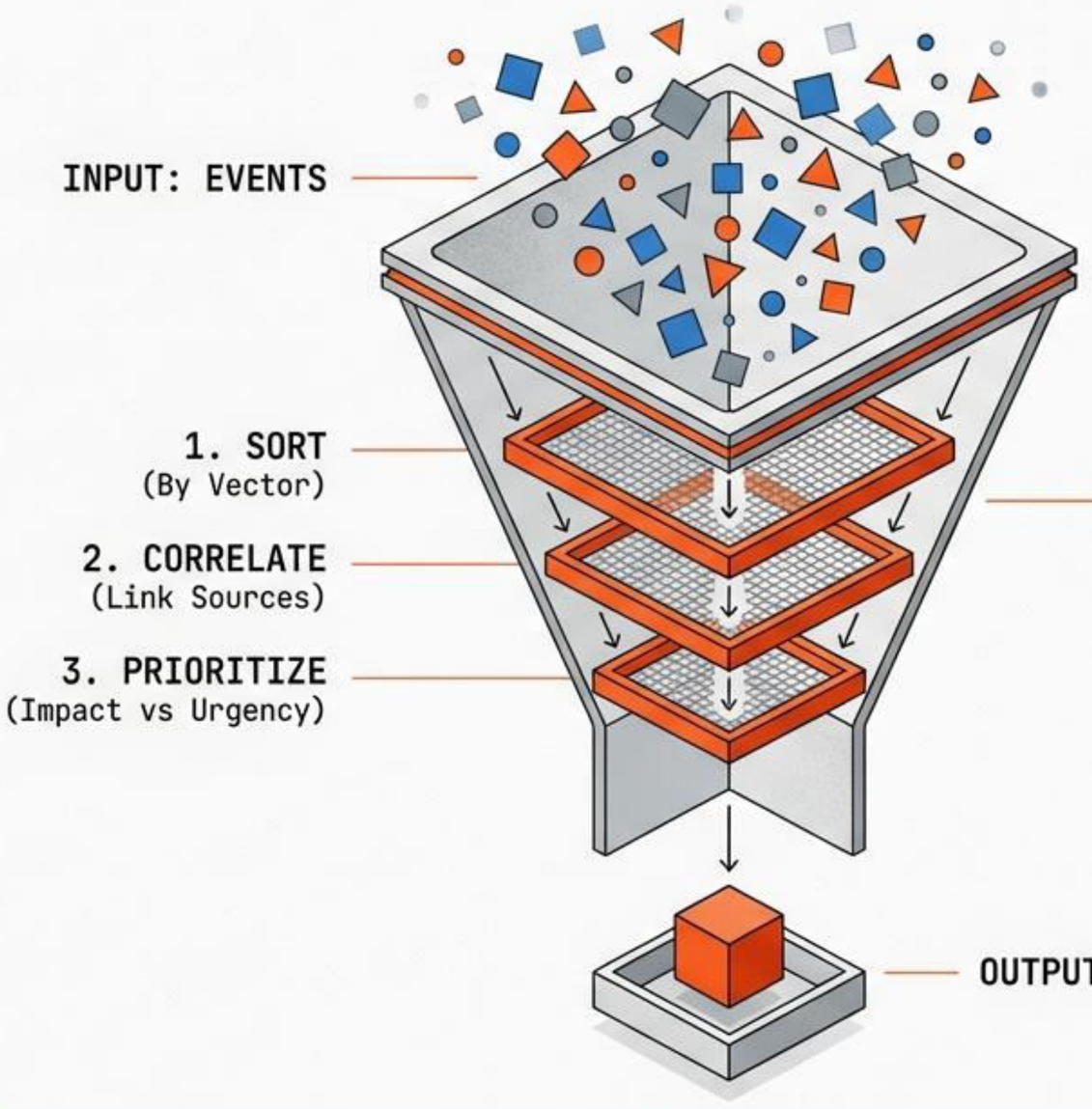
Context
(Subtext: Time, Systems, Attack Vector)

Digital Incident Ticket

```
{
  "TIME": "14:02 UTC",
  "VECTOR": "Suspicious Email",
  "AFFECTED SYSTEM": "Finance-Svr-01"
}
```

Methods: Dedicated CSIRT Email, Hotline, or Helpdesk.

