

Reza Adineh
MINIMAL CYBER UTIOM.DE

UTIOM Framework

Unified Threat-Informed Operations Model Book

Think smarter. Stay secure.

Version 1.2 · Released August 2026

UTIOM Framework Book
 Unified Threat-Informed Operations Model
 By: Reza Adineh

Author	Version & Date of release	Description
Reza Adineh	Public release · August 2025	UTIOM published publicly for the first time: lifecycle, three pillars, seven laws and incident response as the operating mode of security operations.
	V1.0 · February 2026	First edition of the framework book: lifecycle, capability layer model, maturity model, implementation blueprint, metrics and worked examples.
	V1.1 · August 2026	Four assessment instruments published; validation and adversary emulation established as a first-class domain; automation and lifecycle metrics extended.
	V1.2 · August 2026	Book consolidation: corrected standards mapping; framework family, Response Horizon, V-Model, SOC comparison, NIS2/DORA, philosophy, current-site alignment and preservation audit; and the Why UTIOM Is Different three-part synthesis with supporting editorial figures.
	Development · From 2022	Four years of building and testing against real security-operations work before public release.
	Origin · Circa 2018	Core idea surfaced while the author was writing his first book: security operations should be designed as one system rather than assembled from disconnected parts.

Table of Contents

How to read this book?	3
Preface.....	4
Introduction	4
Why UTIOM Exists?	4
Terminology and Scope	6
1 The Foundations.....	7
2 The Unified Lifecycle	13
3 Capability Layer Model	17
4 Standards and Framework Integration	18
5 Threat-Informed Maturity Model.....	19
6 Implementation Blueprint	20
7 Engineering Extensions.....	23
8 Metrics and Performance Indicators	23
9 Industry Use Cases Samples	24
10 Outcomes and Benefits	32
11 Community and Governance.....	32
12 Alignment with NIST Cybersecurity Framework (NIST CSF)	33
13 Alignment with SOC Capability Maturity Models (SOC-CMM).....	34
14 Alignment with the Digital Operational Resilience Act (DORA)	34
15 Conclusion.....	35
16 The Framework Family	36
17 The Response Horizon	37
18 Design and Validation: the UTIOM V-Model	38
19 Traditional SOC Operating Model Compared with UTIOM	39
WHY UTIOM IS DIFFERENT	40
I. It Starts With Management, Not Tools	40
II. Detection Is Engineering, Not Improvisation.....	44
III. Response Is the Operating Mode, Not the Emergency	49
20 UTIOM for NIS2 and DORA	54
21 Philosophy and Core Principles	56
22 A Note on What Strategy Means in UTIOM	57
23 Release History	57
24 Glossary.....	57
25 Further Reading and Sources	62
About the Author.....	63
Appendix A - Operational Use of MITRE ATT&CK	63
Appendix B - UTIOM Measurement Instruments	64

Appendix C - Content Preservation and utiom.de Coverage	64
Appendix D - Current utiom.de Alignment Supplement	65
Appendix E - Archival Original Lifecycle Diagram.....	67

How to read this book?

Who this book is for

CISOs, SOC leaders, security architects, detection engineers, IR leaders

How to use it¹

- Read chapters 1–2 for mindset
- Read 3–6 for implementation
- Use chapter 9 for practical examples

What this book is not

A tool guide, vendor comparison, or compliance checklist.

¹ Feel free to reach me out on my LinkedIn. <https://www.linkedin.com/in/rezaadineh/>

Preface

Security operations have reached a defining moment. Across industries, SOC's overflow with alerts and dashboards, yet the people behind them struggle to answer a single question: What is our purpose?

The Unified Threat-Informed Operations Model—UTIOM—is created to answer exactly that.

UTIOM emerged from fifteen years of building and transforming SOC's for banks, FinTech's, and hybrid enterprises. It recognizes that the gap between strategy and execution is the true vulnerability of modern defence. Technology scales quickly; understanding rarely does. UTIOM bridges leadership vision, engineering discipline, and adversary awareness into one coherent, measurable system.

“Security operations are not about collecting logs, running tools and reacting to alerts; they are about understanding intent.”

This book presents UTIOM as both a philosophy and a practical framework. It blends management science with detection engineering, providing a roadmap any organization can adapt whether cloud-native or legacy, centralized or distributed.

Introduction

Why UTIOM Exists?

Security operations are at a crossroads. The traditional model focused on isolated monitoring and reactive incident response, no longer meets the demands of today's dynamic threat landscape. Many organizations suffer from fragmented responsibilities, siloed tools, and a lack of cohesion between leadership intent and technical execution.

In practice, this produces predictable failure patterns:

- SOC performance measured by volume (alerts, dashboards, tickets) instead of outcomes
- Detection programs optimized for coverage rather than risk reduction
- Response executed through improvisation instead of engineered playbooks
- Engineering work driven by tools and vendor content rather than crown jewels and threat priorities

UTIOM introduces a holistic, lifecycle-driven model that treats Security Operations and Incident Response as one living system, designed and improved like a product.

What UTIOM Is

UTIOM is an operating model that unifies:

- Leadership direction (vision, governance, accountability)
- Threat-informed strategy (threat profiling, risk prioritization)
- Engineering execution (telemetry, detection-as-code, automation)
- Operational response (playbooks, SOAR, containment discipline)
- Continuous improvement (Kaizen, validation loops, maturity management)

UTIOM is built on widely adopted frameworks such as NIST CSF, TOGAF Standard, 10th Edition, MITRE ATT&CK, ISO 27001, and integrates with complementary models like SOC-CMM, plus the author's proprietary frameworks STRATA² and TID-CMM³.

What UTIOM Is Not

UTIOM is not:

- A new compliance framework
- A tool or vendor architecture
- A replacement for NIST CSF, ISO 27001, or SOC-CMM
- A “more detections equals more security” philosophy

UTIOM is a unifying language and lifecycle that helps organizations design security operations that are purpose-driven, threat-informed, and engineering-led.

² STRATA (Strategy, Talent, Resilience, Automation, Telemetry, Adaptability) is a refined version of People, Process, Technology. It is a new concept I published in LinkedIn.

³ A framework of mine, published at tid-cmm.com, that evaluates Threat Detection Coverage, Detection Engineering, Response & Recovery, Analytics & Automation, Threat Intelligence Integrations & Deception, Governance & Continuous Improvement. (for those who are interested, if you followed my works and papers on LinkedIn you can get the idea from my previous published papers.)

This Framework introduces a holistic model: The Unified Security Operations Model. It reimagines the entire discipline of cybersecurity operations as one integrated, lifecycle-driven system. The model unifies leadership strategy, software engineering principles, and continuous improvement into a coherent, adaptive process that drives measurable outcomes. Built on top of widely adopted frameworks--NIST CSF, TOGAF Standard, 10th Edition, MITRE ATT&CK, ISO 27001--and Author's other proprietary frameworks STRATA⁴ and TID-CMM⁵, the model translates theory into practical design. It aligns business value with engineering execution and proposes a universal yet adaptable structure applicable across industries.

The idea of this framework model is simple and it is all about thinking and considering about Security Operation and Incident Response as a live system, as a product, and reminding ourself that this is a system design and this is the way it will work in a meaningful and practical way with expected outcomes, instead of doing separate random operation with no specific goals and siloed way.

If we want to think clearly, and ask a question what is the definition of cyber security and cyber defence? It is actually about Risk control and reducing the Risk, but how it supposed to happen in practice ?

Then the blueprints for operation will come with many different checkboxes. In many companies this is siloed in different teams, different goals, siloed and separated. There are always gap between Management and Engineering.

If we think clearly we will see the core function of doing all of this, in a practical way is to do the right Security Operation; and Security Operation itself is a system process.⁶ The goal of Security Operation is to do the Incident Response in a meaningful way. That means what we can borrow from NIST to prepare for incidents, have the detection and response capabilities and have a lessons learned form each incident.

But actually companies needs in practice to be successful in IR and Security Operation, but based on available reports and data⁷ from many different sources, (But also from the authors experience) we can see the most companies and business they did not think through the Security Operation, They are not mature enough, neither there are no clear vision and plan for improvement, and in many case they do not have the proper plan, process and people, in some case they spend milion or thousands over different siloed technology or buying a service from different vendors, but still they are not satisfied or they are far from being effective and practical in most cases.

NOTE:

There are two main other methodologies that need to be emphasized, the first one is the NIST-CSF, which is actually designed for having a proper Security Operation and, as a result, the right Incident Response, but unfortunately, in my experience, it is not well-received and understood by many companies.

Second is SOC-CMM, which I do like very much, and as a Capability Maturity Model, it could help many Security Operations to have a method and tools to measure specific domains and aspects of a Security Operation, then they would have an idea of their maturity level and their weakness.

Now, let's think one more time, what is a security operation?

Before we can proceed, we need to identify what exactly a security operation. So, a Security Operations with a traditional definition is a function or a unit of People, Processes & Technology to serve the mission of Incident Response for a business.

The core functions would be:

- 1- Monitoring
- 2- Detection
- 3- Analysis
- 4- Response
- 5- Prevention

From a structural point of view, there are 3 basic ways to implement it:

- 1- Internal
- 2- External⁸
- 3- Hybrid systems

A model like SOC-CMM helps measure security operations maturity by providing a structured framework to assess a SOC's capabilities and processes across five key domains: Business, People, Process, Technology, and Services. And I highly

4 STRATA=Strategy, Talent, Resilience, Automation, Telemetry, Adoptability, Evolotion

5 Threat-Informed Detection Capability Maturity Model. Published at tid-cmm.com with eight domains and 58 sub-capabilities, aligned to MITRE ATT&CK Enterprise and crosswalked to NIST CSF 2.0 and SOC-CMM.

6 Security Operation and Incident Response are the same concepts in practice.

7 Reports like SANS SOC Survey, Splunk State of Security Report, Gurucul "Pulse of AI-Powered SOC" Report, CardinalOps State of SIEM Report, Gartner Magic Quadrant for SIEM, Forrester Wave: Security Analytics Platforms, IBM Cost of a Data Breach Report (The "Gold Standard"), Verizon Data Breach Investigations Report (DBIR), Mandiant M-Trends Report

8 Like MSSPs (Managed Security Service Provider)

recommend using it. On the other hand, UTIOM is a framework for businesses and companies to develop their own security operation program in a practical and effective way.

So far, we have seen that Security Operation is a function or unit of operation with a specific goal. So it is the core idea. Basically this function is a system, a system that should be applied via an operational unit with a very specific task, to reduce and control risk of cyber threat in real time and increase the readiness of the cybersecurity team.

Therefore, I used the system design principle, software engineering principal and management principle to develop the UTIOM framework that will help you to implement the security operation in the right way.

So keep in mind that I am trying to bring the best of the other world and put them together to design this framework, so we can rely on them because they are defined models and references.

With all of this in our mind now, we can move forward to the next section to see the foundation of the UTIOM framework.

Terminology and Scope

To avoid ambiguity, UTIOM uses the following definitions:

- Security Operations (SecOps): The overall organizational capability to detect, respond, and continuously reduce cyber risk in operational reality.
- SOC: The organizational function (internal, external, or hybrid) responsible for executing part of SecOps.
- Incident Response (IR): The structured capability to prepare for, detect, analyze, contain, eradicate, recover, and learn from incidents.
- Detection Engineering: The engineering discipline that designs and maintains detection logic, telemetry requirements, testing, and automation as a lifecycle.
- Threat-Informed: Decisions are prioritized based on realistic adversary behaviors and business risk, not generic best practice.

1 The Foundations

Security Operation is like a product and this product need a product designer and a product owner. UTIOM assumes clear ownership of the security operations lifecycle, similar to product ownership in engineering organizations.

1.1 Management and Leadership Principles

“Vision Defines Systems”

Every durable organization begins with a clearly articulated purpose. Let’s borrow from Peter Drucker⁹’s principle, “Without a purpose, there is no management,” captures the essence of governance. In security operations, vision establishes why the SOC exists, what it protects, and how success is measured. Without it, detection efforts drift toward tool management rather than risk management.

TOGAF Standard, 10th Edition¹⁰’s Architecture Vision and ISO/IEC 27001:2022/Amd 1:2024 Clauses 5.1–5.3 both mandate top-management direction. UTIOM extends this requirement by treating Vision as the first operational control in the lifecycle. A well-stated vision defines the business value of security, aligns stakeholders, and sets the boundaries for engineering design.

“Strategy as the Bridge”

Henry Mintzberg¹¹ described strategy as “a pattern in a stream of decisions.” UTIOM interprets this to mean that strategy must continually translate high-level objectives into actionable, prioritized outcomes. Where traditional strategies become shelf documents, the UTIOM Strategy domain behaves like a living architecture: capabilities are built, tested, and refined against evolving risk and threat contexts. The bridge between vision and execution remains active.

“Continuous Improvement and Kaizen¹²”

Borrowed from the Toyota Production System, Kaizen emphasizes that small, consistent improvements lead to compound transformation. Deming’s PDCA cycle provides the mechanics Plan, Do, Check, Act. In UTIOM, Continuous Improvement is not a trailing activity but an integral feedback phase that restarts the entire lifecycle. Each iteration strengthens strategic clarity, detection precision, and operational confidence.

“Improvement is not a phase; it’s a culture.”

“Management and leadership role is crucial, therefore we need to select the right methodology”

"Management by Objectives for Defence" Borrowing from Drucker’s MBO¹³, UTIOM ensures that detection engineers and analysts are not just 'running tools', but are partners in creating value. By setting SMART¹⁴ goals aligned with Crown Jewels protection, the system maintains a 'Spirit of Performance' where every technical action is a traceable step toward a strategic outcome.

Drucker popularized MBO to ensure that everyone in an organization is aligned on shared goals. In a SOC, this prevents "random operation" by ensuring technical tasks serve a strategic purpose.

- Collaborative Goal Setting: Objectives are set through discussion between managers and the technical "knowledge workers" (analysts and engineers), ensuring they understand how their work contributes to the larger vision.
- Cascade of Objectives: High-level strategic goals are translated into day-to-day tasks, such as improving Mean Time to Contain (MTTC) for "Crown Jewel" assets.
- SMART Criteria: Objectives must be Specific, Measurable, Achievable, Realistic, and Time-bound.

9 Peter Ferdinand Drucker (1909–2005) was an Austrian-American author, educator, and management consultant widely regarded as the "Father of Modern Management". He transformed management into a distinct, teachable discipline that balances technical efficiency with social responsibility.

10 The Open Group Architecture Framework. It is a widely used, open standard methodology and framework for designing, planning, implementing, and governing an enterprise's information technology architecture to align with business goals.

11 Henry Mintzberg is a prominent Canadian academic, author, and Professor of Management Studies at McGill University, known for his influential work in business and management that often challenges conventional wisdom. He has written over 150 articles and more than 20 books on topics including strategy, organizational design, and leadership education.

12 Kaizen (改善) is a Japanese term and business philosophy that means "continuous improvement". The word is composed of two characters: "kai" (meaning change) and "zen" (meaning good). The philosophy centers on the idea that many small, incremental changes made consistently over time can lead to significant positive results in efficiency, quality, and productivity.

13 Management by Objectives

14 Specific, Measurable, Achievable, Realistic, and Time-bound

“The "Knowledge Worker" as Assets”

Drucker coined the term "knowledge worker" for employees whose primary asset is their theoretical and analytical knowledge.

- Empowerment and Autonomy: Because SOC analysts often know more about specific threats than their managers, they require autonomy to solve unique problems.
- Continuous Learning: Knowledge is "perishable"; it must be constantly improved and challenged, or it vanishes.
- Focus on Strengths: Effective management makes an employee's strengths productive and their weaknesses irrelevant.

"Systematic Abandonment" As Drucker noted, 'If you want something new, you have to stop doing something old'. UTIOM integrates this by treating the pruning of obsolete telemetry and detections as a core engineering discipline, preventing the SOC from becoming a 'factory of data'.

“Be aware of ‘Effectiveness vs. Efficiency’”

A core Drucker principle is distinguishing between "doing things right" (efficiency) and "doing the right things" (effectiveness).

- Prioritizing Impact: There is nothing so useless as doing efficiently that which should not be done at all. In UTIOM terms, efficiently detecting "random noise" is a failure of management if it doesn't control actual business risk.
- Measuring Outcomes: Focus on metrics that prove effectiveness (e.g., Risk Reduction) rather than just efficiency (e.g., Number of Alerts).

In fact we should think this way:

- "Vision as the Primary Control": Following Drucker's principle that "Purpose is the starting point of management," UTIOM treats the Vision not as a statement, but as the first operational control that dictates the boundaries of all engineering efforts.
- "The Knowledge Worker's Autonomy": In a UTIOM-led SOC, analysts are "Knowledge Workers" whose primary task is to interpret intent, not just operate or manage tools. Management's role is to provide the "Strategy Bridge" so these workers can exercise "Self-Control" through observability. Management should lead all roles to be aware of the operation model in Security Operation and everyone must be aligned and aware of priorities. (The goal is to be Threat-Informed and it won't achieve until everyone would be on the same page.)
- "Systematic Abandonment": To prevent the "factory of data" from becoming bloated, UTIOM adopts Drucker's rule of "abandoning yesterday." Every Continuous Improvement cycle (Section 2.7) must include a review to "slough off" detection rules that no longer protect a Crown Jewel or address a current threat.
- "Effectiveness over Efficiency": Drucker noted that "Efficiency is doing things right; Effectiveness is doing the right things." UTIOM ensures effectiveness by forcing detection rules to be mapped to a specific risk requirement rather than just high-volume research.

1.2 Engineering and Systems Thinking

SOCs often resemble factories of data rather than engineered systems. They assemble technologies like SIEM, EDR, SOAR without a unifying design logic. UTIOM applies systems engineering to security operations: define inputs, outputs, boundaries, and feedback before integrating components.

“Systems Are Engineered, Not Assembled”

From NASA’s engineering philosophy: reliability results from design, not accumulation. UTIOM adopts this by mapping every operational process to its dependencies and feedback signals. For example, telemetry inputs (visibility) produce detection artifacts (outputs) that trigger response mechanisms; response data then feeds the next design cycle.

“DevOps Logic¹⁵ for Detection”¹⁶

Modern engineering thrives on iteration and testing. UTIOM’s detection engineering domain mirrors software practices:

- Test-Driven Detection rules must be verifiable against simulated threats.
- CI/CD Pipelines deploy, validate, roll back safely.
- Version Control trace every rule’s lineage and purpose.
- Observability measure false-positive rates, detection coverage, and rule latency.

By codifying detection as engineering code, UTIOM transforms threat detection from reactive art to accountable science.¹⁷

“Detection becomes engineering, not improvisation.”

“UTIOM standardizes the lifecycle and engineering discipline, not the threats or detections themselves.”

Note:

Beyond just using Git and CI/CD, apply actual software architecture patterns to how you write detections.

- DRY Principle¹⁸ (Don't Repeat Yourself): move repeated logic and exclusions to shared configuration objects. For example, instead of writing the same IP exclusion list into 50 different SIEM rules, move that list into a global "Configuration Object."
- Abstraction Layers: Create a "Common Information Model", so logic survives vendor changes. Your detection logic should not care if the data comes from CrowdStrike, SentinelOne, or Sysmon. The logic should sit on top of a standardized schema.
- Unit vs. Integration Testing: unit tests, integration tests, and effectiveness tests
 - o Unit Testing: Testing a single detection rule against a small JSON log snippet.
 - o Integration Testing: Testing how that rule interacts with the alerting pipeline and the SOAR playbook.
 - o Effectiveness Testing: Testing if the rule would trigger in expected situation.

