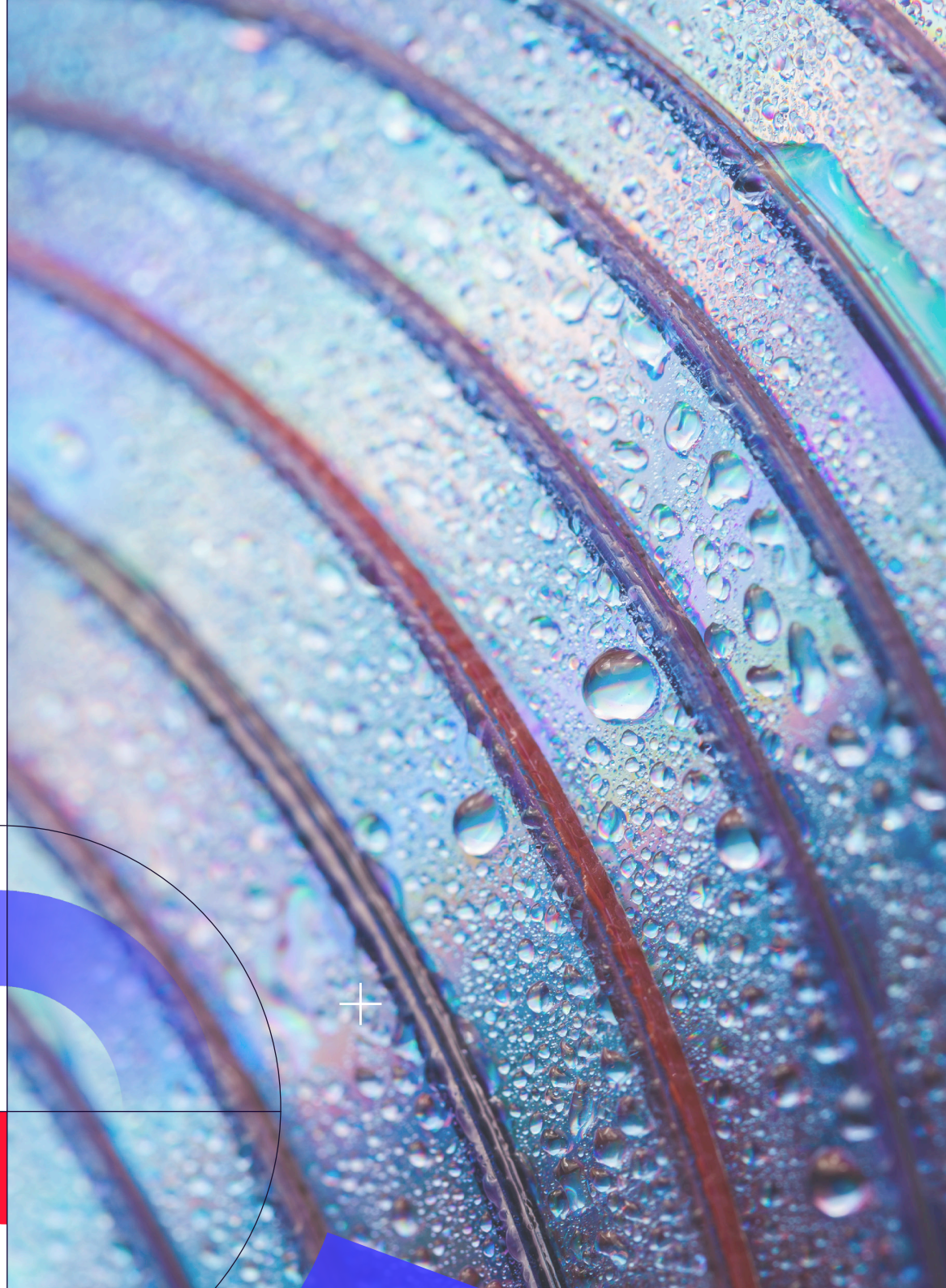
GATEWATCHER

From detection *to decision_*

Why the next era of cybersecurity isn't about seeing more, *it's about acting right*

...or when your usual Mean Time To Detection (MTTD) becomes your *Mean Time To Decision*



*Summary_*

*Executive Summary_*

Cybersecurity is reaching a *structural breaking point.*

For over two decades, organizations have invested in detection: more tools, more sensors, more telemetry, more alerts, more visibility. This progress has strengthened security foundations. Better visibility leads to better signals, and high-quality detection remains a prerequisite for effective defense. Today's environments are instrumented, data-rich, and capable of surfacing threats with a level of depth and context that was previously unattainable.