Phase 3: Triage Operations

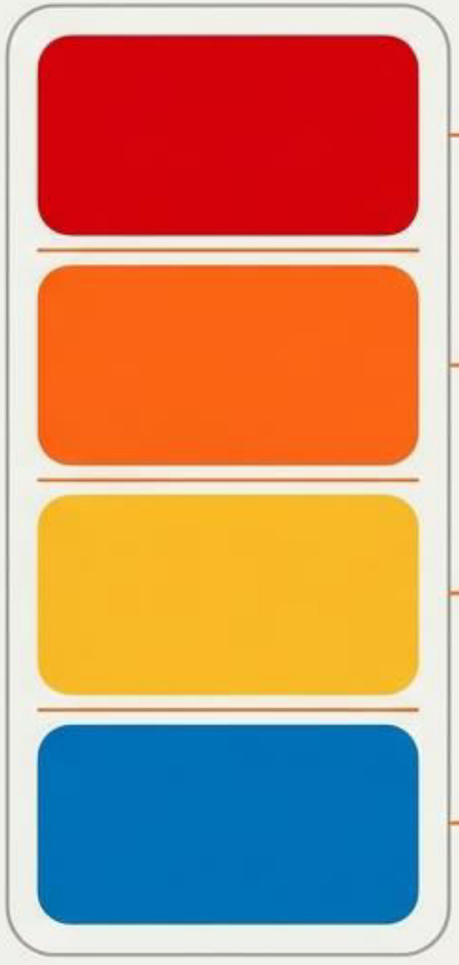


Decision Criteria

Priority Hierarchy:

- 1. Human Life Safety
- 2. Infrastructure Integrity
- 3. Financial Loss
- 4. Reputational Impact

Criteria for Classification (Annex A)



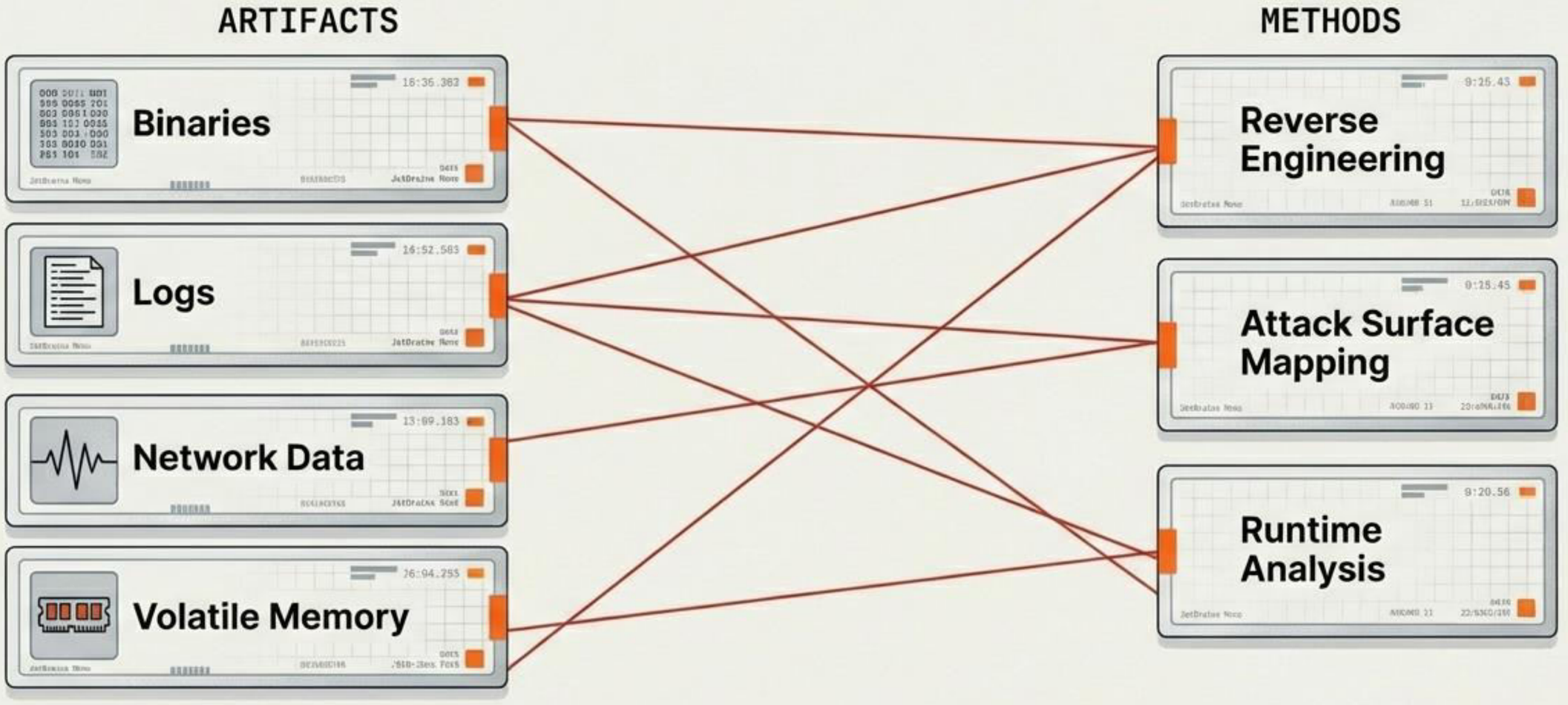
LEVEL 1: SERIOUS
Spread over entire country, fatal financial loss, core services stopped.