Borrowed from Industrial Design: Cognitive Ergonomics and "Affordance"

In industrial design, a well-designed tool "tells" you how to use it and it is purpose driven. So a Security Operation should be designed in the same way. Security operations must be designed for human cognition:

- Signal-to-Noise Ratio (SNR) Optimization: Industrial designers remove clutter to focus the user on the primary control. Optimize signal-to-noise ratio through grouping and narrative incidents.
- Standardized Interfaces: Ensure that regardless of the tool, the "Output" (the alert) always follows the same visual hierarchy: What happened? Why does it matter? What is the first step to fix it? And so on. We need the whole story, the big picture, the time-line, not random single alerts.
- Reducing "Alert Fatigue" as a Design Goal: Treat alert fatigue and analyst burnout not as a HR issue, as a system design failure.

“Resilience and Graceful Degradation”

Assume components fail. Security operations must remain functional when sensors are bypassed or degraded:

- Redundant visibility paths (e.g. identity and network telemetry as backup to endpoint)
- Backpressure and circuit breakers for log spikes

15 Detection Engineering Life Cycle" (DELC)

16 Do not rely on default detection rules in place, tailor them to your environment. (Even if the default rule looks good for you, you still need to keep them updated regularly.)

17 In case you are not ready to implement the codified system for detection development, do not skip this, it is more about the concept and idea of how to develop a detection code in a managed controlled way like we do release a stable software. For start consider any methodology to develop a code and having a version control for it, and being able to trace a detection for the whole lifecycle of it.

18 The DRY principle is a fundamental software development guideline introduced by Andy Hunt and Dave Thomas in their 1999 book The Pragmatic Programmer. The core idea is that every piece of knowledge, logic, or data within a system should have a single, unambiguous, and authoritative representation.

- Meta-detections that monitor the health of telemetry and detection pipelines

“Less, But Better: The Minimalism of Defense” Following Dieter Rams¹⁹ principle that 'Good design is as little design as possible.' UTIOM rejects the accumulation of tools, logs and running different separate teams and process. Instead, it focuses on the 'Honesty' of detection—ensuring that every alert accurately reflects a business risk and provides an 'Understandable' path to response. By prioritizing 'Unobtrusive' systems that only signal when necessary, we eliminate the noise of the 'data factory' and protect the analyst's cognitive ergonomics. We should design a unified system that works purposefully.

“Feedback Loops as Learning Systems”

Every SOC event true positive, false positive, near-miss becomes structured feedback. Data from detection and response flows back into telemetry design and strategic planning. This creates a self-correcting ecosystem capable of continuous adaptation without external audits.

“Design, don’t assemble. Detection should be built with purpose, not patched with panic.”

“Systems Engineering: Requirements Traceability (The V-Model)^{20,21}

Systems engineering dictates that a system’s success is measured by how well it meets specific requirements. In many SOC, detections are added randomly based on "cool" research rather than system needs.

- Requirements Mapping: Every detection artifact should be traced back to a specific risk or threat model (e.g., MITRE ATT&CK). If a detection doesn't map to a requirement, it is usually "waste" in the system.
- Verification vs. Validation:
 - o Verification: Does the rule work as intended? (e.g., Does the regex match the log?)
 - o Validation: Does the rule actually stop the business risk? (e.g., Does it catch the actual attacker? Or it is just a random prebuilt rule with no risk assigned?)

1.3 The Convergence

Leadership provides direction and intent; engineering provides precision and reliable execution. When disconnected, organizations experience strategic confusion above and operational fatigue below. That is a common point of failure. UTIOM unifies them through a recursive lifecycle that binds strategy, engineering, and intelligence.

So before we see the schematic concept in a high level diagram, let’s recap the idea of UTIOM:

We typically have 3 main pillar for running a Security Operation:

- 1- Leadership & Governance
- 2- Engineering & Enablement

19 Dieter Rams is a highly influential German industrial designer. He is best known for his long tenure as the head of design for the consumer electronics company Braun from 1961 to 1995, and for his work with the furniture company Vitsoe. His design philosophy, encapsulated by the phrase "less, but better" (Weniger, aber besser), has had a lasting impact on 20th-century aesthetics and modern design practices, notably influencing designers at Apple, such as Jony Ive.

20 V-Model, a structured approach used primarily in software development and systems engineering. The V-Model is a procedural model that visually demonstrates the relationship between each stage of the development life cycle and its corresponding testing phase, which creates the "V" shape.

21 The V-Model is a procedural model that visually demonstrates the relationship between each stage of the development life cycle and its corresponding testing phase, which creates the "V" shape.

Left Side (Verification/Development Phases): The process moves downward from high-level, abstract requirements to detailed design specifications. This phase ensures you are "building the product right" according to the plan.

Right Side (Validation/Testing Phases): The process moves upward, involving testing activities that correspond directly to a development phase on the left. This phase ensures you are "building the right product" that meets the user's actual needs.

The Bottom of the V: Represents the coding or implementation phase, where the actual product is built.

IAPM - International Association of Project Managers

Requirements Traceability in the V-Model

Requirements traceability is the ability to track the life of a requirement from its origin through development and testing back to its source or vice versa.

Purpose: It ensures that every single requirement defined at the beginning of the project is accounted for, implemented, and thoroughly tested.

Mechanism: Traceability links connect requirements documents (left side) to their relevant test cases (right side). For example, the initial user requirements are linked to the User Acceptance Tests (UAT).

Benefit: This clear, bidirectional link makes it easier to track progress, manage changes, ensure quality and compliance (especially in safety-critical industries like automotive or medical devices), and prevent overlooked requirements.

3- Operations & Analysis

And each one of them having their own subprocess. In zoom-out we will have the Unified Threat Informed Operation Model. UTIOM provides the unified loop that keeps these pillars aligned through continuous feedback.

For implementing UTIOM we do need to define our Security Operation Vision, with a defined Vision we can now define our Security Operation Strategy, and with a Risk-Based approach we can review our assets and define our Crown-jewels, this can lead to check our visibility of our critical assets and continuous development of threat detection rules for them, having detection rules can led to developing proper response plan/playbooks.

The Unified Loop:

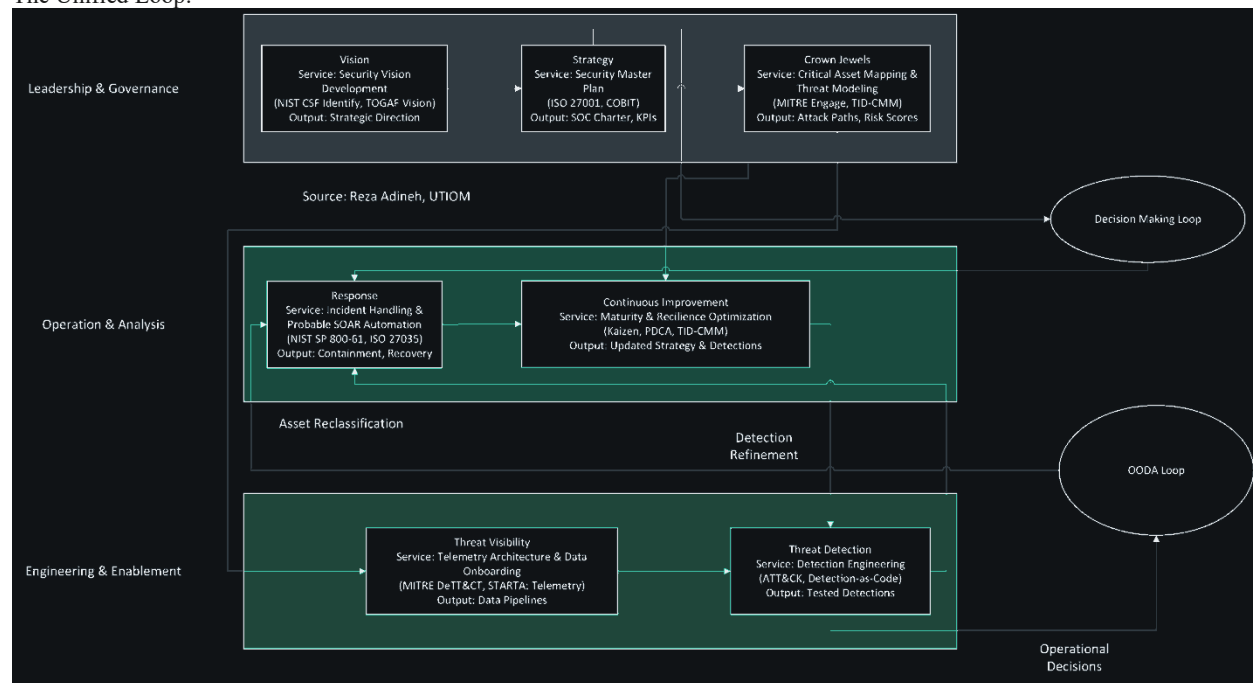


Figure 1- UTIOM high level

Each phase consumes and produces knowledge. Outputs of one become inputs to the next. This cyclical logic converts fragmented operations into an adaptive control system.

Why Unification Matters?

- Strategic Traceability: executives can trace any incident to a policy, metric, or capability.
- Engineering Efficiency: teams build only what serves defined business and threat priorities.
- Cultural Alignment: analysts understand purpose; leaders understand constraints.

The convergence yields a system that learns both top-down and bottom-up a Threat-Informed Organization rather than a reactive monitoring centre.

“A SOC without a vision is an alert factory.”

1.4 UTIOM Concept review

A well-defined vision and strategy function like a north star. In Security Operation without defining vision and strategy and knowing the crown jewels it is not possible to accomplish anything successful.

In this section we will see how this UTIOM framework will help you to unified a meaningful threat informed detection and response in a practical way.

Starting with vision, a practical way of defining vision would be defining a meaningful goal, like we are aware of all critical Risk that target our Crown Jewels.

From strategic point of view we need to define at least some basic strategies but practical, doing a threat profiling for our business is one mandatory thing and is the main basic step, that should define the baseline for threat detection approaches. While we knew about our adversaries, their intent, motivation and their probable capabilities, now we can be ready for defend, and align our detection and response program accordingly.

So in summary, UTIOM's practical sequence:

- Define vision for Security Operation, (Vision is why or the target destination, is the goal of the SecOps)
- Define, develop and implement strategy for Security Operation, The main basic activity is about Implementing Threat Profiling and Risk prioritization. (Vision define strategy, Strategy is how to achieve to the defined Vision, it is the practical, logical actionable roadmap to use the vision and implement our Design.)
- Identifying business key assets & crown jewels, Providing Threat Visibility, (Threat Detection should be an ongoing continues process, and it is fed by Threat modelling and threat intelligence mainly) and model realistic threats against them.
 - Developing aligned Threat Modelling,
 - Checking the visibility status by being sure we generate and collect main necessary telemetry,
 - Considering implementation of deception solutions (In a more mature situation placement of deception solution for a proactive detection and analysis),
- Engineer visibility, ensure telemetry exists where it matters most
- Engineer detection as a lifecycle (code, testing, fidelity, coverage)
- Engineer response via playbooks and automation aligned to threats and crown jewels
- Continuously improve using lessons learned and validation loops (purple team)²²

Important note:

Mapping UTIOM to NIST Incident Response

This framework is exactly aligned with Incident Response steps and is a way to modernize, extend and implement the Incident Response for Security Operation in a Threat Informed Way and Risk aware approaches.

NIST SP 800-61 Rev. 3 (2025) supersedes Rev. 2 and integrates incident response across the six Functions of CSF 2.0. The four-phase lifecycle shown below is the legacy SP 800-61 Rev. 2 model, retained here for practitioner familiarity and historical comparison:

- 1- Preparation
- 2- Detection & Analysis
- 3- Containment, Eradication & Recovery
- 4- Post Incident Activity

So to map it with UTIOM it is as below:²³

NIST Incident Response Functions	Unified Threat Informed Operation Model (UTIOM) Functions
Preparation	Vision, Strategy, CJ, Threat Profiling, Threat modelling, Threat Visibility
Detection & Analysis	Threat Detection Engineering (rules, tuning, analysis workflows)
Containment, Eradication & Recovery	Response (playbooks, containment automation, recovery coordination)
Post Incident Activity	Continuous Improvement(learning loop, updates to strategy and engineering)

In the next section we will explain the Unified Lifecycle that UTIOM farmwork provide for an effective modern and unified way of implementing Incident Response for a Security Operations.

22 With having the threat profiling, knowing targeted high risk threats, having threat modelling and related threat detection rules, leveraging threat intelligence, we can work on threat hunting with a clear strategy of what we should looking for. Furthermore, in order to improve our threat detection program we can use the OODA loop, in order to see how effective is our current detection rules. For testing the rules, using Purple teaming, Red teaming is the way to go.

Knowing threat detections, we can now think of response plan and if possible business continuity plan based on realistic threats we already monitoring. It could lead to asset reclassification as well.

This is the last step of our main steps, continuous improvement. With continuous improvements we will take a look to the whole cycle, and see how and where we can improve. And this could lead to refine the strategies.

23 UTIOM complements, not replaces, all mapped frameworks.

2 The Unified Lifecycle

Security operations become effective only when they are cyclical, not linear. UTIOM defines seven connected domains that together describe the full life of defence and Threat Informed Incident Response.

Each domain is:

- A decision space
- A feedback loop
- A measurable capability²⁴

First missing point in many organization is not having the right vision for their Cyber Security Operation or their Risk management. Defining the Vision must lead to define the right strategy. And the strategy should be aligned with the business/company Crown Jewels²⁵; and knowing the business critical assets (Crown Jewels)^{26, 27} will provide the threat visibility through threat modelling, and with having threat visibility we can continuously develop meaningful, aligned threat detection rules that actually matters, not random detection from different source that has nothing to do about our real world cyber risk. While we know what we are looking to detect, then we can develop our response plan based on that and at the final phase of this process we will have a Continuous Improvement to revise and use the lessons learned.

2.1 Vision Defining Purpose

While we considers Security Operations as a engineered system we must define how this system would be successful. All engineered systems begin with purpose. In SecOps, purpose answers why we defend and what success means. Without it, SOC's default to counting alerts instead of outcomes.

Core Activities

- Define the business intent of the SOC.
- Align Security Operation Vision with Business CJs.
- Establish governance and accountability.
- Identify success metrics (e.g., availability, confidentiality, safety, continuity).

Outputs

- Long Term and short Term Security Operation Vision.
- Vision statement and policy charter.
- Stakeholder map and alignment workshop results.
- Baseline metrics (e.g., detection confidence, time-to-resolution).

Referenced Frameworks

- TOGAF Standard, 10th Edition Vision
- ISO/IEC 27001:2022/Amd 1:2024 Clauses 5.1–5.3
- NIST CSF 2.0 (GV.OC, GV.RR).

“Vision is the compass; tools are merely instruments.”

2.2 Strategy Translating Vision into Design

Vision without strategy is intention without motion. UTIOM views strategy as a capability-building system rather than a document. Every decision must connect a risk to a measurable improvement.

Core Activities

24 Mainly qualitativie, some quantitavie

25 Each role in a security Operation must be aware of their operational vission and mission, and this vision and missison are defined based on business operational critical assets.

26 It is super crucial for defence team to know the CJs, check the endnotes for more details.

27 from Sun Tzu's The Art of War : "If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle." Key Takeaways from the Text

Sun Tzu doesn't just mention "strengths and weaknesses" in passing; he dedicates an entire chapter (Chapter 6: Weak Points and Strong) to how you should apply that knowledge.

Self-Knowledge: This is about "knowing yourself"—understanding your own resources, morale, and limitations.

In cyber security, applying Sun Tzu via a SWOT lens means moving from reactive "firefighting" to proactive defense. Knowing yourself involves rigorous asset discovery and vulnerability management—identifying your "Weaknesses" (unpatched software) and "Strengths" (i.e., robust encryption). Knowing the enemy means utilizing Threat Intelligence to understand the "Threats" (specific hacker groups/TTPs) and "Opportunities" (gaps in the attacker's own infrastructure). By aligning these, a CISO ensures that security controls aren't just a wall, but a strategic maneuver that makes the cost of an attack higher than the potential reward.

- Threat and risk prioritization. (Threat Profiling²⁸ as a core function).
- Resource planning and capability road-mapping.
- Defining measurable KPIs and KRIs tied to crown jewels.

Outputs

- SOC Master Plan and quarterly objectives.
- Threat profile and prioritization model.
- Capability increment schedule.
- Stakeholder scorecards.

Referenced Frameworks

- COBIT 2019 Governance.
- ISO 27001 6.1–6.2, 8.2–8.3
- STRATA²⁹ Strategy.
- TID-CMM³⁰ Strategic Alignment.

2.3 Crown Jewels Focusing on What Matters

No organization can protect everything equally. Crown Jewel Analysis (CJA) identifies critical assets, processes, and data whose compromise would create disproportionate damage.

Core Activities

- Asset inventory and classification.
- Mapping Threat profile with CJ.
- Business impact mapping.
- Threat modelling for identified Crown Jewel (CJ).
- Critical Asset mapping to the high risk Threats.

Outputs

- CJ registry with owners.
- Threat profile mapped with CJ and defined high priority TTPs.
- Attack-path diagrams for CJs.
- Checklist of Protection, Detection, Visibility and Response capability readiness for CJs based on top priority TTPs.
- Mapped related MITRE ATT&CK TTP with CJs.
- Dependency matrix linking CJ to data sources.
- Threat Detection rules logic.

Referenced Frameworks

- MITRE Engage
- ISO 27001 Clause 8
- TID-CMM Threat Prioritization.

“You can’t build meaningful visibility without knowing what deserves to be seen.”

2.4 Threat Visibility Engineering Telemetry

Visibility is the bloodstream of detection. UTIOM designs visibility from the CJs outward, ensuring telemetry covers what matters first.

Core Activities

- Map ATT&CK tactics to data sources.³¹
- Map Threat Modelling to data sources.³²
- Define logging, retention, and access standards.
- Implement data quality and normalization checks.

28 Threat profiling is a proactive cybersecurity process that involves identifying, analyzing, and documenting the specific, relevant adversaries and threats targeting an organization. (<https://www.linkedin.com/pulse/cyber-threat-profiling-understanding-different-actors-reza-adineh/?trackingId=NkWFdbDGToWs8KNUWh51Rw%3D%3D>), (<https://www.linkedin.com/pulse/crowdstrike-mandiant-red-canary-reza-adineh-qrcgf/>)

29 <https://www.linkedin.com/pulse/from-ppt-strata-reza-adineh-ysqhf/?trackingId=%2FkSuK87cQRGkLDSGcxCSw%3D%3D>

30 Threat Informed Detection Capability Maturity Model

31 Means those TTPs which are mapped to CJs.

32 We can leverage Threat-Informed Detection Capability Maturity Model in this activity.

- Implementation of Deception variation aligned with CJ.³³

Outputs

- Visibility Blueprint and Gap Report.
- Mapped Threat models to required data sources.
- Telemetry onboarding roadmap. (Defined required data pipeline for CJs high priority Threats)
- Threat Activity visibility.
- Metrics: % CJ coverage per Threat, log quality index.