However, as detection capabilities have scaled, a new constraint has emerged. Cybersecurity teams are now operating in environments where the volume, velocity, and complexity of signals exceed their ability to consistently analyze and act on them. Thousands of alerts must be triaged, correlated, and validated, with each step requiring expertise, time, and context.

In practice, the limiting factor is no longer access to data, but the ability to transform that data into timely, confident decisions.

The industry has therefore optimized heavily for seeing, but less for deciding. This has created a structural imbalance within Security Operations Centers (SOCs): strong detection coverage, but limited capacity to translate signals intoreliable, scalable outcomes. Organizations are therefore caught between two unsatisfactory options, see more and drown, or filter more but introduce blindspots...

This shift calls for a broader definition of performance. Beyond Mean Time to Detect, organizations must now also prioritize Mean Time to Decision: the ability to reach a clear, evidence-based, and actionable conclusion with confidence and speed.

> We believe, a new paradigm is emerging:
> **Cybersecurity is evolving from detection-centric to *decision-driven_***

In this model, detection provides the depth, coverage, and fidelity of signals, while decision capabilities transform those signals into prioritized, contextualized, evidence-based, confidence-scored, and actionable outcomes.

Organizations that embrace this shift will fully leverage their detection capabilities, accelerating remediation, improving resilience, and scaling their operations without proportionally increasing costs or human effort.

Those that do not will continue to face growing volumes of signals with limited ability to convert them into effective action.

Key metrics at a glance

— **Mean Time to Detect, MTTD**
The time it takes to identify that something suspicious or malicious is happening.

— **Mean Time to Remediate, MTTR**
The time it takes to contain and remediate the threat once it has been identified.

— **Mean Time to Decision,** *the new MTTD*
The time it takes to understand the situation well enough to make a confident, actionable decision.

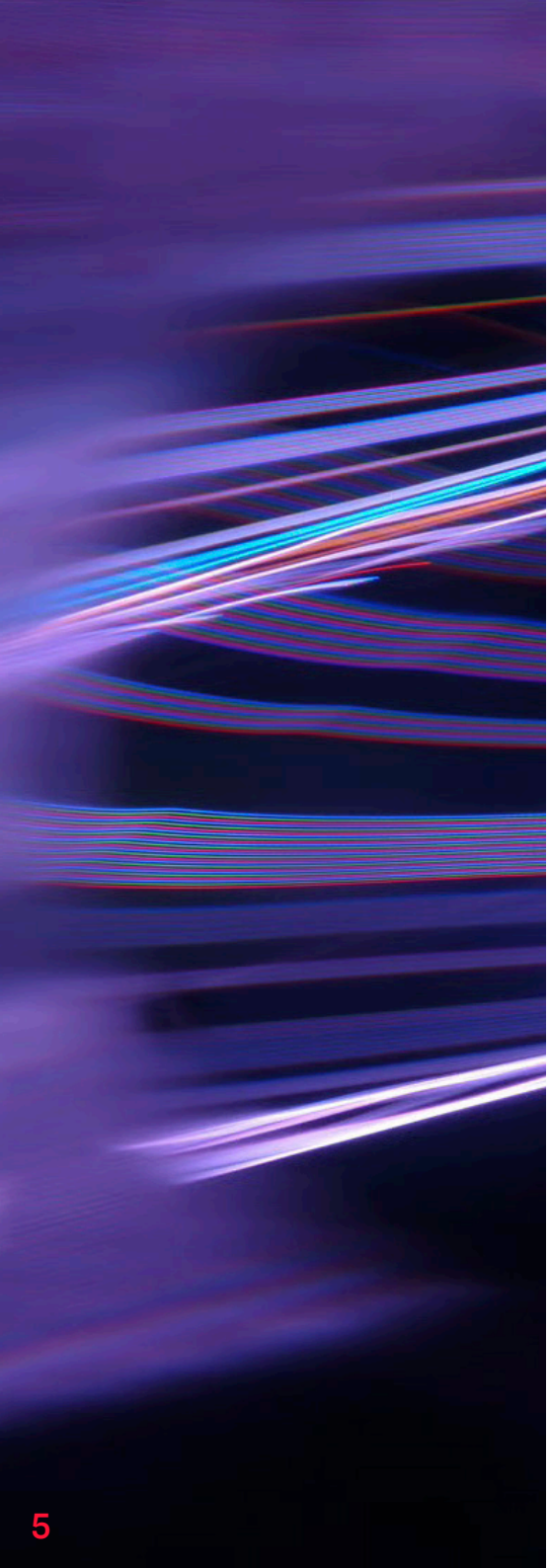
MTTD tells you how fast you see.