LEVEL 2: ALERT
Impacting numerous organizations, spreading externally.

LEVEL 3: CAUTIOUS
Impacting internal systems, increased vulnerability.

LEVEL 4: CONCERNED
Hacking trials, new worms released, potential damage.

Phase 4: Analysis Operations



DETECTION	NOTIFICATION	TRIAGE	ANALYSIS	RESPONSE	REPORTING

CSIRT RUNBOOK STATUS: ● ACTIVE (Orange Dot) | VERSION: 1.0 | DATE: 2024.01.01

Deep Dive: Scope of Analysis

Tactical Modernism

Paper White

INTRA-INCIDENT (Micro)

What is happening NOW?

Focus: Resolution of the specific ticket.
Data: Local traces, system logs, code.

INTER-INCIDENT (Macro)

How does this relate to OTHERS?

Focus: Strategic Intelligence.
Data: Identifying APTs, Time chains, Modus Operandi.

DETECTION	NOTIFICATION	TRIAGE	ANALYSIS	RESPONSE	REPORTING

Phase 5: Response - Containment

Tactical Modernism

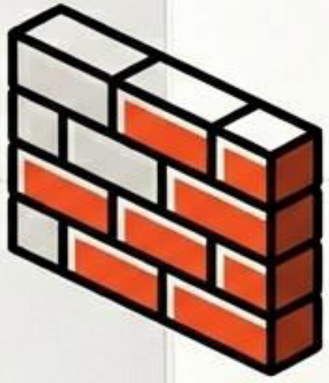
Paper White

ISOLATION

Action: Remove host from network.

Risk: Alerting adversary, losing live connection data.

BLOCKING



Action: Firewall/Port blocks, URL filtering.

Benefit: Stops specific vectors.