Referenced Frameworks

- NIST SP 800-137
- MITRE DeTT&CT
- CIS Critical Security Controls v8.1
- STRATA Telemetry

2.5 Threat Detection Engineering Awareness

You can't detect what you can't observe, but observation without interpretation is noise. Detection must be engineered, version-controlled, and threat-informed.

Core Activities

- Develop Detection rules referenced by Thread modelling in previous steps.
- Develop rules mapped to ATT&CK TTPs.
- Apply Detection-as-Code practices (Git, CI/CD, testing).
- Measure fidelity, coverage, and operational cost.
- Automate QA and regression testing.
- Red/Purple Teaming planning for Detection Verifications.

Outputs

- Detection Repository with traceability.
- QA Reports with coverage metrics.
 - % of implemented and tuned detection rules per Threat Modelled
 - % of implemented deception in each operational zone
- False positive and false negative monitoring.
- Mean Time to Detect (MTTD) evaluation based on top TTPs.

Referenced Frameworks

- MITRE ATT&CK Enterprise v19.2
- DeTT&CT
- Sigma
- STRATA Automation.
- TID-CMM Detection QA.

“Detection built from behaviours lasts longer than detection built from indicators.”

2.6 Response Executing with Precision

Response is the natural continuation of detection. UTIOM positions incident handling as an engineered workflow, not an improvisation.

Core Activities

- Developing Response plan, Playbooks aligned with defined Threats.(prioritized threats and crown jewels)
- Automate containment through SOAR.(In case of absence of SOAR, consider containment plan without SOAR)
- Define escalation paths³⁴ and CJ-specific playbooks.
- Track MTTR, MTTC and containment SLA.

Outputs

- Playbook Library and Response Matrix.
- Incident Records with contextual tags.
- Lessons Learned Repository.

Referenced Frameworks

- NIST SP 800-61 Rev. 3
- ISO/IEC 27035 series (Parts 1–4)

³³ Deploy deception selectively where it increases adversary cost.

³⁴ And decision gates.

- FIRST CSIRT Services Framework v2.1
- STRATA Resilience
- TID-CMM Process Execution.

2.7 Continuous Improvement Learning Systems

No design remains optimal forever. Continuous Improvement is the intelligence loop that converts experience into new strategy.

Core Activities

- Post-incident reviews and Kaizen sessions.
- Red/Purple team validation of detection coverage.
- Update threat models and roadmaps.
- Conduct periodic benchmarking and maturity assessments.

Outputs

- Updated Vision and Strategy documents.
- Proper aligned input for protection, Detection and Response.
- Action plans with owners and timelines.
- Maturity scorecards (UTIOM / TID-CMM / SOC-CMM).

Referenced Frameworks

- Deming PDCA
- Kaizen
- SOC-CMM
- STRATA Adaptability.
- TID-CMM Feedback.

“Learning is the final deliverable of every incident.”

3 Capability Layer Model

UTIOM operates across three mutually reinforcing planes. Each layer represents both a technical depth and an organizational perspective.

Layer/Pillar	Focus	Main Goal	Primary Activities	Key Frameworks
Foundational (Leadership & Governance)	1. Vision, 2. Strategy, Missions, 3. Operations Model, 4. Governance, Architecture,	• Know The related Threat • Know yourself	Strategic planning, Role definition, Threat Profiling, Risk alignment	NIST CSF (Identify), ISO 27001, TOGAF Standard, 10th Edition
Operational & Analysis	1. Telemetry, 2. Visibility 3. Detection, 4. Analysis, 5. Response, 6. Feedback & Optimization	• Analysis & Response	Threat modelling, Log onboarding, Analysis, SIEM/EDR operations, playbook execution	ATT&CK, ISO/IEC 27035 series (Parts 1–4), STRATA Resilience
Engineering & Enablement	1. Protection, 2. Visibility, 3. Detection, Automation & QA, 4. Feedback & Optimization	• Build Detection Rules • Build Response Plan	Detection-as-Code, CI/CD, purple team validation, Kaizen loops, hunting, benchmarking	GitOps, DeTT&CT, TID-CMM Detection QA, SOC-CMM, PDCA, STRATA Adaptability

“Layers aren’t hierarchies they are symbiotic perspectives.”

4 Standards and Framework Integration

UTIOM deliberately aligns to recognised standards to support traceability, standards alignment and operational evidence across the security operations lifecycle of a security operation running a complete incident response process. UTIOM tries to provides traceability between business intent and operational execution.

UTIOM Domains	NIST CSF 2.0	ISO/IEC 27001:2022 + Amd 1:2024	Other Frameworks	Description
Vision	GV.OC, GV.RR, GV.PO.4.1–4.2, 5.1–5.3		TOGAF Standard, 10th Edition — Architecture Vision	Executive intent, accountability and governance of the security operation
Strategy	GV.RM, ID.RA	6.1–6.2, 8.2–8.3	COBIT 2019, STRATA	Threat profiling, risk prioritisation and capability roadmapping
Crown Jewels	ID.AM, ID.RA	A.5.9, A.5.12	MITRE Engage, TID-CMM	Asset criticality, business impact, threat modelling and attack paths
Threat Visibility	DE.CM	A.8.15, A.8.16	MITRE DeTT&CT, CIS Critical Security Controls v8.1, STRATA Telemetry	Telemetry design, logging standards and data coverage per modelled threat
Threat Detection	DE.AE, DE.CM	A.8.16, A.5.7	MITRE ATT&CK Enterprise v19.2, Sigma, TID-CMM, STRATA Automation	Detection engineering, testing and quality assurance
Response	RS.MA, RS.AN, RS.CO, RS.MI, RC.RP	A.5.24–A.5.26, A.5.28–A.5.30	NIST SP 800-61 Rev. 3, ISO/IEC 27035 series (Parts 1–4), FIRST CSIRT Services Framework v2.1, TIR-CMM	Containment, eradication, recovery and engineered playbooks
Continuous Improvement	ID.IM, GV.OV	Clause 10, A.5.27	SOC-CMM, Kaizen, PDCA, STRATA Adaptability	Feedback loops, validation, learning and maturity management

5 Threat-Informed Maturity Model

UTIOM's maturity ladder measures integration, threat realism, and engineering discipline.

Level	Designation	Characteristics	Threat-Informed Capability	Outcome
0	Absent	Fragmented ownership, Weak Visibility	None	Chaos, alert fatigue
1	Reactive / Threat-Aware	Initial ATT&CK-aligned detections around CJs	Awareness	Context replaces noise
2	Structured / Threat-Informed	CJ-based visibility & versioned rules + Aligned TI ³⁵	Intentional Design	Predictable defence
3	Integrated / Unified	Feedback ↔ Detection ↔ Strategy linked	Collaboration	Traceable operations
4	Adaptive / Engineering-Led	CI/CD + Purple Team loops	Automation	Rapid iteration & QA
5	Autonomous / Threat- Informed Automation	SOAR + Deception + Continuous Red/Purple teaming and validation	Intelligence	Self-optimizing SOC

Each level builds both vertical (maturity) and horizontal (unification) growth.

Level 5 is aspirational and depends on business risk tolerance, automation safety, and organizational maturity.

6 Implementation Blueprint

Implementation follows five progressive phases, each self-validating through metrics.

Phase	Core Actions	Main Deliverables
1- Strategic Alignment	Define vision & governance, Conduct CJ analysis, Threat Profiling and prioritization, Map threats to business risk	- Security Master Plan - Operation Model - Vision Statement - CJs profiles - Measurement Framework - Threat Profiles
2- Visibility Architecture	Threat modelling, Map CJ attack paths to data sources, build telemetry pipeline,	- Threat Models - Visibility Matrix - Gap Analysis - Data Quality KPIs
3- Detection Engineering	Build Detection-as-Code pipeline, apply CI/CD, QA tests, Providing required data feed for detection	- Detection Repository - QA Reports - Coverage Metrics
4- Response Execution	Deploy Response playbooks, Deploy SOAR playbooks, measure MTTR, refine containment flows	- Playbook Catalog - Incident KPIs
5- Feedback & Evolution	Kaizen reviews, Red/Purple team validation, update strategic roadmap	- Updated KPI - Dashboard Maturity Benchmark - Detection assessment and verification reports

“Implementation is a journey of validation, not deployment.”

6.1 Mapping Security Operations Processes to UTIOM

Common Traditional SOC Process	How It's Commonly Treated	UTIOM Interpretation	UTIOM Lifecycle Anchor
Threat Intelligence	Separate upstream function	Incident Response before impact, shaping assumptions and priorities	Strategy → Crown Jewels
Threat Modeling	If even exist. Design-time exercise	Incident Response planning against likely adversaries. (Unified and integrated Detection & Response)	Strategy → Threat Visibility
Detection Engineering	If even exist. Technical rule-writing task	Incident Response encoded into logic and telemetry. Detection is purposeful and a live operating system. High fidelity detection rules compare to random default detection rules.	Threat Detection Engineering
Threat Hunting	Proactive activity outside IR	Incident Response without alerts, hypothesis-driven. Purposeful.	Threat Detection → Response
Monitoring & Alerting	Firefighting approaches usually. Real-time alert handling	Continuous low-intensity Incident Response. Monitoring for what matters most. Knowing the priority and Threat Informed monitoring & alerting.	Threat Detection
Alert Triage	Firefighting approaches usually. Noise reduction steps if possible.	Decision refinement inside Incident Response. Threat Informed Detection aligned with Response readiness.	Response
Incident Investigation	Core IR activity	Strategic awareness. High-intensity Incident Response in highest matured implementation.	Response

Common Traditional SOC Process	How It's Commonly Treated	UTIOM Interpretation	UTIOM Lifecycle Anchor
Containment & Eradication	Separated Process. Usually distributed between different teams. Firefighting approaches. Reactive technical action.	Pre-designed Incident Response execution. The Response is mature and predefined and aligned with Threat Detection. Response is a part of a living operating system.	Response → Resilience
Forensics	Post-incident activity. Usually lack of required data.	Incident Response validation and learning. It is part of live operating system after incident.	Continuous Improvement
Lessons Learned	Optional retrospective	Incident Response feedback loop. It is a part of live operating system. It is ongoing process and it is not just restricted to an optional retrospective after an incident.	Continuous Improvement
Metrics & Reporting	Management overhead	Incident Response health indicators	Vision → Strategy
Training & Exercises	Separate readiness program. (If it exist at all)	Incident Response rehearsal	Resilience & Adaptability

Mapping Common IR phase from SANS and NIST model to UTIOM:

UTIOM Lifecycle Stage	SANS IR Phase(s)	NIST IR Phase(s)	What it means in UTIOM (modern, realistic)	Key capabilities (explicit)
Vision	Preparation	Preparation	Define purpose, success criteria, decision authority, and resilience outcomes tied to business services.	Impact tolerance, crisis posture, comms principles
Strategy	Preparation	Preparation	Translate vision into priorities, operating model, measurable outcomes, and investment focus.	Coverage goals, SOC-as-product cadence, metrics/SLOs
Crown Jewels	Preparation	Preparation	Identify critical services, data, identities, and trust boundaries; define what must not fail.	Service tiering, identity crown jewels, dependencies
Threat Modeling	Preparation	Preparation	Model likely adversaries, paths, and abuse cases against crown jewels; define “detection stories” and response intent.	Threat scenarios, ATT&CK technique selection, kill-chain paths, misuse cases, assumptions, crown-jewel attack paths
Threat Visibility Engineering	Preparation	Preparation	Engineer telemetry and evidence pipelines across endpoint/identity/network/cloud to support the modeled threat paths.	Logging design, enrichment, evidence readiness, deception sensors wiring
Threat Detection Engineering	Preparation (+ readiness)	Preparation (+ readiness)	Build detections as engineered artifacts aligned to modeled behaviors and telemetry reality; define tuning/acceptance.	Rule lifecycle, test cases, purple teaming validation, detection SLOs
Threat Detection Operations	Identification	Detection & Analysis	Continuous sensing, triage, enrichment, validation, and scoping decisions.	Entity timelines, investigation playbooks, intel-as-context
Threat Hunting	Identification (proactive)	Detection & Analysis (proactive)	Hypothesis-led hunts derived from threat models and visibility gaps; feeds detection backlog.	Hunt library, gap-driven hunts, campaign hunts
Response	Containment, Eradication, Recovery	Containment/Eradiation/Recovery	Execute containment, eradication, and recovery with clear authority, playbooks, and business-aware actions. Fully aligned with threat detection that already covers high risk top priority Cyber Threats.	Tiered handling, branch/service playbooks, automation, reporting triggers
Resilience (sub-stage)	Recovery	Recovery (within CER)	Restore safely, reinforce controls, prevent recurrence, and validate return-to-service.	Safe restore gates, identity re-issue, hardening, compensating controls
Continuous Improvement	Lessons Learned	Post-Incident Activity	Convert incidents and exercises into system improvements across strategy, threat models, telemetry, detections, and playbooks.	RCA, backlog grooming, retests, purple team re-validation, model refresh

7 Engineering Extensions

1. Detection-as-Code Pipelines versioned rules with automated testing and rollback.
2. SOAR Orchestration context-driven containment and notification flows.
3. Deception Fabric honeypots and tokens collect live adversary telemetry.
4. Continuous Red/Purple Team perpetual validation of detections and response.
5. Unified Telemetry Schema consistent taxonomy across multi-cloud sources.

8 Metrics and Performance Indicators

Category	Metric	Description	Purpose
Visibility	% CJ coverage per MITRE tactic % CJ coverage per Customized Threat Modelled Data Quality Index	Telemetry depth, Coverage per crown jewel and threat model, Completeness, parsing success, latency	Ensures data relevance & usability
Detection	% of implemented and tuned detection rules per Threat Modelled % of implemented deception in each operational zone Mean Time to Detect (MTTD)	Ratio of implemented Threat modelled detection rules Time between compromise and alert, Traceability to threat model	Measures readiness & responsiveness
Response	% of implemented Response rule per detection rule Mean Time to Contain (MTTC) Mean Time to Recover/Response (MTTR)	Ratio of implemented response per detection Time from alert to containment, and resolve	Evaluates efficiency, Measures operationalization, Measures execution
Feedback	Detection Validation Rate Response readiness validation	Ratio of tested total detections rules and response playbooks (Whole IR process)	Assessment of learning loop
Strategy	% Budget linked to risk priority % of aligned process % of integration & automations % of Covered Detection per Threat Profile & TTPs	Strategic alignment Continuous improvements,	Confirms governance effectiveness,

9 Industry Use Cases Samples

9.1 Cloud-Native FinTech

Vision:

- Reduce operational and systemic risk across critical payment services while maintaining availability and regulatory trust. (*Reduce Operation Risk of Payment services)

Strategy³⁶:

- Adopt a threat-informed detection and response strategy focused on a high-confidence APT threat profile targeting cloud-native FinTech payment ecosystems. Prioritize adversary behaviors that impact payment integrity and identity trust boundaries.

Example³⁷:

In the below table we consider most related APTs that potentially could target the service in this example.

Group Name	Nexus	Primary Objective	Key TTPs & Recent Activity
Lazarus Group	North Korea	Currency Generation	Targeted German crypto-exchanges and banks via AppleJeuS malware and trojanized DeFi apps.
Pulsar Kitten	Iran	Espionage / Influence	Observed in mid-2025 using credential phishing targeting German industrial and transportation hubs with links to finance.
APT28 (Fancy Bear)	Russia	Geopolitical Sabotage	Active in late 2024/2025 targeting German government-affiliated financial bodies to disrupt sanctions-related data.

36 Imagine this Banking service is Running in Europ, e.g Germany, then we can identify the potentail APT groups that targeting such and industry. Based on recent 2025 and early 2026 reports from CrowdStrike, Mandiant (Google Cloud), Trellix, and BaFin (Germany's financial regulator), the threat landscape for the German financial sector is dominated by a mix of state-sponsored APTs and highly organized eCrime groups.

Germany remains a top-tier target in Europe, suffering an estimated €267 billion in cybercrime-related losses in 2024, with that figure rising into 2025/2026.

37 Strategic MITRE ATT&CK Mapping

According to the CrowdStrike 2025 European Threat Landscape Report, adversaries targeting Germany have reached record-low "breakout times" (averaging 48 minutes).

Initial Access

T1566 (Phishing): Germany is the "phishing capital" of Europe. Recent reports highlight "Quishing" (QR Code Phishing) via physical mail or fake bank notifications.

T1190 (Exploit Public-Facing Application): Massive exploitation of perimeter devices like VPN appliances (Fortinet, Ivanti) and edge routers to bypass MFA.

T1195.002 (Supply Chain Compromise): A critical 2025 trend. BaFin reports that 67% of ICT incidents in German banking originated at third-party service providers rather than the banks themselves.

Persistence & Lateral Movement

T1078 (Valid Accounts): Use of Initial Access Brokers (IABs) to buy stolen credentials. Stolen credentials rose to the second most common entry vector in 2025.

T1021.001 (Remote Desktop Protocol): Groups like Akira and RansomHub frequently use RDP for movement after gaining a foothold via compromised VPNs.

Exfiltration & Impact

T1657 (Financial Theft): Focus on Instant Payment Regulation (IPR) vulnerabilities.

T1486 (Data Encrypted for Impact): While encryption is common, 2025 saw a pivot toward Data-Only Extortion (stealing data and threatening leak without encrypting files) to avoid EDR detection.

3. Critical Regional Trends (Germany Focus)

DORA Compliance (Jan 2025): The Digital Operational Resilience Act is now fully active. German banks are reporting a spike in "ICT incidents," largely due to the new mandatory reporting requirements for supply chain failures.

Violence-as-a-Service: A chilling trend noted by CrowdStrike in late 2025 involves hybrid adversaries (like Renaissance Spider) using Telegram to coordinate physical threats against bank employees or IT staff to force credential handovers.

AI-Driven Vishing: Voice phishing calls to German bank employees using deepfake audio of senior executives increased by over 400% in the last year.

Group Name	Nexus	Primary Objective	Key TTPs & Recent Activity
APT41	China	Espionage / Gain	Significant 113% increase in activity in Q1 2025; targets German financial IT supply chains to gain long-term persistence.
Scattered Spider	eCrime/Global	Financial Gain	Rapid exploitation of Okta/SSO; observed hitting European financial service providers with 24-hour "breakout" speeds.

Mapping APT & crime groups to Payment API abuse:

Actor Type	Likely API Focus
APT (espionage)	Silent access, monitoring transactions
FIN groups	Payment manipulation, laundering
Ransomware crews	Exfil + extortion via transaction data
Hacktivists	API DDoS, payment disruption

This is where APT TTPs + financial crime converge.

Crown Jewels³⁸:

- Payment APIs(public and internal),
- Identity Pipelines (authN/authZ, token issuance, session lifecycle),
- Transaction processing logic and settlement workflows,
- Supporting assets: CI/CD pipelines, cloud IAM roles,
- secrets management,
- serverless workloads,
- event streams.

Visibility³⁹:

38 It potentially includes any critical assets that serves business operations, so in more technical level we must consider more details: e.g. DNS, related Network Services, Related containers, related Operating Systems and Applications, etc.

39 Payment API attack surface (what attackers actually go after)

Typical components:

API Gateway (REST, GraphQL)

Auth layer (OAuth2, mTLS, JWT, API keys)

Backend payment service

Integration with core banking or PSP

External consumers (apps, partners, merchants)

This maps beautifully to MITRE ATT&CK.