MTTR tells you how fast you act.

MTTDecision determines how effectively you decide in between.

The purpose of this white paper is to demonstrate why Mean Time to Decision should redefine MTTD, because in modern cybersecurity operations, the true measure of effectiveness is no longer how quickly a threat is detected, but how quickly it can be understood and acted upon with confidence.

Detection starts the clock.
Decision stops the chaos



01

DETECTION MATURITY:
The turning point to decision-driven operations_

1. From visibility's peak to decision's edge

From the early SIEMs of the 2000s (built to centralize logs and enable correlation), to today's EDR, NDR, and XDR platforms, cybersecurity has steadily expanded its detection capabilities.

This evolution has been both necessary and valuable. Organizations have become increasingly **data-native**, leveraging richer, higher-quality telemetry across endpoints, networks, identities, and cloud environments. Detection today is no longer blind or fragmented, it is deep, contextual, and increasingly multi-source by design.

This progress matters. Better data leads to better signals. And better signals are the foundation of effective security.

But this evolution has also been guided by a simple belief:

> If we detect everything,
> *we can stop anything_*

This made sense in less complex contexts. Today, it's like upgrading from a bicycle to a race car... but keeping bicycle brakes.

Detection is a critical first step. But without decision, signals turn into noise. At that point, alert volume is no longer coverage, but a potential liability and a source of risk.

2. SOCs are drowning, not blind

*The asymmetry problem_*

Detection is infinite, human decision capacity isn't. This creates a structural imbalance: signals grow exponentially but human cognition does not.

The result is inevitable: *decision saturation.*

More *data*
More *alerts*
More *ambiguity*
Less *effective* action

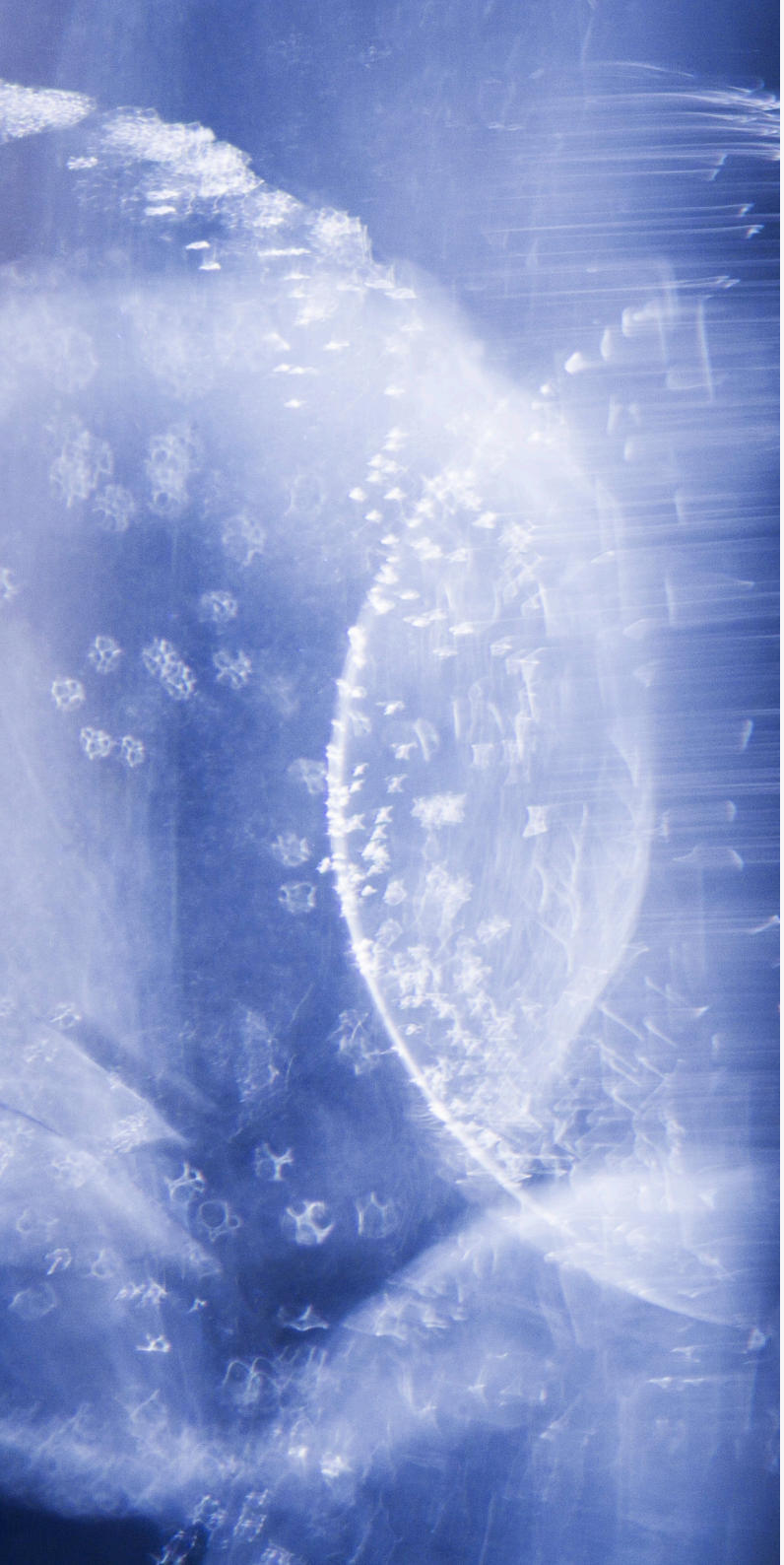
Cybersecurity has created a paradox of abundance:
the more we see, the harder it becomes to decide.