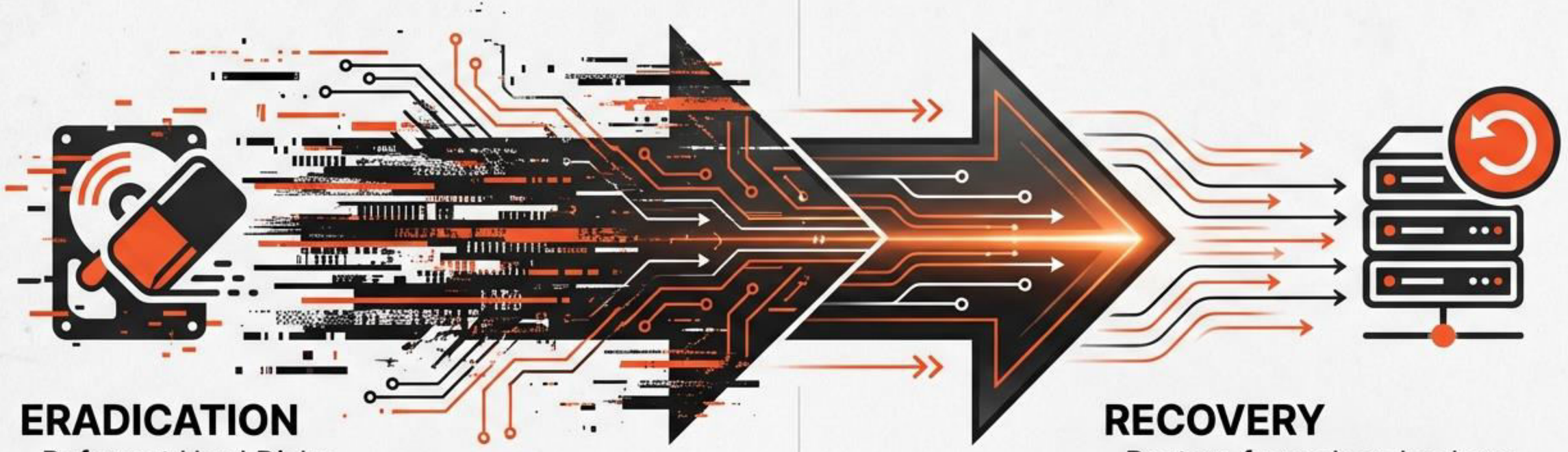
SHUTDOWN

Action: Power down hardware.

WARNING: **Destroys volatile evidence (RAM). Requires business owner approval.**

DETECTION	NOTIFICATION	TRIAGE	ANALYSIS	RESPONSE	REPORTING

Phase 5: Eradication & Recovery



ERADICATION

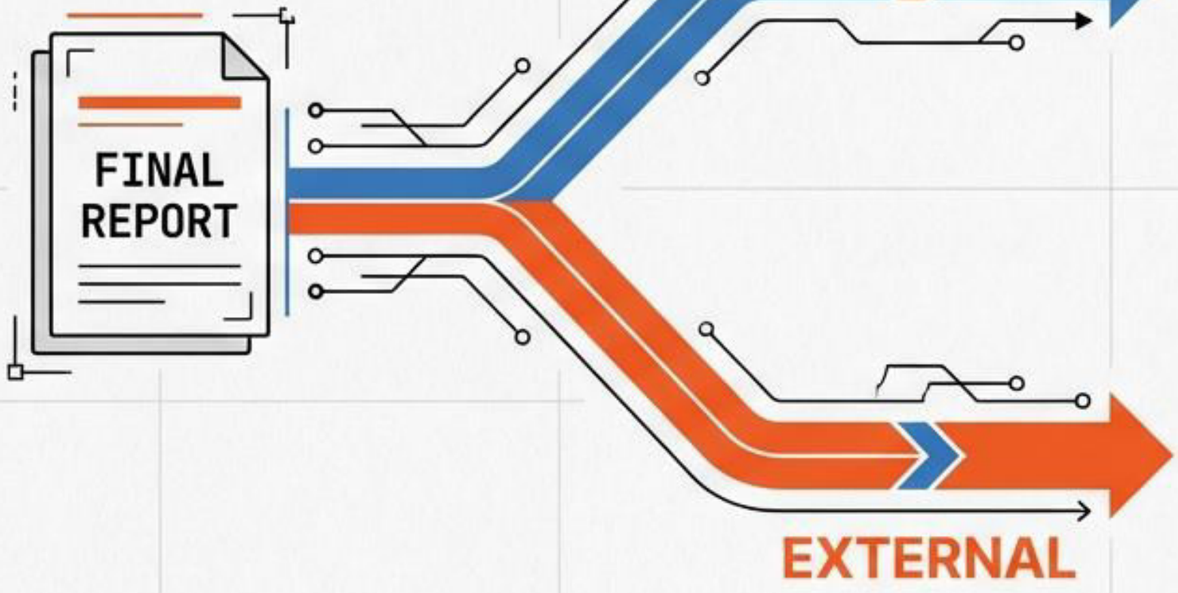
- Reformat Hard Disks
- Media Wiping
- Firmware Flashing

Note: Preserve evidence for legal first!

RECOVERY

- Restore from clean backups
- Patch Vulnerabilities
- Reset Credentials
- Activate Warm/Hot Recovery Sites