MITRE ATT&CK alignment to a Payment API

Initial Access

What it looks like in payments

Stolen API keys

Compromised OAuth tokens

Exploited API endpoint logic

MITRE

T1078 – Valid Accounts

T1550 – Use of Authentication Material

T1190 – Exploit Public-Facing Application

Payment-specific signals

Token used from new ASN / country

Sudden jump in payment initiation calls

Missing mTLS on endpoints that usually have it

Execution / Abuse

What it looks like

Abuse of legitimate endpoints

Replay of signed requests

Parameter manipulation (amount, beneficiary)

- Threat modeling of payment and identity flows,
- Mapping to ATT&CK Cloud and Identity techniques
- Telemetry engineering: API gateway logs, serverless execution logs, IAM control-plane activity, token

Detection⁴⁰:

MITRE

T1204 – User Execution (API consumer acting “legit”)

T1059 – Command & Scripting Interpreter (if backend abused)

T1565 – Data Manipulation

Payment signals

Same token, multiple different beneficiaries

Amount just below approval threshold

Repeated failed + successful payment attempts

Persistence (very common, very dangerous)

What it looks like

Long-lived tokens

Rogue API clients registered

Backdoor OAuth apps

MITRE

T1098 – Account Manipulation

T1136 – Create Account

T1556 – Modify Authentication Process

Payment signals

New API client with broad scopes

Token lifetime suddenly extended

Auth flows bypassing normal refresh logic

Discovery

What it looks like

Enumerating endpoints

Probing limits, currencies, accounts

MITRE

T1087 – Account Discovery

T1046 – Network Service Discovery

Payment signals

High volume of 4xx responses

Sequential account or IBAN probing

OPTIONS / schema discovery abuse

Impact (this is where money moves)

What it looks like

Fraudulent payments

Liquidity drain

Regulatory breach

MITRE

T1657 – Financial Theft

T1485 – Data Destruction (cover tracks)

Payment signals

Sudden burst of high-value transfers

Payments outside customer behavior profile

Failures in downstream reconciliation

40 Detection engineering aligned to Payment API (very practical)

Core log sources you MUST have

API Gateway access logs

OAuth / IAM logs

Payment transaction logs

Backend service logs

WAF / bot protection logs

High-value detections

Token reuse across geographies

One token → many beneficiaries

- Privileged identity abuse and permission escalation
- API key misuse, token replay, anomalous API access
- Fraud patterns correlated with identity and API signals
- Persistence attempts via cloud configuration and identity layers,
- Characteristics: behavior-based, correlated, mapped to threat model and crown jewel risk.

Response:

- Scenario-specific playbooks aligned to crown jewels
- Automated IAM containment, session invalidation, credential revocation
- SOAR-driven fraud escalation with human decision gates for high-impact actions
- Evidence preservation and forensic readiness integrated into workflows

Sample Result: 60 % reduction in MTTR after six months, reduced blast radius for identity-related incidents, improved trust and resilience for payment services.

Note: This is a high level narrative to demonstrate the idea of the frameworks function in practice with an example. So just remember here we skipped all required details in this example and it is a high level demonstration of how to use the framework in practice. I skipped details in the example to make it simple and just demonstrate the usage concepts.

In short with knowing the main threat actors, and TTPs we can align out Threat modelling and prioritize the high risk Threat target our environment. As a result we can have high fidelity detection rules, a more meaningful usage of threat Intelligence for threat hunting and a high readiness for response and automation response.

Amount threshold evasion patterns
 API call rate $\neq$ historical baseline
 mTLS downgrade or missing client certs
 This is ATT&CK applied to money, not generic infra noise.

9.2 Hybrid Bank

Vision:

- Protect financial trust and service availability by minimizing operational disruption from cyber incidents across both digital and physical banking environments.

Strategy:

- Adopt a threat-informed, crown-jewel-driven security operations model focused on rapid containment of high-impact incidents rather than broad, alert-heavy monitoring.

Crown Jewels:

- ATM network and transaction processing
- SWIFT messaging infrastructure
- Online and mobile banking platforms

These assets were prioritized based on business impact, regulatory exposure, and systemic risk.

Threat Visibility:

Engineered unified telemetry across:

- Endpoints and servers in branch environments
- Core banking and SWIFT systems
- Cloud and hybrid digital banking platforms

Telemetry was normalized and correlated to support cross-environment attack visibility rather than siloed monitoring.

Threat Detection:

Detection engineering was aligned to realistic adversary behavior, with priority coverage for:

- Credential misuse and account takeover
- Lateral movement between branch and core systems
- Remote execution and persistence techniques

Detections were mapped to MITRE ATT&CK and tuned for high-fidelity, actionable signals against crown jewels.

Response:

Implemented a tiered incident response model:

- Central SOC coordination for threat triage and decision-making
- Branch-specific playbooks enabling localized containment actions
- Clear escalation paths for incidents affecting regulated systems (e.g., SWIFT)

Response workflows emphasized speed, consistency, and business context.

Continuous Improvement:

Post-incident reviews were used to:

- Refine crown jewel prioritization
- Improve detection logic and telemetry gaps
- Update playbooks based on real incident outcomes

Possible expected Outcome:

- Mean time to contain (MTTC) reduced by **45%**
- Improved consistency of response across regional branches
- Clear alignment between security operations and business risk

9.3 OT-Heavy Manufacturer

Context:

The organization is a large industrial manufacturer with mixed legacy and modern OT environments, including programmable logic controllers (PLCs), industrial HMIs, and segmented production networks. Business risk is dominated not by data loss, but by availability, safety, and production continuity. Even short disruptions can result in financial loss, contractual penalties, and safety incidents.

The organization operates under strict constraints: ^{SEP}no active scanning in OT, limited patching windows, and zero tolerance for response actions that could disrupt production processes.

Vision:

Ensure continuous and safe manufacturing operations by detecting and containing cyber threats targeting industrial control systems without impacting production availability or safety.

Security success was explicitly defined as preventing unplanned downtime, not maximizing alert volume or coverage metrics.

Strategy:

Adopt a threat-informed, availability-first security operations strategy focused on:

- Early detection of adversary activity targeting OT control logic and industrial protocols
- Passive visibility and behavioral detection rather than intrusive controls
- Response actions engineered to be manufacturing-safe, predictable, and reversible

The strategy intentionally avoided IT-centric SOC patterns and instead aligned detection and response design with industrial risk tolerance.

Crown Jewels:

Crown Jewels were identified through business impact analysis and operational dependency mapping:

- Production Controllers (PLCs, RTUs, Safety Controllers)^[1] Compromise could halt production lines or introduce unsafe operating conditions.
- Industrial Engineering Workstations and Logic Repositories^[1] Unauthorized modification of control logic posed long-term integrity and safety risks.
- R&D and Manufacturing Process Data^[1] Theft or manipulation could impact competitive advantage and product quality.

These assets were prioritized over peripheral IT systems, even when the latter generated more security events.

Threat Visibility (Telemetry Engineering):

Visibility was engineered outward from Crown Jewels using passive, non-intrusive methods:

- Passive OT network monitoring at key aggregation points
- Protocol-aware telemetry for:
 - o Modbus
 - o DNP3
 - o IEC-104 (where applicable)
- Asset behavior baselining for controllers and engineering stations
- Separation of IT and OT telemetry pipelines, with correlation at the analysis layer

No active probing, vulnerability scanning, or disruptive inspection was introduced into production zones.

Outputs included:

- OT Visibility Blueprint mapped to Crown Jewels
- Known-good behavioral baselines for control traffic
- Clear telemetry gaps documented and tracked over time

Threat Detection Engineering:

Detection was engineered around behavioral deviation, not signatures or generic alerts.

Priority detection logic included:

- Anomalous command sequences sent to controllers
- Unauthorized write operations to PLC memory or logic blocks
- Protocol misuse or deviation from established communication patterns
- Engineering workstation activity outside approved maintenance windows
- Lateral movement attempts between IT and OT boundary zones

Detections were:

- Explicitly mapped to realistic OT threat scenarios
- Tuned for high confidence, even at the cost of lower coverage
- Designed to minimize false positives that could trigger unnecessary operational intervention

Detection validation relied on tabletop simulations and controlled engineering tests rather than live production testing.

Response (Manufacturing-Safe Execution):

Response workflows were engineered with availability and safety as non-negotiable constraints.

Key principles:

- No automated containment actions directly affecting controllers
- Segmentation-based containment at network boundaries
- Human-in-the-loop decision points for any action impacting production systems

- Clear coordination with OT engineers and plant operators

Response playbooks included:

- Controlled isolation of affected network segments
- Credential and access revocation for compromised engineering workstations
- Evidence preservation without system shutdown
- Safe rollback procedures aligned with maintenance windows

Response success was measured by containment without disruption, not speed alone.

Continuous Improvement (Kaizen Loop):

Each incident, anomaly, or near-miss fed a structured learning loop:

- Refinement of behavioral baselines
- Adjustment of detection thresholds
- Updates to response playbooks based on operational feedback
- Periodic validation exercises with OT and engineering teams

Continuous improvement focused on small, safe increments, avoiding disruptive changes to stable production environments.

Outcome:

After two years of operating under the UTIOM lifecycle:

- Zero unplanned production downtime caused by cyber incidents
- Improved confidence and trust between security, OT engineers, and operations
- High-fidelity detections with minimal alert fatigue
- Clear executive visibility into operational cyber risk

Most importantly, security operations were perceived as an enabler of resilience, not a threat to manufacturing stability.

Key Takeaway:

In OT environments, security operations succeed not by reacting faster, but by designing systems that respect operational reality. UTIOM enabled the organization to unify threat-informed detection, engineering discipline, and manufacturing-safe response into a single, coherent operating model.

9.4 Final example to review: Threat-Informed Operations Using Vendor Intelligence

Context:

A financial services organization operates a hybrid environment spanning on-prem core banking systems, cloud-based digital channels, and SaaS platforms. The SOC consumes multiple threat intelligence feeds but historically struggled to translate reports into actionable detection and response improvements.

A recent CrowdStrike / Mandiant / Microsoft threat intelligence report highlights increased activity by financially motivated and state-aligned actors abusing:

- Valid credentials
- Identity federation misconfigurations
- Lateral movement via remote management tooling
- Persistence through cloud and identity abuse

Rather than treating the report as “informational,” the organization applies UTIOM to operationalize it.

Vision:

Ensure continued availability and trust of digital banking services by detecting and containing identity-centric intrusions before they impact regulated systems or customers.

Success is defined not by alert volume, but by time-to-detect identity abuse affecting crown jewels.

Strategy:

Based on the report, leadership agrees to:

- Prioritize identity and access abuse over malware-centric threats
- Focus detection and response effort on pre-impact attacker behavior
- Accept reduced coverage elsewhere to improve depth around critical services

This strategy explicitly deprioritizes low-risk alerts and reallocates effort toward high-impact identity attack paths.

Crown Jewels:

Using the framework, the SOC identifies:

- Cloud identity provider (IdP) and admin roles
- Online banking authentication flows
- Privileged access to payment and settlement systems

These are mapped as blast-radius amplifiers if compromised.

Threat Modeling:

The intelligence report is translated into **explicit threat models**, not narratives.

For each relevant adversary objective, **attack trees** are constructed starting from the crown jewels and expanding outward across identity, SaaS, cloud, and hybrid trust boundaries.

For the given scenario, threat modeling explores paths such as:

- Compromise of SaaS administrator accounts via phishing, MFA fatigue, or token theft
- Abuse of identity federation or trust relationships to pivot into cloud workloads
- Lateral movement from user context to privileged service and automation accounts
- Persistence through conditional access bypass, token replay, or role re-assignment

Each attack tree is analyzed to determine:

- Where controls already exist and are effective
- Where partial protection exists but is bypassable
- Where visibility is missing or insufficient
- Where detection or response would be too late to limit impact

Threat scenarios are then mapped to specific MITRE ATT&CK techniques, expected telemetry, and decision points. This produces detection stories and visibility requirements, not alerts.

The output of this stage is a coverage map that explicitly shows:

- Protected paths
- Observable paths
- Blind spots
- High-risk paths with unacceptable blast radius

This coverage map directly drives Threat Visibility Engineering, ensuring telemetry, logging, and evidence pipelines are designed to observe the highest-risk attack paths before incidents occur.

Threat Visibility Engineering:

The SOC reviews whether required evidence exists for the modeled scenarios:

- Authentication logs with token metadata
- Conditional access decision logs
- Admin API usage telemetry
- Identity role assignment changes

Gaps are identified, and telemetry pipelines are adjusted before any incident occurs.

Deception elements are added:

- Canary admin accounts
- Honeytokens embedded in privileged SaaS workflows

Threat Detection Engineering:

Detection engineers implement analytics aligned to the modeled behavior:

- Anomalous token usage across regions and services
- Privilege escalation following suspicious authentication patterns
- Admin API usage outside normal change windows

Purple team exercises emulate the reported attack paths to validate:

- Telemetry completeness
- Detection timing
- Analyst decision quality

Failed detections are treated as engineering defects, not analyst mistakes.

Threat Detection Operations:

When detections trigger:

- Alerts are enriched with crown jewel context
- Analysts assess impact, not just severity
- Identity timelines are built to confirm attacker intent

Low-context alerts are suppressed by design.

Response:

Playbooks derived from strategy are executed:

- Immediate session invalidation and token revocation
- Privilege rollback and access isolation
- Targeted communication with identity and business owners

Response authority is clear, and containment is scoped to protect critical services without unnecessary disruption.

Resilience:

Before services are fully restored:

- Identity trust relationships are reviewed
- Conditional access policies are tightened
- Detection coverage is revalidated

Restoration is gated on risk reduction, not just system uptime.

Continuous Improvement:

Post-incident or post-exercise reviews feed back into:

- Threat models (new variations observed)
- Detection logic (false positives, missed signals)
- Strategy (shift in adversary focus confirmed)

Metrics are updated to reflect real operational readiness, not tool performance.

Outcome:

- Faster detection of identity abuse
- Reduced analyst noise
- Clear linkage between threat intelligence and SOC action
- Demonstrable improvement in containment time for high-impact scenarios

Threat intelligence is no longer “read and forgotten”, it becomes an input to a living operational system.

10 Outcomes and Benefits

- End-to-end traceability from strategic vision to technical execution.
- Threat-informed detection capabilities that are engineered, not assumed.
- Alignment of SOC metrics with executive expectations.
- Reduced operational noise and higher signal quality.
- A living maturity roadmap that improves itself each cycle.
- Product design and product ownership
- Economic constraints
- UTIOM operates on multiple timelines:
 - o Strategic (months / years)
 - o Operational (days / weeks)
 - o Incident (minutes / hours)

11 Community and Governance

UTIOM is an open, living framework licensed under Creative Commons BY-SA 4.0. intended to evolve through transparent sharing and peer review.

Open Resources

- GitHub Repository documentation, examples, toolkit.
- Notion and Excel Dashboards self-assessment and scoring.
- Quarterly Kaizen Sessions community review and benchmark updates.

“Frameworks mature when communities learn together.”

12 Alignment with NIST Cybersecurity Framework (NIST CSF)

UTIOM aligns naturally with the NIST Cybersecurity Framework by providing an **operational execution layer** across all six CSF 2.0 Functions — GOVERN, IDENTIFY, PROTECT, DETECT, RESPOND and RECOVER. The crosswalk lists UTIOM's primary direct category relationships; Protect outcomes are driven through Strategy, Crown Jewels, architecture and preventive controls rather than a single mapped domain. NIST CSF 2.0 defines outcomes. UTIOM defines the operating model that delivers them.

- **Govern**
UTIOM Vision and Strategy establish the risk appetite, roles and policy direction that CSF 2.0 places under GOVERN, and make them operational controls rather than statements.
- **Identify**
UTIOM Vision, Strategy, and Crown Jewels directly support asset prioritization, risk understanding, and business context definition.
- **Protect**
Strategy-driven controls and telemetry engineering inform preventive measures aligned to prioritized assets.
- **Detect**
Threat Visibility and Threat Detection stages operationalize CSF detection outcomes through threat-informed analytics mapped to real adversary behavior.
- **Respond**
UTIOM Response formalizes coordinated, playbook-driven incident handling consistent with CSF response planning and execution objectives.
- **Recover**
Continuous Improvement ensures lessons learned are translated into improved posture, resilience, and operational readiness.

Key Differentiator:

While NIST CSF defines *what* good cybersecurity looks like, UTIOM defines *how to operationalize it inside a modern SOC*.

12.1 Alignment with NIST Cybersecurity Framework 2.0 (CSF 2.0)

NIST CSF 2.0 introduces GOVERN as a first-class function, emphasizing strategy, risk ownership, accountability, and outcomes. UTIOM naturally operationalizes this shift by embedding governance and decision-making directly into security operations.

GOVERN

UTIOM Vision and Strategy directly align with CSF 2.0's Govern function by:

- Defining security objectives based on business outcomes
- Establishing risk ownership through Crown Jewels identification
- Translating executive intent into operational priorities

UTIOM ensures governance is not a static policy layer but an active driver of operational behavior.

IDENTIFY

UTIOM's Crown Jewels stage fulfills CSF 2.0 Identify outcomes by:

- Prioritizing critical assets, services, and data
- Linking assets to business impact and systemic risk
- Establishing threat-informed risk context

This shifts identification from asset inventories to business-critical focus.

PROTECT

UTIOM Strategy influences Protect outcomes by:

- Guiding preventive controls toward prioritized assets
- Informing architectural decisions using threat and risk context
- Avoiding uniform control application in favor of risk-weighted protection

Protection becomes intentional and risk-driven, not checkbox-based.

DETECT

UTIOM Threat Visibility and Threat Detection directly operationalize Detect by:

- Engineering telemetry based on realistic adversary behavior
- Aligning detections to MITRE ATT&CK techniques
- Focusing on high-fidelity signals affecting Crown Jewels

Detection is treated as an engineering discipline, not alert accumulation.

RESPOND

UTIOM Response maps cleanly to CSF 2.0 Respond by:

- Enabling coordinated, role-aware response workflows
- Supporting tiered escalation and decision-making
- Embedding playbooks aligned with business and regulatory impact

Response is consistent, measurable, and context-aware.

RECOVER

UTIOM Continuous Improvement aligns with Recover by:

- Feeding incident outcomes back into strategy and detection
- Improving resilience through learning loops
- Reducing recurrence and systemic weakness

Recovery is not just restoration, but evolution of capability.

Key Insight :

NIST CSF 2.0 defines outcomes. UTIOM defines the operating model that delivers them.

13 Alignment with SOC Capability Maturity Models (SOC-CMM)

UTIOM is designed to accelerate SOC maturity progression by structuring operations around outcomes rather than tools or team silos.

- Lower maturity SOC's benefit from UTIOM's clear lifecycle and prioritization logic, reducing alert fatigue and operational chaos.
- Higher maturity SOC's leverage UTIOM to:
 - Integrate threat intelligence into detection engineering
 - Shift from reactive alerting to proactive, threat-informed operations
 - Institutionalize continuous improvement loops

UTIOM acts as a practical operating model that enables SOC-CMM capability growth across:

- People (roles, decision authority, skills)
- Process (repeatable, measurable workflows)
- Technology (telemetry, detection, automation)
- Governance (metrics, feedback, improvement)

Key Differentiator:

SOC-CMM measures *how mature a SOC is*; UTIOM provides the mechanism to become mature.