Phase 6: Reporting Operations



TARGET: CISO, Legal, Management

- Root Cause
- Impact Analysis
- Lessons Learnt

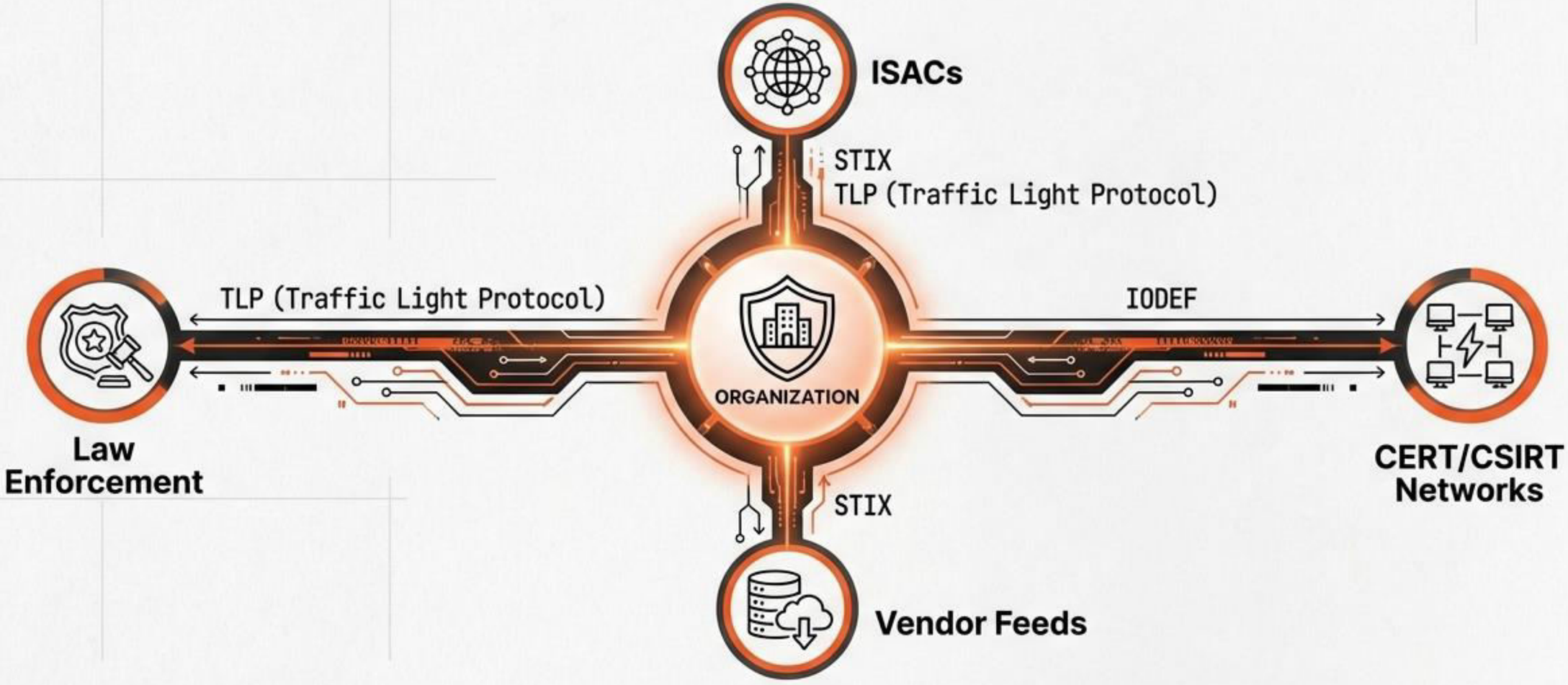
GOAL: Process Improvement

TARGET: Customers, Authorities (GDPR), Law Enforcement, Media

- Regulatory Notifications
- Public Statements

NOTE: Requires Legal/Comms Officer approval

Information Sharing



Sharing Indicators of Compromise (IoC) strengthens collective defense.

Operational Checklist

FLIGHT CHECK

- ☐ **DETECT:** Is PoC distinguishing Events from Incidents?
- ☐ **TRIAGE:** Are filters based on Impact and Urgency?
- ☐ **ANALYZE:** Is evidence preserved (Chain of Custody)?
- ☐ **RESPOND:** Does containment balance damage vs. evidence?
- ☐ **REPORT:** Is knowledge fed back into the Plan?

Incident response is not just technology; it is a business process for survival.

DETECTION | NOTIFICATION | TRIAGE | ANALYSIS | RESPONSE | **REPORTING**

Vulnerability handling
30.03.2026, 14:00-16:00 CET

Designing the process and demonstrating the OSCRAT workflow for vulnerability scanning, identification, registration, tracking, and reporting.

How SBOM works in practice as a key part of the vulnerability handling chain

How to build your product’s SBOM and keep it usable as part of technical documentation and supply-chain transparency.

Thank you!

Miroslav Mitev, PhD
+359 896 198 875
phdmitev@gmail.com