14 Alignment with the Digital Operational Resilience Act (DORA)

UTIOM directly supports DORA's objectives by embedding operational resilience into day-to-day security operations.

- ICT Risk Management
Crown Jewels and threat-informed Strategy focus risk management efforts on systems critical to financial stability.
- Incident Detection and Response
Threat Visibility and Detection improve early identification of systemic risks and significant incidents, enabling faster containment.

- Incident Classification and Reporting
Tiered Response and structured playbooks support consistent incident classification, escalation, and regulatory reporting.
- Operational Resilience and Learning
Continuous Improvement ensures operational lessons are captured and translated into improved resilience and preparedness.

Digital Operational Resilience Testing

Articles 24–25 require a risk-based digital operational resilience testing programme covering ICT systems supporting critical or important functions. Article 26 additionally requires advanced testing by means of threat-led penetration testing (TLPT) for financial entities identified under the criteria in Commission Delegated Regulation (EU) 2025/1190. These are not the same obligation: the first applies broadly, the second only to identified entities. UTIOM’s purple-team validation and detection effectuality records provide operational evidence supporting both, without determining which applies.

Key Differentiator:

DORA mandates resilience; UTIOM operationalizes resilience through measurable, repeatable security operations aligned to real threats.

UTIOM does not replace standards or regulations. It connects them to reality.

15 Conclusion

UTIOM is a unifying language for modern defence strategic in vision, engineering in method, and human in execution. It translates intent into architecture and architecture into learning. Whether implemented in a global SOC or a two-person cloud team, the principles remain the same: define purpose, engineer detection, and learn continuously.

“UTIOM is not a just another process; it is a language that unites defenders.”

UTIOM is a new approach to unified separated, siloed teams and process all into one practical and unified methodology.

“UTIOM assumes clear ownership of the security operations lifecycle, similar to product ownership in engineering organizations. Role of Security Operation Lead.”

Security Operations as a Product:

UTIOM deliberately treats Security Operations and Incident Response as a product rather than a static function or reactive service. Like any well-designed product, a SOC must have a clear vision, an evolving strategy, engineered features, measurable outcomes, and continuous feedback from real-world usage. This mindset shifts the focus from operating tools and managing alerts to delivering consistent risk reduction, resilience, and business value. In UTIOM, improvement is not an initiative; it is the product lifecycle itself.

Security operations will not mature by adding more tools.

They mature when treated as a system, designed with intent, and improved deliberately.

16 The Framework Family

UTIOM is the operating model. Two capability maturity models measure its pillars in depth, and both rest on the same premise: everything a security operations function does is incident response.

The modules do not fill gaps in UTIOM. They add measurement depth. UTIOM defines how security operations should work; a module tells you, with evidence, how well one part of it actually works in your organisation.

UTIOM. The operating model. How should the whole security operation be designed and run? Version 1.2, with four assessment instruments.

TID-CMM. The detection module. Would we actually see the adversaries most likely to attack us? Published at tid-cmm.com. Eight domains, 58 sub-capabilities, aligned to MITRE ATT&CK Enterprise and crosswalked to NIST CSF 2.0 and SOC-CMM.

TIR-CMM. The response module. Could we stop it, inside the breakout window, with the authority to act? Published at tir-cmm.com. Introduces the Containment Lattice and the Containment Margin metric, and measures decision latency separately rather than folding it into MTTR.

RSMM. The Realistic SIEM Maturity Model. Is the SIEM a security tool or expensive log storage? Five levels from Blame Collector to Outcome-Driven SIEM.

STRATA. The organisational model. Strategy, Talent, Resilience, Automation, Telemetry and Adaptability, replacing the People, Process and Technology triad.

16.1 How UTIOM produces what the modules measure

- Crown Jewels produces the asset registry and threat models that TID-CMM uses to derive its in-scope ATT&CK set.
- Strategy produces the documented adversary profile that TID-CMM's threat intelligence domain scores.
- Threat Visibility produces the telemetry blueprint and accepted gap report that its telemetry assurance computation consumes.
- Threat Detection produces the version-controlled, tested, traceable content its detection engineering domain measures.
- Validation produces the emulation evidence its adversarial validation domain requires.
- Response and Continuous Improvement produce the containment authority, rehearsed playbooks and feedback loops that TIR-CMM measures.

The order matters. TID-CMM and TIR-CMM measure depth in one pillar each. UTIOM decides what that pillar should be pointed at.

17 The Response Horizon

Ask a SOC manager when incident response begins and most will say: when something is detected. That answer is the reason so many security operations struggle.

By the time an alert fires, almost every decision that determines the outcome has already been made. Whether the right telemetry exists. Whether the detection was tuned for this environment. Whether a playbook exists for this asset. Whether anyone knows who can authorise isolating a production system at two in the morning.

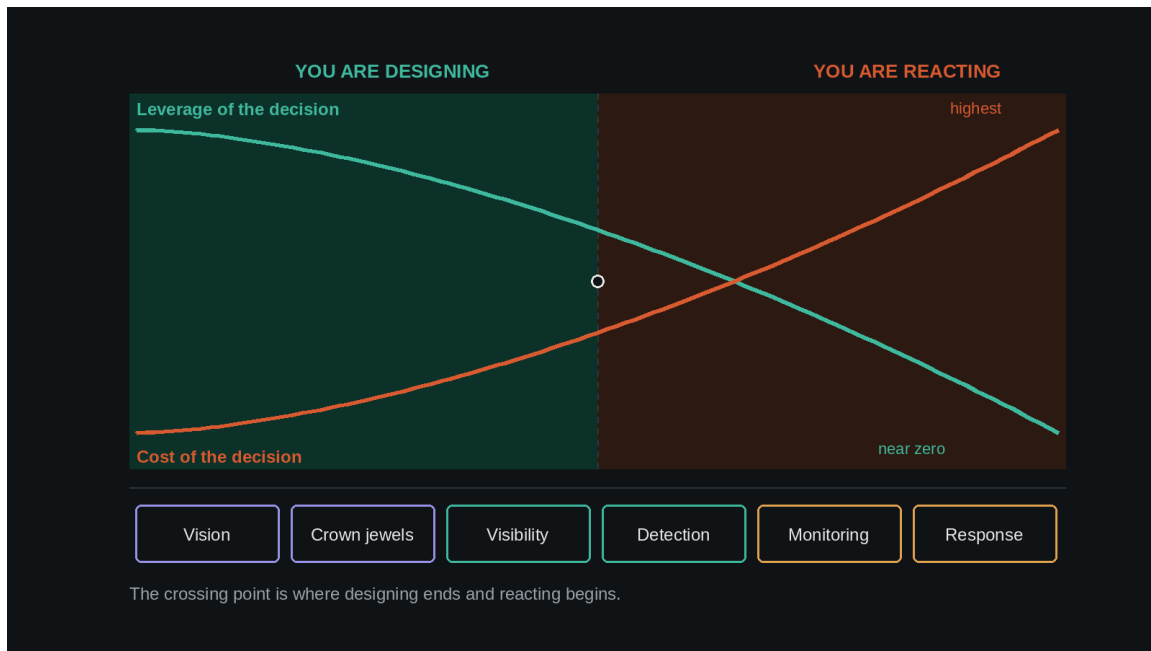


Figure 2. The Response Horizon. Leverage falls and cost rises as the moment of impact approaches. The crossing point separates designing from reacting.

17.1 Two curves

Leverage falls. A decision about which assets are critical, made during strategy work, shapes every detection rule and playbook that follows. The same question asked mid-incident buys almost nothing.

Cost rises. Designing telemetry coverage for an identity attack path is a planning exercise. Discovering during an intrusion that the logs were never enabled is a forensic dead end with regulatory consequences.

Most organisations live to the right of the crossing point and describe it as being busy.

17.2 Move decisions left

For each recurring incident type, identify the decisions currently made under pressure and ask which could be made in advance. Containment authority. Isolation thresholds. Business impact tiers. Evidence preservation requirements. Every one moved left is minutes recovered and errors avoided.

18 Design and Validation: the UTIOM V-Model

Every design decision in UTIOM carries a matching activity that proves it. Drawn as a V, the left arm descends through design and intent, the base is detection engineering, and the right arm ascends through validation and operation.

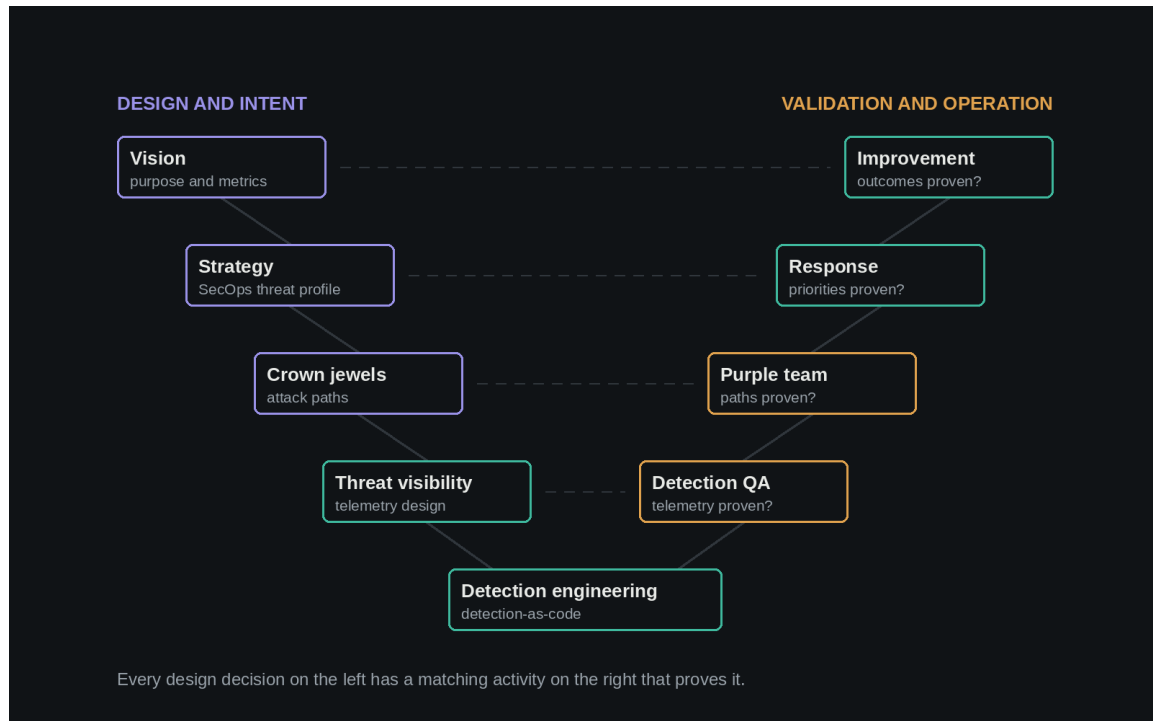


Figure 3. The UTIOM V-Model. Read across any row: purple team exercises prove the attack paths were real, detection QA proves the telemetry delivers, response outcomes prove the threat profile chose the right adversaries.

Strip away the right arm and the left arm is unverified assumption. This pairing is what separates a documented framework from a demonstrated capability, This pairing provides operational evidence supporting the NIS2 Article 21(2)(f) effectiveness-assessment requirement; UTIOM is an operational method for supporting that requirement, not a mechanism prescribed by NIS2.

19 Traditional SOC Operating Model Compared with UTIOM

The difference is not tooling. Both models can run the same platforms. The difference is what drives the work, what counts as success, and where the decisions that determine an outcome actually get made.

What triggers work. An alert fires and the queue sets the agenda, against a threat profile and crown jewel registry setting the agenda.

How priorities are set. Alert severity or whoever escalated loudest, against business consequence.

Where strategy sits. A document referenced at audit, against an operational control driving what gets built and in what order.

Where incident response sits. A downstream phase activated when something goes wrong, against the operating mode of which all other functions are expressions.

How detection is built. Vendor content enabled and tuned reactively, against detection engineered from threat models with every rule traceable.

What visibility means. Whatever the platform ingests, against a design decision with gaps documented and formally accepted.

How response is prepared. A generic plan rarely exercised, against pre-engineered playbooks with authority defined in advance.

What gets measured. Volume of alerts and tickets, against risk reduction measured by coverage per threat modelled and containment margin.

How validation happens. Occasionally as a penetration test, against continuous validation where failed detections are engineering defects.

How improvement happens. After a major incident, against an embedded feedback loop producing engineering change.

Relationship to standards. Compliance treated as the objective, against standards operationalised and validated against real adversary behaviour.

19.1 What is genuinely new in UTIOM

Incident response as the operating mode. Not a phase activated by alerts, but the state security operations are always in, at varying intensity.

Design paired with validation. Every design decision carries a matching activity that proves it.

Crown jewels as the universal anchor. The reference point every downstream decision traces to.

Staged maturity that refuses to flatter. A level counts only when every criterion below it is satisfied.

Security operations as a living product. Owned, versioned, measured and continuously improved.

WHY UTIOM IS DIFFERENT

I. It Starts With Management, Not Tools

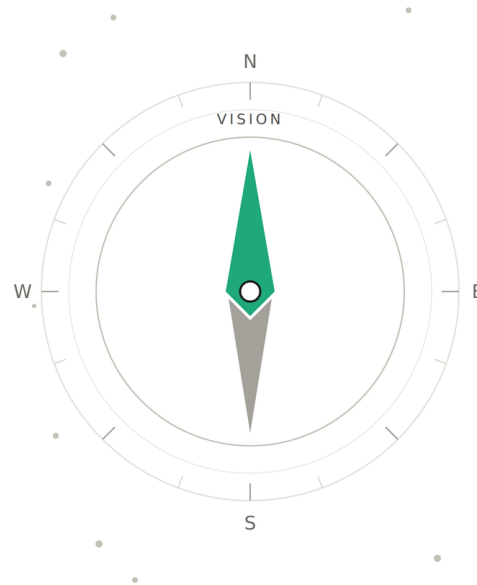
This chapter opens a three-part section on what distinguishes UTIOM from conventional security operations frameworks: its management foundation, its engineering discipline, and its treatment of response as the operating mode itself.

WHY UTIOM IS DIFFERENT · PART 1

Management, not tools.

"The compass defines direction; tools merely execute it."

UTIOM — UNIFIED THREAT-INFORMED OPERATIONS MODEL



Ask a struggling SOC what it needs, and you will hear a list of tools. A better SIEM. More automation. Another threat intelligence feed. Ask the same SOC what its purpose is, and the room goes quiet.

That silence is the problem UTIOM was built to solve. And it explains the first thing that makes UTIOM different from conventional security operations frameworks: it does not begin with technology, compliance, or even threats. It begins with management science.

Most security frameworks descend from audit. They inherit the audit worldview: controls, checklists, evidence, certification. UTIOM descends from a different lineage — Peter Drucker, Henry Mintzberg, W. Edwards Deming, John Boyd, Dieter Rams, Sun Tzu. Not one of them worked in cybersecurity. All of them solved the problem security operations actually has.

From management science to doctrine

Six bodies of thought, translated into one operating model — and made enforceable as seven laws.

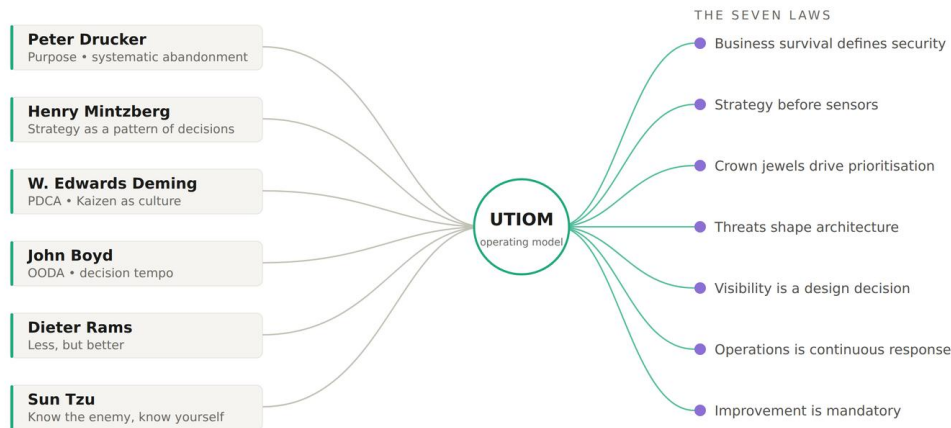


Figure — Six thinkers, none of them in security, translated into enforceable doctrine.

Because here is the uncomfortable truth this framework is built on: most SOC failures are management failures wearing technical costumes. Alert fatigue is not a staffing problem. Detection sprawl is not a content problem. Improvised response is not a skills problem. They are the predictable output of operations that were assembled instead of designed. This chapter shows how each principle was translated — and why being loyal to them changes what a SOC becomes.

Drucker: Without a Purpose, There Is No Management

Drucker's most quoted insight is also his most ignored in security: *"Without a purpose, there is no management."*

UTIOM takes this literally. Vision is not a poster or a mission statement — it is the **first operational control** in the lifecycle. Before a single log source is onboarded, the organization must be able to answer why the SOC exists, what it protects, and what success looks like in terms of business survival. Every downstream decision — telemetry, detection, response — inherits either that clarity or that ambiguity.

The doctrine states it bluntly: **a SOC without a vision is an alert factory**. The compass defines direction; tools merely execute it.

Drucker gives UTIOM three more gifts that almost no security framework has absorbed:

Systematic abandonment. *"If you want something new, you must stop doing something old."* In UTIOM, every improvement cycle must retire detection rules that no longer protect crown jewels. Detection libraries are treated as perishable inventory, not accumulated wealth. Rule count is not a metric of strength — sometimes it is a metric of neglect.

Knowledge workers. Analysts are autonomous specialists, not tool operators. A framework that measures them by tickets closed misunderstands what they are for.

Effectiveness over efficiency. Doing the right things beats doing things right. A SOC can be brutally efficient at triaging alerts that never mattered.

Mintzberg: Strategy Is a Pattern, Not a Document

Henry Mintzberg defined strategy as *"a pattern in a stream of decisions."* Not an annual PowerPoint. Not a shelf document reviewed once a year and disconnected from execution. UTIOM operationalizes this: your real strategy is visible in what you build, what you sequence, and what you decline — week after week. If the strategy document says "threat-informed defense" but the stream of decisions says "whatever the vendor shipped this quarter," then the vendor is your strategist.

This is why UTIOM embeds strategy as a daily operational control rather than a leadership ritual. Governance and operations belong in the same place. Strategy and execution must be traceable as two ends of the same thread.

Deming: Improvement Is Not a Phase, It's a Culture

From Deming and the Toyota Production System, UTIOM takes the Plan-Do-Check-Act cycle and Kaizen — and refuses to treat them as ceremony.

Continuous Improvement is a full lifecycle domain in UTIOM, with the same standing as Detection or Response. Every incident ends in a Kaizen review. Every purple team exercise feeds the threat model. Every failed detection is an engineering defect with an owner and a date — not a lesson filed and forgotten.

The phrasing in this framework is deliberate: *"Improvement is not a phase; it's a culture."* And its consequence is measurable: small, consistent changes compound better than periodic overhauls. No design remains optimal forever, so a SOC that is not learning is decaying — quietly, and on schedule.

"Learning is the final deliverable of every incident."

Boyd: The Adversary Sets the Tempo

John Boyd's OODA loop — observe, orient, decide, act — was born in air combat, where the pilot with the faster decision cycle imposes the terms of the fight.

UTIOM applies this without dilution. Response is measured against adversary breakout time, not against internal SLAs alone. Decision latency is tracked separately from MTTR, because the two hide different failures: a team can respond quickly and still decide slowly.

This is also where one of UTIOM's structural ideas comes from — moving decisions left.

Containment authority, isolation thresholds, business impact tiers: decided at design time, in daylight, not improvised at 3 a.m. during an incident. Decisions that should be made at design time otherwise get made during incidents instead — at the exact moment leverage is lowest and cost is highest.

Rams: Less, but Better

Dieter Rams designed radios and shelving, and his tenth principle — *"Good design is as little design as possible"* — may be the most subversive idea UTIOM imports.

In UTIOM, analyst attention is a scarce engineered resource. Signal-to-noise ratio is a design specification. Alert fatigue is classified as a **system design failure**, not an HR issue to be solved with hiring or resilience training.

This is the minimalism of defense: less, but better. Well-designed security operations are not loud. They are deliberate, predictable, and boring — and boring, in this discipline, is a compliment earned through engineering.

Sun Tzu: Know the Enemy and Know Yourself

The oldest principle in the stack is the one most organizations fail on the second half of: *"Know the enemy and know yourself."*

Modern threat intelligence has made knowing the enemy almost fashionable. Knowing yourself — a real crown jewel registry, an honest maturity assessment, documented visibility gaps formally accepted rather than discovered mid-incident — remains rare. UTIOM makes both mandatory, and makes crown jewels the universal anchor: telemetry, detection, playbooks, and budget all trace back to what actually keeps the organization alive.

No organization can protect everything equally. Pretending otherwise is not ambition; it is the absence of prioritization.

Why This Foundation Matters

Put these principles together and something changes in kind, not degree. Security operations stop being a cost center that reacts to noise and become a **living, engineered system — a product** with a vision, a strategy, engineered features, measurable outcomes, and continuous feedback.

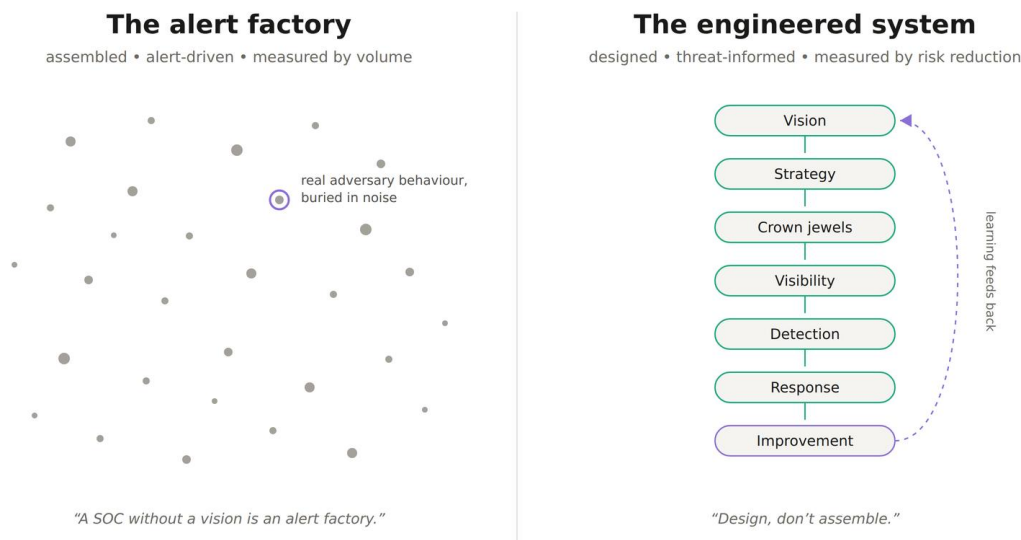


Figure — The difference vision makes: an alert factory, or a system with a purpose.

This is the root of every other difference UTIOM has. The seven laws of its doctrine — business survival defines security, strategy before sensors, crown jewels drive prioritization, and the rest — are not arbitrary rules. They are what Drucker, Mintzberg, Deming, Boyd, Rams, and Sun Tzu sound like when translated into security operations and made enforceable.

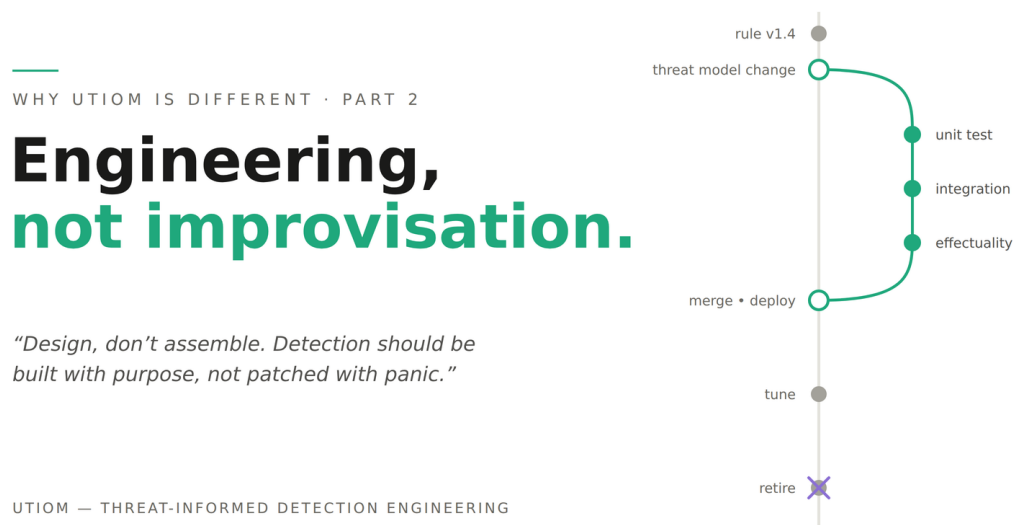
Frameworks that start from audit produce organizations that pass audits. Frameworks that start from tools produce organizations that operate tools. UTIOM starts from management — and produces organizations that can explain, in business language, why every detection exists, why every euro was spent, and why the SOC deserves to exist at all.

"Security operations will not mature by adding more tools. They mature when treated as a system, designed with intent, and improved deliberately."

That is the first difference. It is also the one that makes all the others possible. The next chapter follows this foundation into the detection layer, where management principle becomes engineering discipline.

II. Detection Is Engineering, Not Improvisation

This is the second chapter in a three-part section on what distinguishes UTIOM from conventional security operations frameworks. The first made the case that UTIOM starts from management science, not tools. This one shows where that foundation becomes concrete: the detection layer, and the measurement model that keeps it honest.



In Part 1, I argued that most SOC failures are management failures wearing technical costumes. Fair question in response: fine — but management principles don't catch adversaries. Detections do. So what does UTIOM actually change about how detection gets built? Start with a sentence from TID-CMM, the detection maturity model inside the UTIOM family, because it describes the industry's open secret better than any statistic:

"A rule that has never fired on a true positive, running on a log source that stopped reporting six weeks ago, mapped to a technique your adversaries do not use, counts exactly the same as a detection proven to catch a real intrusion in minutes."

That is how most organizations count detection today. Rule count as strength. Matrix coverage as capability. Dashboards as evidence. UTIOM's answer is a single reframing that the book states as doctrine:

"Detection becomes engineering, not improvisation."

Engineering means requirements, tests, pipelines, failure modes, maintenance, retirement — and measurement that refuses to flatter. Here is what that looks like, and why so few frameworks demand it.

Three Ways SOCs Lie to Themselves

TID-CMM was built to expose three endemic problems, and they are worth naming before any solution, because every one of them produces a green dashboard:

ATT&CK, a serious threat-modeling pass typically leaves 150–250 that matter to a given organization. Detection sprawl is impossible by construction, because a rule with no ancestor in that chain has no right to exist — and a backlog scoped to what is real is a backlog a team can actually finish.

Every detection has an ancestor

The traceability cascade: a rule with no line back to a crown jewel has no right to exist.

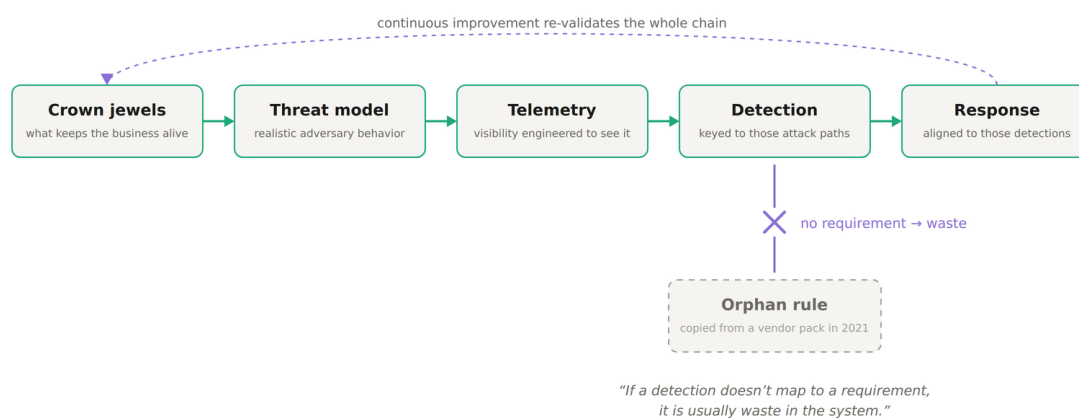


Figure — Detection traceability from crown jewels to validated response.

Visibility Comes First — and Some Gaps Are Physics

Before UTIOM lets you write a single rule, it makes you answer an uncomfortable question: would you even see the behavior you want to detect?

"You can't build meaningful visibility without knowing what deserves to be seen."

The Threat Visibility domain does the unglamorous work most frameworks skip: mapping ATT&CK tactics and threat models to actual data sources, defining logging and retention standards, enforcing data quality and normalization, placing deception aligned to crown jewels. Its output — a visibility blueprint and gap report — is the *input* to detection engineering. The book calls visibility the bloodstream of detection, and the metaphor is exact: rules built on telemetry you don't reliably collect are decoration.

TID-CMM makes this brutally concrete. TID-CMM analysis of ATT&CK v19.2 finds that 423 Windows techniques — 89 percent — reference Sysmon-class telemetry. If that telemetry, or its EDR equivalent, is absent, then in TID-CMM's words: *"that is not a gap in your rule set. It is a gap in physics."* No amount of detection engineering fixes physics. The model computes which techniques your actual log sources can support, bands them — assured, partial, weak, blind — and ranks which telemetry to enable next by how many blind techniques it unblocks. *"Detection is bounded by visibility, and that is now measurable."*

And where a gap remains, UTIOM demands it be documented and formally accepted. A blind spot you chose is a risk decision. A blind spot you discover mid-incident is a design failure.

Detection-as-Code: The Software Discipline, Uncut

UTIOM mirrors modern software practice in full, not as a buzzword:

Version control. Every rule's lineage and purpose is traceable — who built it, against which threat, changed when, and why.

CI/CD pipelines. Detections deploy, validate, and roll back safely, in managed release cycles instead of hand-edits in a production console.

DRY — Don't Repeat Yourself. The exclusion list pasted into fifty rules is maintenance debt with a countdown timer. Shared logic moves into shared objects, once.

Abstraction layers. This one quietly protects years of work. In the book's words: *"Your detection logic should not care if the data comes from CrowdStrike, SentinelOne, or Sysmon. The logic should sit on top of a standardized schema."* When the EDR contract changes — and it will — your detection capital survives the migration.

Three tiers of testing. Unit tests validate a single rule against isolated log snippets. Integration tests confirm it plays correctly with alerting pipelines and SOAR playbooks. Effectuality tests answer the only question leadership cares about: does it actually fire when the real behavior happens? A rule that has never been tested against a simulated adversary is not a detection. It is a hypothesis.

Three tiers of testing

A rule that has never been tested against a simulated adversary is not a detection. It is a hypothesis.

Every tier is a CI/CD gate: fail it, and the rule never reaches production.
Automated regression testing re-runs all three on every change.

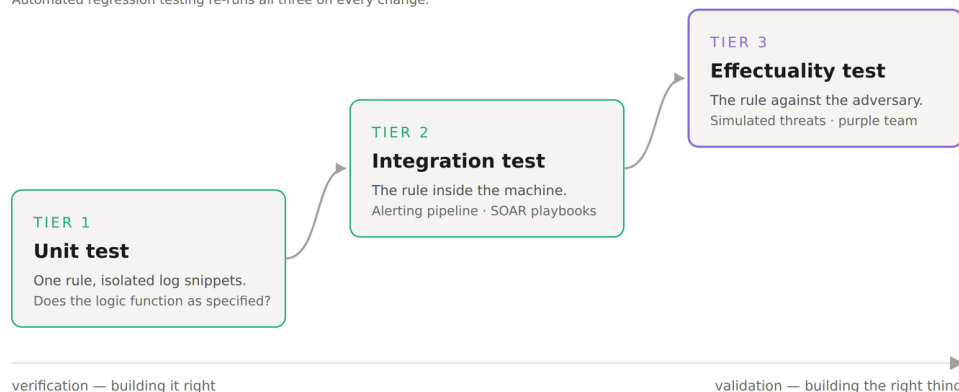


Figure — A rule untested against a real adversary is a hypothesis, not a detection.

Behaviors Outlive Indicators

UTIOM also takes a position on what a detection should be made of:

"Detection built from behaviours lasts longer than detection built from indicators."

A hash, a domain, an IP — the adversary discards these between breakfast and lunch. A behavior — anomalous command sequences, unauthorized write operations, protocol misuse, impossible token usage across regions — persists as long as the tactic itself persists. The book's OT manufacturing case study builds its entire detection layer this way: behavioral signals around what must never happen to the process, not fingerprints of last month's malware.

Indicators still have a place. They are just not the foundation. Foundations are supposed to last.

The Detection You Retire Is as Important as the One You Build

Here Part 1's Drucker returns, wearing an engineer's badge. Systematic abandonment — "*if you want something new, you must stop doing something old*" — is a core engineering discipline in UTIOM, not a spring-cleaning ritual. Every improvement cycle prunes rules that no longer protect crown jewels and telemetry that no longer feeds a detection. The book's warning is vivid: without deliberate pruning, the SOC becomes a *factory of data*.

Ask a SOC how many detections it has and it will answer proudly. Ask how many it retired last quarter and you learn whether it is engineering or hoarding.

Assume Components Fail

Real engineering disciplines design for failure, and UTIOM is unusual among security frameworks in demanding the same of detection: **redundant visibility paths**, so identity and network telemetry carry the load when the endpoint sensor is bypassed; **backpressure and circuit breakers**, so a noisy day doesn't silently drop the telemetry that mattered; and **meta-detections** — detections that watch detection itself: a critical log source going quiet, ingestion latency breaching its SLA, a pipeline stage failing.

The most dangerous outage in security operations is the one that produces no alert — the silent visibility failure that turns your SIEM into a confident liar. Remember the rule from TID-CMM's opening line: it had stopped reporting *six weeks ago*, and nobody noticed. Meta-detections exist so that sentence can never be written about you.

The Analyst Is Part of the System

UTIOM extends engineering discipline to the point where most frameworks stop: the human reading the alert.

Every alert, regardless of source tool, follows the same hierarchy: **what happened, why it matters, and what the first step to fix it is**. Signal-to-noise ratio is optimized deliberately, through grouping and narrative incidents rather than raw event streams. And alert fatigue is classified — in writing, as doctrine — as a system design failure, never an HR issue.

That classification changes who is accountable. When analysts burn out, the question is no longer "why can't they keep up?" but "which engineer let this noise into the pipeline?" Dieter Rams' minimalism, imported in Part 1, does its hardest work here: every alert must honestly reflect a business risk and offer an understandable path to response. Less, but better — as detection philosophy.

The Score That Refuses to Flatter

All of this discipline needs measurement, and this is where the UTIOM family departs hardest from the industry. Most maturity models are self-congratulation machines: answer optimistically, score high, present the chart. TID-CMM is built so that it *cannot* flatter you — through integrity constraints that only ever lower a score, never raise it:

Evidence ceilings. A rapid self-assessment — answers from team knowledge, no artifacts — cannot score above 3.00, no matter how confident the answers. Scores above 3 require *named evidence*: a specific test report, a specific validation exercise, a specific artifact someone is accountable for. Claimed capability and proven capability are different numbers, and the model keeps them different.

No grading your own homework. If the assessment tool suggested your threat scope and you simply accepted it, your threat-intelligence score is capped — because a model that supplies its

own input and then scores you on it has measured nothing. Your threat model must be *chosen*, deliberately, by you. That constraint is Mintzberg's strategy-as-pattern, enforced in software. **Validation gates.** Detection that has never faced adversarial emulation cannot claim the upper levels, whatever the rule count. The purple team is not an enrichment activity; it is the price of the score.

This is the same honesty the engineering practices build in — the V-Model's evidence discipline, effectuality testing, meta-detections — expressed as arithmetic. It is also why a TID-CMM score is worth defending in front of a board, and a rule count is not. And these instruments are not a sales funnel: The model, workbooks and assessment tool are publicly available and free to use under TID-CMM's published licence terms, and the assessment runs entirely locally in the browser. The honesty is the product.

Why This Makes UTIOM Different

Most frameworks tell you *what* to detect and leave the how to vendors. UTIOM does something more durable — in the book's own words: *"UTIOM standardizes the lifecycle and engineering discipline, not the threats or detections themselves."* Threats change weekly. Discipline compounds for years.

Design, don't assemble. Detection should be built with purpose, not patched with panic.

That is the second difference — and it is the one your adversary will notice first.

The next chapter follows this engineering discipline across the alert boundary, into response.

III. Response Is the Operating Mode, Not the Emergency

The first chapter of this section argued that UTIOM starts from management science, not tools. The second showed detection rebuilt as an engineering discipline. This chapter is about what happens after the alert — and why UTIOM refuses to treat it as an "after" at all.

WHY UTIOM IS DIFFERENT · PART 3

The operating mode, not the emergency.

"A validated detection that fires into an organisation which cannot contain is a very expensive alarm."



Every security framework has a response chapter. It sits at the end, after detection, the way an ambulance sits at the bottom of a cliff. The org chart agrees: detection engineers over here, incident responders over there, a ticket queue between them, and a plan in a binder for the day something terrible happens.

UTIOM's doctrine takes that entire arrangement and inverts it with one law — the sixth of its seven:

"Operations is continuous response."

In UTIOM, response is not a phase that begins when detection ends. It is the SOC's permanent operating mode — the thing the whole system was built to do. Vision, strategy, crown jewels, visibility, detection: all of them are expressions of incident response at different distances from impact. Choosing what telemetry to collect is response, done years early. Writing a detection is response, done months early. Deciding tonight who may isolate a production server is response, done hours early. The incident is merely the moment all those earlier decisions are graded.

And there is a second model in the UTIOM family that does the grading. TID-CMM, from the previous chapter, asks: *would you see it?* Its sibling **TIR-CMM** — the Threat-Informed Response Capability Maturity Model — asks the question that makes CISOs shift in their chairs: *could you act on it — inside the adversary's breakout window, with someone permitted to pull the trigger?*

Because, in TIR-CMM's words: **"A validated detection that fires into an organisation which cannot contain is a very expensive alarm."**

Everything the previous chapter built can end exactly there. This chapter is about making sure it doesn't.

The Only Metric the Adversary Respects

Boyd's OODA loop, from the opening chapter, said the faster decision cycle imposes the terms of the fight. TIR-CMM turns that philosophy into a single, unforgiving number — the **containment margin**:

$$\text{breakout time} - (\text{time to detect} + \text{time to decide} + \text{time to contain})$$

Positive margin: you contained inside the adversary's window, and the incident is a story you tell. Negative margin: the adversary reached the next asset before your containment landed, and the incident is a story someone else tells about you. There is no partial credit, because the adversary gives none — a response slower than adversary tempo fails the model's Level 3 outright, however elegant the process behind it.

The containment margin

breakout time – (detect + decide + contain). The decision is usually what eats it.



Figure — Containment margin turns response speed into an adversary-relative measure.

Inside that margin hides the term almost nobody measures. Aggregate MTTR blends everything into one forgiving average. TIR-CMM splits out **MTTDecide** — the time from a validated alert to someone *authorizing* containment — and calls the gap it exposes the most fixable failure in incident response. Organizations spend millions shaving minutes off detection, then lose hours waiting for a decision-maker who is asleep, in a meeting, or unsure they're allowed to say yes. Which leads to the doctrine's sharpest observation about failed responses: **"The playbook was never the constraint."** The documents were fine. The permission was missing.

Decisions Move Left of the Incident

The opening chapter introduced UTIOM's response horizon: leverage falls and cost rises as impact approaches, and the crossing point is the boundary between designing and reacting. Most organizations live to the right of it, making their hardest decisions at the exact moment those decisions are most expensive and least reversible — 3 a.m., adrenaline high, information low. UTIOM's answer is to move the decisions left, into daylight, where they are cheap and powerful: **Containment authority**, decided in advance. Who may isolate which systems, up to what blast radius, without convening anyone. On-call means authority is awake even when executives are not.

Isolation thresholds and business impact tiers, agreed with the business before any incident. Which crown jewels justify stopping revenue to save them — answered once, calmly, instead of debated during the breach.

Escalation paths and SLAs as engineered artifacts with owners and tests, not tribal knowledge. TIR-CMM enforces the same principle mechanically: automation without pre-granted authorization scores as *demonstration, not response*. A SOAR platform that can isolate a host but must wait for a human chain of permission has automated the easy part and kept the bottleneck. The doctrine already told us why: decisions that should be made at design time otherwise get made during incidents instead — at maximum cost.

An Unrehearsed Playbook Is an Assumption

UTIOM demands response as engineered workflow, not improvisation: playbooks aligned to the threat model, containment automated through SOAR, escalation defined, MTTR and MTTC tracked. TIR-CMM adds the constraint that keeps all of that honest — rehearsal. In its bluntest line:

"An unrehearsed playbook is an assumption wearing a document's clothing."

Under TIR-CMM's scoring rules, an untested playbook counts as an assumption, not a capability — its failures will surface *exactly once, under maximum cost*. This is the previous chapter's testing discipline, carried across the alert boundary: unit tests had effectuality tests; playbooks have exercises. A response capability that has never run against a simulated adversary is in precisely the same epistemic state as a detection that has never fired: unproven, and unprovable from the document alone.

The same evidence discipline applies to the score itself. Like its detection sibling, TIR-CMM caps what self-assessment can claim — a twenty-minute pulse check cannot assert what only evidence-led review can prove. Claimed capability and proven capability stay different numbers, on both sides of the alert.

Respond Like the Threat Model, Not Like the Template

Generic incident response plans fail for the same reason generic detection fails: they are shaped like a standard, not like your organization. The threat-informed principle that scoped detection to 150–250 techniques in the previous chapter scopes response too.

TIR-CMM structures this as a **containment lattice**: response options mapped across attack-path stages and asset classes, scoped to your crown jewels — typically a few dozen cells that actually matter, instead of six hundred hypotheticals. For each cell, the question is concrete: at this stage, on this asset class, what can we actually do, who may do it, and how fast? A missing option on a crown jewel is not an acceptable gap; under the model's rules it is a violation of the threat-informed principle itself.

The containment lattice

Response options per attack-path stage and asset class, scoped to crown jewels — not per technique.

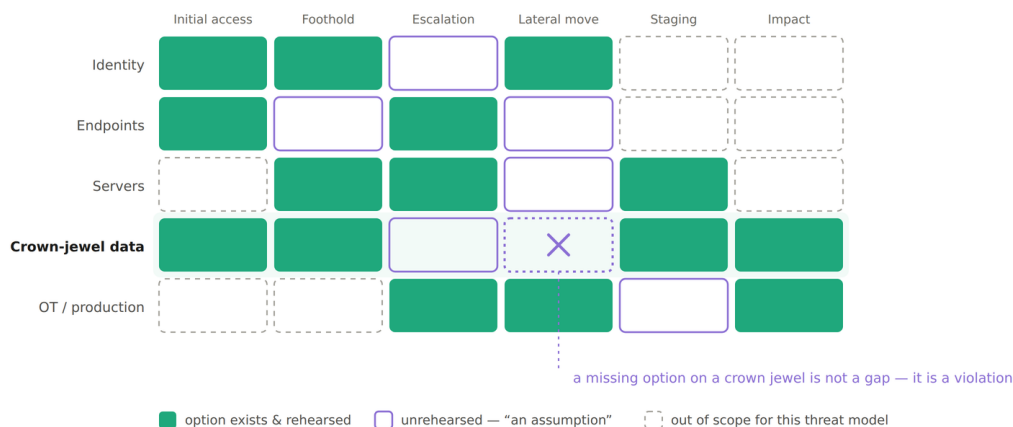


Figure — Response options scoped to the crown jewels, not to six hundred hypotheticals.

And the lattice's highest-leverage row is the one response frameworks usually ignore: prevention and hardening. The reasoning is pure UTIOM — *"prevention buys the one thing response cannot manufacture, which is time."* Every attack path pre-hardened is minutes added to your containment margin before any alert fires.

Learning Is the Final Deliverable

The seventh law — *"improvement is mandatory"* — is where response stops being an ending and becomes an input. The doctrine is explicit: **"Learning is the final deliverable of every incident."** Not the report. Not the timeline. The learning.

Every incident and every exercise closes with a Kaizen review that feeds the whole chain upstream: the threat model gains a technique it had underweighted; visibility gains the log source whose absence hurt; detection gains the rule that would have fired earlier; a playbook loses the step that wasted eleven minutes; the containment margin gets recomputed against what the adversary actually did. Deming's cycle, from the opening chapter, turning at operational tempo. This is the loop that separates a SOC that has ten years of experience from a SOC that has one year of experience ten times.

The Family, Complete

Step back and the architecture of the UTIOM family becomes visible as one thread:

One thread, closed

The operating model defines the lifecycle; two maturity models make it prove itself; learning feeds it back.

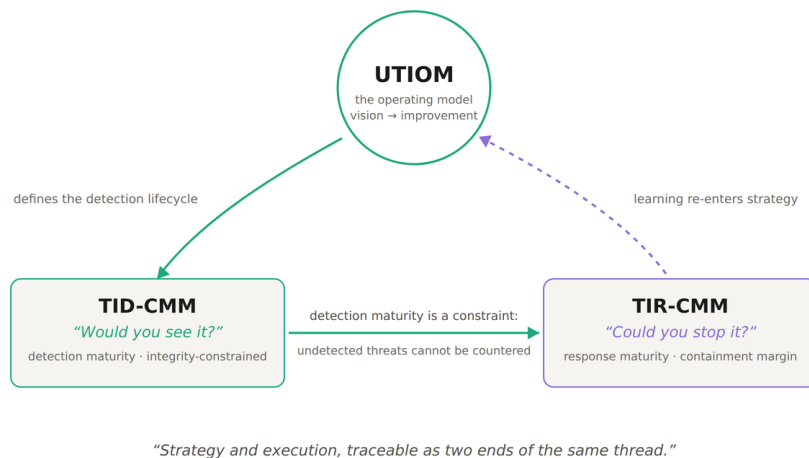


Figure — UTIOM defines the operating model; TID-CMM and TIR-CMM prove it.

UTIOM defines the operating model — how the whole lifecycle should work, from vision to improvement. **TID-CMM** measures the question *would you see it?* — and refuses to let visibility gaps or untested rules inflate the answer. **TIR-CMM** measures *could you stop it?* — and refuses to let unrehearsed playbooks or absent authority inflate that one. Detection maturity flows into response measurement as a constraint, because undetected threats cannot be countered; response reality flows back into strategy, because that is what continuous improvement means. Strategy and execution, traceable as two ends of the same thread — exactly the operating principle this

section started with. All three are publicly available and free to use under their respective licence terms.

What distinguishes UTIOM is that it closes that loop. Most measure fragments; UTIOM connects the fragments and makes each one prove itself.

The quiet standard for the destination is worth repeating: well-designed security operations are not loud. They are deliberate, predictable, and boring. A SOC where the margin is positive, the authority is awake, the playbooks are rehearsed, and every incident makes the system smarter — that SOC has earned its boredom.

That is the third difference: UTIOM treats response not as the emergency at the end of the pipeline, but as the purpose the entire pipeline exists to serve.

20 UTIOM for NIS2 and DORA

European regulation has moved from asking whether controls exist to asking whether they work. NIS2 requires policies on assessing effectiveness. DORA requires risk-based digital operational resilience testing; Article 26 additionally requires advanced threat-led penetration testing for identified financial entities. Both make senior management accountable rather than delegating compliance to a security team.

20.1 NIS2, Directive (EU) 2022/2555

Commission Implementing Regulation (EU) 2024/2690 specifies technical and methodological cybersecurity risk-management requirements and incident significance criteria for the entity categories expressly covered by that Regulation — specified DNS service providers, TLD registries, cloud providers, data-centre providers, CDNs, managed service providers, managed security service providers, trust service providers and the specified online marketplace, search engine and social networking platform categories. It does not apply to every NIS2 entity.

NIS2 has broad sectoral scope across essential and important entities and applies much more broadly across sectors than DORA, covering essential and important entities across energy, transport, banking, health, water, digital infrastructure, public administration, manufacturing, food, chemicals, postal services, waste management, space and research. Far more organisations than DORA, which is limited to financial entities.

Article 21 requires risk analysis, incident handling, business continuity, supply chain security, and policies and procedures to assess the effectiveness of cybersecurity risk management measures. That last requirement is where most programmes are weakest, because effectiveness cannot be evidenced by a control inventory. Article 20 makes management bodies responsible for approving and overseeing these measures. Article 23 requires an early warning within 24 hours, an incident notification within 72 hours, and a final report not later than one month after the incident notification. Where the incident is still ongoing at that point, a progress report is submitted and the final report follows within one month after handling of the incident is completed.

20.2 DORA, Regulation (EU) 2022/2554

DORA applies to financial entities and establishes a Union oversight framework for designated critical ICT third-party service providers, across ICT risk management, incident classification and reporting, digital operational resilience testing, with advanced threat-led penetration testing (TLPT) under Article 26 for identified financial entities, third-party risk and information sharing. It is more prescriptive than NIS2

on testing: Articles 24–25 require a risk-based digital operational resilience testing programme, and Article 26 additionally requires advanced testing by means of TLPT for financial entities identified under the applicable criteria. Commission Delegated Regulation (EU) 2025/1190 specifies the TLPT identification criteria, internal-tester requirements, scope, testing methodology, results and closure, remediation, and supervisory cooperation.

20.3 GDPR Article 33

Where Article 33 notification is required, the controller must notify the competent supervisory authority without undue delay and, where feasible, within 72 hours after becoming aware of the personal data breach, unless the breach is unlikely to result in a risk to the rights and freedoms of natural persons. The processor must notify the controller without undue delay after becoming aware of a personal data breach. UTIOM supports operational readiness; it does not determine whether the legal notification threshold has been met. Operationally, meeting that deadline depends heavily on how quickly the organisation can detect, classify and scope the breach.

20.4 Mapping requirements to UTIOM outputs

NIS2 Article 21(2)(a), risk analysis. Crown jewel registry with named owners, business impact mapping, and threat models per asset.

NIS2 Article 21(2)(b), incident handling. Pre-engineered playbooks per crown jewel and containment authority with named individuals.

NIS2 Article 21(2)(f), effectiveness. UTIOM uses adversary emulation, detection-validation records and response-readiness evidence as operational evidence supporting the Article 21(2)(f) effectiveness-assessment requirement.

NIS2 Article 20, management accountability. Vision and Strategy governance artefacts, stakeholder map, and KPIs tied to crown jewels.

NIS2 Article 23, reporting timelines. Contextual incident records tagged with crown jewel, TTPs and attack path, plus MTTD measured per priority TTP.

DORA, ICT risk management. Crown-jewel-driven prioritisation with dependency matrices.

DORA Arts. 24–25, digital operational resilience testing. Adversary emulation aligned to the documented threat profile.

GDPR Article 33. Telemetry engineered outward from crown jewels, with dependency mapping that makes impact scoping a lookup rather than an investigation.

UTIOM is an operating model, not legal advice and not a certification scheme. Obligations vary by member state transposition, sector and entity classification.

21 Philosophy and Core Principles

UTIOM is built on the belief that effective security operations are not the result of more tools, more alerts, or more activity, but of clear intent, informed prioritisation and disciplined execution.

21.1 Five core principles

Strategy before execution. Security operations must be guided by vision and intent, not driven by tooling or alerts. A capability built because a product supports it, rather than because a threat demands it, is spend without direction.

Focus on what truly matters. Not all assets are equal. Protecting crown jewels is more effective than attempting uniform coverage.

Threat-informed by default. Detection and response should be designed around real adversary behaviour, not assumptions or generic indicators.

Engineering over intuition. Visibility, detection and response are engineered capabilities that must be designed, tested and measured. Detection built as craft depends on who is on shift; detection built as engineering survives them leaving.

Learning as a system property. Continuous improvement is not an activity performed after incidents. It is an embedded feedback loop across the whole lifecycle.

21.2 Five differentiators

Strategy-first, not tool-first. Governance and intent as active drivers, not static documents.

Threat-informed by design. Engineered around realistic attacker behaviour, not indicator matching.

Crown-jewel focused. Prioritised around assets carrying real business, regulatory and systemic risk.

Operational, not theoretical. Designed for real security operations with limited resources and real constraints.

Framework-agnostic, standards-aligned. Complements and operationalises NIST CSF 2.0, SOC-CMM, DORA and NIS2 without replacing any of them.

21.3 What UTIOM does for an organisation

UTIOM is an operating framework that helps organisations unify siloed security functions into a single threat-informed operation. It connects management, engineering and operations through one lifecycle, provides the methodology to run it, and can be measured, so that maturity is demonstrated rather than asserted.

22 A Note on What Strategy Means in UTIOM

Strategy in UTIOM means the security operations strategy, not the business strategy. The two are distinct and must not be confused.

Business strategy is an input. It tells you what the organisation is trying to achieve, which services it cannot afford to lose, and what regulatory obligations it carries. UTIOM consumes that; it does not produce it.

The security operations strategy is the answer to it: which adversaries realistically target an organisation of this shape, which assets carry the business consequence, what capability gets built in what order with what owner and what date, and how success will be measured.

They must align, not merely coexist. A security operations strategy that cannot be traced back to a business objective is an engineering plan wearing a strategic title. One that works against business objectives will be routed around and eventually defunded.

23 Release History

Version 1.2, August 2026. Standards mapping corrected to NIST CSF 2.0 and ISO/IEC 27001:2022 + Amd 1:2024. Framework family, Response Horizon, V-Model, traditional SOC comparison, NIS2 and DORA, philosophy sections, and the Why UTIOM Is Different three-part synthesis with supporting editorial figures added. Terminology clarified throughout.

Version 1.1, August 2026. Assessment instruments published: maturity, capability, metrics and the improvement roadmap, with an offline workbook and a self-hosted package.

Version 1.0, February 2026. First public edition. Full lifecycle, capability layer model, maturity model, implementation blueprint, metrics, and worked industry examples.

Public release, August 2025. UTIOM published publicly for the first time: the lifecycle, three pillars, seven laws, and the argument that incident response is the operating mode of security operations.

Development, from 2022. Four years of building and testing against real security operations transformation work in banking, FinTech and hybrid enterprise environments.

Origin, circa 2018. The core idea surfaced while writing the author's first book: security operations were being assembled from parts rather than designed as a system.

24 Glossary

Terms as they are used in this book. Where a term has a broader industry meaning, the UTIOM usage is given first and the distinction noted.

24.1 UTIOM lifecycle terms

Vision. The first operational control. A documented statement of why the security operation exists, what it protects, how success is measured and who owns the outcome. Not a mission statement; an active constraint on everything built downstream.

Strategy. The security operations strategy, distinct from the business strategy. Threat profiling, risk prioritisation and a capability roadmap with owners and dates. Business strategy is an input to it, not a synonym for it.

Crown jewel. An asset, service, dataset or identity whose compromise would cause disproportionate damage relative to everything else. Determined by business consequence, not technical sensitivity. The anchor for all downstream prioritisation.

Crown jewel registry. The documented set of crown jewels with named business owners, business impact mapping, threat models, attack paths and dependency matrices.

Threat visibility. The engineering discipline of deciding what telemetry must exist to observe modelled attack paths against crown jewels, then building it. Distinct from log collection, which is volume without direction.

Visibility gap report. A documented statement of what cannot currently be seen, formally accepted by leadership. Turns blind spots from accidents into recorded architectural decisions.

Threat detection. The engineering of analytics that recognise adversary behaviour within available telemetry. In UTIOM, every rule must trace to a threat model, a technique and a crown jewel.

Response. Pre-engineered containment, eradication and recovery, with authority and escalation thresholds defined before the incident rather than during it.

Continuous improvement. The feedback loop that converts incidents, exercises and near-misses into engineering change across telemetry, detection, playbooks and strategy.

24.2 UTIOM concepts

Threat-informed. Designed around documented adversary behaviour rather than generic indicators, vendor content or assumption. The opposite of coverage-driven.

Detection-as-code. Treating detection content as software: version controlled, peer reviewed, tested before production, deployed through a pipeline and systematically retired.

Trace completion rate. The proportion of live detection rules that can be walked from rule to threat model to technique to crown jewel to business consequence. A rule that cannot complete the chain is waste.

The Response Horizon. The observation that the leverage of a decision falls and its cost rises as the moment of impact approaches. The crossing point separates designing from reacting.

The V-Model. The pairing of each design activity with the activity that validates it. Purple team proves attack paths, detection QA proves telemetry, response outcomes prove the threat profile.

Systematic abandonment. Drucker's principle applied to detection: every improvement cycle must retire rules that no longer protect a crown jewel. A detection library is perishable inventory, not an asset.

Meta-detection. A detection that monitors the health of the detection and telemetry pipeline itself, so that silent failures surface before an incident does.

Alert fatigue. Treated in UTIOM as a system design failure rather than a staffing problem. If analysts are overwhelmed, fidelity is too low or operational cost per rule is too high.

Operational cost per rule. Analyst minutes consumed per detection rule per period. The metric that exposes alert fatigue as an engineering problem with an engineering fix.

Quiet operations. The mature state in which noise decreases because intent is clear, response accelerates because paths are predefined, and learning compounds. Well-designed security operations are deliberate, predictable and boring.

24.3 The framework family

UTIOM. Unified Threat-Informed Operations Model. The operating model that connects leadership intent, engineering discipline and operational execution into one lifecycle.

TID-CMM. Threat-Informed Detection Capability Maturity Model. Measures the engineering pillar in depth: whether detection is genuinely driven by adversary behaviour, whether the telemetry exists to see it, and whether any of it has been proven. Published at tid-cmm.com.

TIR-CMM. Threat-Informed Response Capability Maturity Model. Measures the operations pillar: whether containment authority exists before the incident and whether you can act inside the adversary breakout window. Published at tir-cmm.com.

RSMM. Realistic SIEM Maturity Model. Five levels from Blame Collector to Outcome-Driven SIEM, measuring the platform that detection runs on.

STRATA. Strategy, Talent, Resilience, Automation, Telemetry and Adaptability. A refinement of the People, Process and Technology triad, supplying the organisational dimension of UTIOM.

Containment Margin. A TIR-CMM metric: adversary breakout time minus the sum of detect, decide and contain. Negative margin means the adversary reaches the objective first.

24.4 Metrics

MTTD. Mean Time to Detect. In UTIOM, measured against top-priority TTPs rather than as an aggregate, because an average hides the cases that matter.

MTTC. Mean Time to Contain. From confirmed incident to contained adversary activity.

MTTR. Mean Time to Recover. From containment to validated return to service.

Detection validation rate. The proportion of live detection rules that have actually been tested by emulation or simulation. Untested detection is an assumption.

Response readiness validation. The proportion of playbooks exercised within the review period.

Leading indicator. A measure of what will happen: coverage per threat modelled, validation rate, playbook coverage. What a programme should steer by.

Lagging indicator. A measure of what already happened: MTTD, MTTC, incidents handled. Useful for reporting, arriving too late to steer by.

Breakout time. The interval between an adversary's initial access and their first lateral movement. The clock against which response tempo should be measured.

24.5 Standards and external frameworks

NIST CSF 2.0. The Cybersecurity Framework, revised in 2024 to add GOVERN as a first-class function alongside Identify, Protect, Detect, Respond and Recover. Defines outcomes; UTIOM defines the operating model that delivers them.

ISO/IEC 27001:2022/Amd 1:2024. Information security management standard. Annex A was restructured into 93 controls across four themes: Organizational A.5, People A.6, Physical A.7 and Technological A.8. The 2013 fourteen-domain numbering is retired.

SOC-CMM. Security Operations Centre Capability Maturity Model by Rob van Os. Measures maturity across business, people, process, technology and services. Measures how mature a SOC is; UTIOM provides the mechanism to become mature.

MITRE ATT&CK. A curated knowledge base of adversary tactics and techniques observed in real intrusions. In UTIOM, a shared vocabulary scoped to crown jewels rather than a coverage checklist.

MITRE DeTT&CT. An open methodology for scoring detection coverage against ATT&CK using data source quality and visibility. Where ATT&CK describes adversary behaviour, DeTT&CT measures whether you could see it.

MITRE Engage. A framework for adversary engagement, deception and denial operations. Used in UTIOM to place deception along modelled crown jewel attack paths.

Sigma. A generic, platform-agnostic signature format for detection rules, translatable to most SIEM query languages. Supports the portability principle in detection engineering.

NIS2. Directive (EU) 2022/2555. Cybersecurity obligations for essential and important entities across most critical sectors. Article 21 requires risk management measures including assessment of their effectiveness; Article 20 makes management bodies accountable; Article 23 sets 24-hour early warning, 72-hour incident notification and a final report not later than one month after the incident notification.

DORA. Regulation (EU) 2022/2554 on digital operational resilience for the financial sector. Five pillars covering ICT risk management, incident reporting, digital operational resilience testing, with advanced threat-led penetration testing (TLPT) under Article 26 for identified financial entities, third-party risk and information sharing.

TIBER-EU 2025. The European framework for threat intelligence-based ethical red teaming, updated by the Eurosystem in 2025 to align with DORA's TLPT regulatory technical standards; it provides operational guidance for TLPT where used consistently with DORA and the applicable RTS.

GDPR Article 33. Where notification is required, the controller must notify the competent supervisory authority without undue delay and, where feasible, within 72 hours after becoming aware of the personal data breach, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.

24.6 Method and engineering terms

OODA loop. Observe, Orient, Decide, Act. Boyd's decision cycle, applied in UTIOM at incident tempo between engineering and operations.

PDCA. Plan, Do, Check, Act. Deming's improvement cycle, the operational structure behind UTIOM's continuous improvement phase.

Kaizen. Japanese term for continuous improvement through small, consistent changes rather than periodic overhauls.

DRY principle. Don't Repeat Yourself. A software principle applied to detection: shared logic, exclusion lists and normalisation belong in shared configuration objects, not duplicated across rules.

Common Information Model. A normalised schema that detection logic sits on top of, so that content survives a change of platform or data source.

Purple team. A collaborative exercise where offensive emulation and defensive engineering work together, with the objective of improving detection rather than proving compromise.

Adversary emulation. Executing the specific techniques of a profiled adversary against your own environment to validate whether telemetry, detection and analyst decisions perform as designed.

Living off the land. Adversary tradecraft that uses legitimate credentials, tools and platform APIs rather than deploying detectable malware.

25 Further Reading and Sources

The works and standards this framework draws on, grouped by the part of the lifecycle they inform.

These mappings are the author's operational crosswalk for UTIOM. They are not official NIST, ISO or regulatory mappings, do not establish conformity or compliance by themselves, and are not legal advice. Validate them against the organisation's applicable profile, ISO Statement of Applicability, regulatory classification, national transposition and competent-authority guidance.

25.1 Standards and regulation

NIST — Cybersecurity Framework 2.0; SP 800-61 Rev. 3 (2025) Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile; IR 8183 Rev. 2 Cybersecurity Framework 2.0 Manufacturing Profile (Initial Public Draft); SP 800-137 Information Security Continuous Monitoring.

ISO/IEC — ISO/IEC 27001:2022 + Amd 1:2024 Information security management systems; 27035-1:2023 Principles and process; 27035-2:2023 Guidelines to plan and prepare for incident response; 27035-3:2020 Guidelines for ICT incident response operations; 27035-4:2024 Coordination.

European Union — Directive (EU) 2022/2555 (NIS2); Commission Implementing Regulation (EU) 2024/2690; Regulation (EU) 2022/2554 (DORA); Commission Delegated Regulation (EU) 2025/1190; Regulation (EU) 2016/679 (GDPR); TIBER-EU 2025 framework for threat intelligence-based ethical red teaming.

Other — COBIT 2019 governance objectives; TOGAF Standard, 10th Edition Architecture Development Method; CIS Critical Security Controls v8.1; FIRST CSIRT Services Framework v2.1.

25.2 Threat-informed defence

MITRE — ATT&CK Enterprise v19.2 knowledge base; Engage adversary engagement framework; D3FEND countermeasure knowledge graph.

Community — DeTT&CT by Marcus Bakker and Ruben Bouman; Sigma detection rule format; Atomic Red Team; Caldera.

Maturity models — SOC-CMM by Rob van Os; DML by Ryan Stillions; the Pyramid of Pain by David Bianco.

25.3 Management and engineering thinking

Peter Drucker — The Practice of Management; Management by Objectives; the concept of the knowledge worker and systematic abandonment.

Henry Mintzberg — Strategy as a pattern in a stream of decisions, rather than a document.

W. Edwards Deming — The Plan-Do-Check-Act improvement cycle.

Toyota Production System — Kaizen as small, consistent, compounding improvement.

John Boyd — The OODA loop as a model for decision tempo under adversarial pressure.

Hunt and Thomas — The Pragmatic Programmer, and the DRY principle applied here to detection content.

Dieter Rams — Principles of good design, applied to alert output and cognitive load.

Sun Tzu — The Art of War, for the principle that self-knowledge precedes effective defence.

25.4 The framework family

UTIOM — utiom.de. Framework book, assessment instruments and supporting material.

TID-CMM — tid-cmm.com. Threat-Informed Detection Capability Maturity Model.

TIR-CMM — tir-cmm.com. Threat-Informed Response Capability Maturity Model.

STRATA and RSMM — Published through the author's writing. See utiom.de for current links.

About the Author

Who am I?

Reza Adineh is a German-based cybersecurity architect and visionary with over 15 years of experience designing and leading Security Operations Centres across banking, cloud, and hybrid environments. After years of building & Operating SOC's, realized that true resilience doesn't come from technology alone it comes from unifying strategy, engineering, and continuous learning. From that vision, UTIOM was born. As creator of the STRATA and TID-CMM frameworks and founder of Minimal Cyber, focuses on transforming detection and response into intelligent, adaptive systems that connect purpose, people, and precision.

License:

© 2026 Reza Adineh

This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International Licence (CC BY-SA 4.0). To view a copy of this licence, visit creativecommons.org/licenses/by-sa/4.0/. You are free to share and adapt this material, including commercially, provided you give appropriate credit, link to the licence, and distribute your contributions under the same licence. MITRE ATT&CK® is a registered trademark of The MITRE Corporation. UTIOM is not affiliated with or endorsed by MITRE.

Appendix A - Operational Use of MITRE ATT&CK

ATT&CK is a shared vocabulary, not an operating model and not a coverage target. UTIOM turns it into capability through five steps:

Scope from the environment: intersect what you run, what you protect and who realistically targets you.

Anchor to crown jewels: model realistic attack paths to each critical asset and prioritise techniques on those paths.

Translate techniques to telemetry: measure what is actually collected and at what quality; structural blind spots are visibility gaps.

Engineer detection: normalise, version, test and trace each rule to a technique, threat model and crown jewel.

Validate with emulation: test telemetry completeness, detection timing and analyst decisions against profiled adversaries.

Metric	Honest denominator
Coverage per tactic	Adequately observed tactics / tactics in the scoped threat profile

Metric	Honest denominator
Coverage per threat model	Modelled attack paths with required telemetry / total modelled paths
Trace completion rate	Rules traceable to technique, model, crown jewel and impact / rules sampled
Detection validation rate	Rules tested by emulation / total live rules
MTTD per priority TTP	Detection time for prioritised behaviours, not an estate-wide aggregate

Appendix B - UTIOM Measurement Instruments

A framework that mandates measurement must provide instruments. The UTIOM assessment suite operationalises the model through four complementary instruments:

Instrument	Scope	Primary output
Maturity Assessment	50 gated criteria across six maturity levels	Evidence-based maturity position
Capability Assessment	105 indicators across ten lifecycle domains	Domain capability profile
Metrics Calculator	Leading and lagging operational measures with formulas	Performance and outcome evidence
Improvement Roadmap	Prioritised actions based on assessment gaps	Sequenced transformation plan

Appendix C - Content Preservation and utiom.de Coverage

This final v1.2 uses the author's authoritative source edition as its master so that all footnotes, hyperlinks and the approved black cover remain intact. It was cross-checked against the v1.0/v1.1 published manuscript, the revised working draft and the substantive concepts published on utiom.de. At the time of this revision, utiom.de publishes Framework v1.3 and Framework Book v1.2, with Book v1.2 available for online reading and as PDF; this consolidated book is v1.2, released August 2026.

Source or topic	Final v1.2 location/status
v1.0/v1.1 original chapters, examples and implementation material	Retained in Chapters 1-15
All source footnotes	Retained and structurally verified
Original high-level UTIOM lifecycle diagram	Retained in the foundations/lifecycle material
Canonical utiom.de V-shape diagram	Retained exactly as published; not recreated
Response Horizon and source article	Chapters 17 and related diagram
Framework family: UTIOM, TID-CMM, TIR-CMM, RSMM and STRATA	Chapter 16 and glossary
Traditional SOC comparison and V-model design/validation pairing	Chapters 18-19

Source or topic	Final v1.2 location/status
NIS2, DORA and GDPR alignment	Chapter 20
Philosophy, differentiators and strategy clarification	Chapters 21-22
Release history, glossary and further reading	Chapters 23-25
Corrected NIST CSF 2.0 / ISO/IEC 27001:2022/Amd 1:2024 table	Chapter 4; old table replaced
Operational ATT&CK use and measurement instruments	Appendices A-B
Licence	CC BY-SA 4.0 wording retained from the authoritative v1.2 source

Verification sources for version 1.2

NIST, The Cybersecurity Framework (CSF) 2.0 and CSF 2.0 Reference Tool, 2024.

ISO, ISO/IEC 27001:2022/Amd 1:2024 and ISO/IEC 27002:2022.

European Union, Directive (EU) 2022/2555 (NIS2).

European Union, Regulation (EU) 2022/2554 (DORA).

European Union, Regulation (EU) 2016/679 (GDPR), Article 33.

UTIOM Framework Book v1.0/v1.1, the authoritative v1.2 source, and utiom.de; reviewed August 2026.

Appendix D - Current utiom.de Alignment Supplement

This supplement makes the current public-site concepts explicit in the book rather than leaving them implied. It follows the substantive pages listed in the utiom.de sitemap in August 2026.

The six problems UTIOM solves

Failure pattern	Operational consequence	UTIOM response
No defined purpose	Teams optimise for different outcomes because success is undefined.	Vision is the first operational control: purpose, ownership, protection scope and measures are defined before capability.
Fragmented silos	Intelligence, hunting, detection, monitoring and response lose context at hand-offs.	Treat them as expressions of one incident-response discipline at different distances from impact.
Alert fatigue	Analyst attention follows volume rather than business risk.	Prioritise detections by crown jewel and threat profile; retire rules without a defensible trace.
Tool-driven engineering	Vendor defaults create large libraries unrelated to relevant threats or critical assets.	Require traceability from rule to behaviour, threat model, crown jewel and business consequence.
No defensible spend	Budget discussions become renewals and headcount rather than risk reduction.	Map investment and metrics to named risk priorities and business consequences.
Compliant on paper, exposed in reality	Documented controls pass audit without proving effectiveness against relevant adversaries.	Operationalise NIST CSF, ISO 27001 and DORA through the lifecycle and validate behaviour in practice.

The seven SOC operating-model components

Component	Required design decision
Vision	Why the SOC exists, what it protects, how success is measured and who owns the outcome.
Strategy	Which adversaries are realistic and what capability is built, in what order, with owners and dates.
Asset prioritisation	Critical services, data and identities, with business owners, threat models and attack paths.
Visibility engineering	Required telemetry, quality, attack-path coverage and formally accepted blind spots.
Detection engineering	How analytics are built, tested, versioned, traced and retired.
Response	Critical-asset playbooks, containment authority, escalation thresholds and decision gates.
Continuous improvement	How findings become engineering changes with owners, dates and refreshed models.

Internal, outsourced and hybrid structures

Structure	Operating-model requirement
Internal	Define on-call coverage, specialist depth, out-of-hours escalation and knowledge continuity.
Outsourced	Retain ownership of vision, strategy and crown jewels; define provider boundaries and containment authority.
Hybrid	Assign an explicit owner to tuning, escalation, production containment and detection scope at every boundary.

Assessment instruments and current framework family

Item	Current public-site state
UTIOM	Framework v1.3; seven lifecycle phases, three pillars and four assessment instruments. Framework Book v1.2 is published online and as PDF. This consolidated book is v1.2.
Maturity Assessment	50 gated criteria across six levels.
Capability Assessment	105 indicators across ten lifecycle domains, scored 0-5.
Metrics Calculator	70 metrics with explicit formulas, separating leading and lagging indicators.
Improvement Roadmap	Combines completed assessments into a sequenced ninety-day plan.
Assessment privacy	Browser-only operation: no backend, database, analytics or signup; clearing site data removes results.
TID-CMM	v1.5; eight domains, 58 sub-capabilities and ATT&CK v19.2.

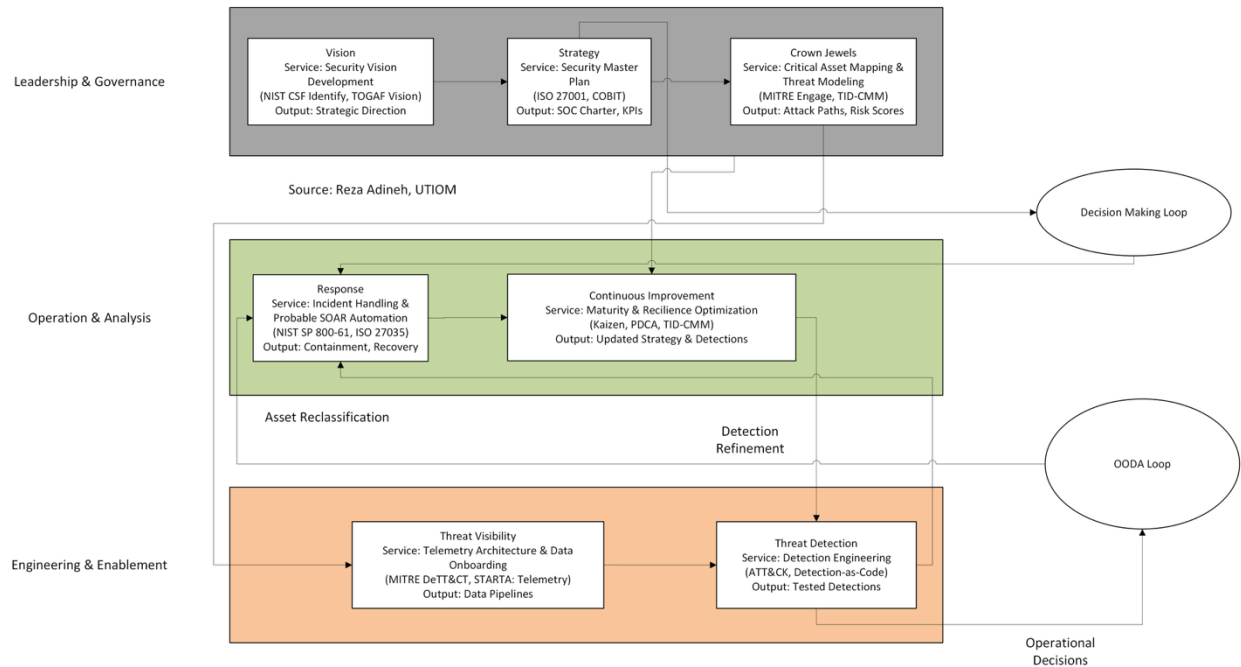
Item	Current public-site state
TIR-CMM	v1.0; 58 sub-capabilities and the current published response-capability model.

Live-site page coverage

utiom.de page	Book coverage
What is UTIOM?	Introduction; Chapters 1-3 and 22
What problem does UTIOM solve?	Appendix D: six failure patterns
Standards alignment	Chapters 4, 12-14 and corrected mapping table
SOC operating model	Chapters 18-19 and Appendix D: seven components and delivery structures
MITRE ATT&CK in the SOC	Appendix A and Chapters 2, 7-8
Philosophy	Chapter 21 and Response Horizon
UTIOM in one minute	Lifecycle, framework family and assessment-instrument sections
Traditional SOC vs UTIOM	Chapter 19
NIS2 and DORA	Chapter 20
Changelog and About	Release history, framework family, author and licence sections
Assessment tools	Appendices B and D; maturity, capability, metrics and roadmap

Appendix E - Archival Original Lifecycle Diagram

The main lifecycle diagram is presented in the harmonised dark-green publication theme. The unmodified original artwork from the v1.0/v1.1 manuscript is reproduced below so that no source visual is lost or silently replaced.



Archival figure. Original UTIOM high-level operating-model diagram, unchanged. Source: Reza Adineh, UTIOM.