Contrary to popular belief, most SOCs are not lacking visibility. They are overwhelmed by it.

> Analysts spend a significant portion of their time on **triage, correlation, and context gathering**
> False positives remain high across most environments
> Alerts arrive **fragmented and decontextualized**

"The real question is no longer:
"Did something happen?"

But:
"What should we do about it?"



Recent data shows that alert overload is not only persisting, but in some cases worsening. In 2025, **76% of security leaders reported experiencing alert fatigue***, driven by continuously increasing alert volumes and fragmented detection environments. More critically, 2026 report found that **3/4 of IT teams experienced outages due to missed critical alerts**, directly linking alert fatigue to operational failure**.

Similarly, IDC reported that between 23% and 30% of alerts are routinely ignored, with mid-sized organizations often struggling the most to keep up with the volume.

This is not a new phenomenon. As early as 2020, research conducted by Forrester*** estimated that security teams were already handling around 11,000 alerts per day on average, with more than a quarter left uninvestigated, amounting to several thousand alerts effectively ignored every single day. At the same time, 77% of decision-makers acknowledged that manual triage processes were significantly slowing down alert handling. Interestingly, mid-sized organizations, often assumed to be more agile, tended to perform worse than both smaller and larger counterparts, suggesting that scale alone does not solve the problem.

Together, these findings highlight a structural issue: despite advances in detection, the ability to effectively process and act on alerts has not kept pace, and the gap continues to widen.

* 2025 Pulse of the AI SOC: Why SOC is Breaking - https://gurucul.com/blog/2025-pulse-of-the-ai-soc-why-soc-is-breaking/

** Alert fatigue drives UK IT outages & rising burnout - https://itbrief.co.uk/story/alert-fatigue-drives-uk-it-outages-rising-burnout

***The 2020 State Of Security Operations. SecOps Teams Struggle To Hit Key Metrics In Quest To Keep Up With The Growing Volume OfSecurity Alert, Forrester Consulting Thought Leadership PaperCommissioned By Palo Alto Networks April 2020.

3. The hidden metric: Time of confusion

The industry usually measures **MTTD (Mean Time to Detect)** and **MTTR (Mean Time to Respond).**

But it ignores a critical phase in between:
Time of confusion.

This is the time it takes for an analyst to understand:

- What is happening?
- Whether it matters?
- What action is appropriate?

In many SOCs, this added time is the **true bottleneck.**

Sully saved everyone.
A machine might've also saved the plane.

In 2009, US Airways Flight 1549 lost both engines shortly after takeoff. Captain Sully had only seconds to assess the situation, discard unsafe options, and choose: return to La Guardia Airport or land on the Hudson River.

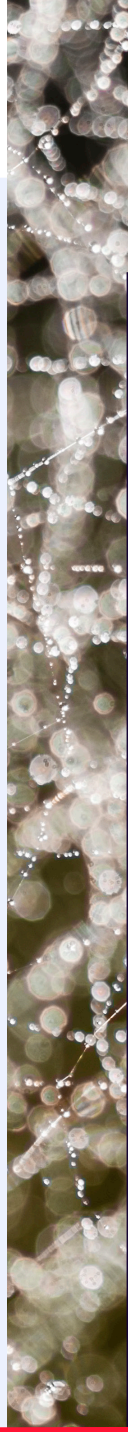
He chose the Hudson, and saved every life. Afterward, simulations told a different story.

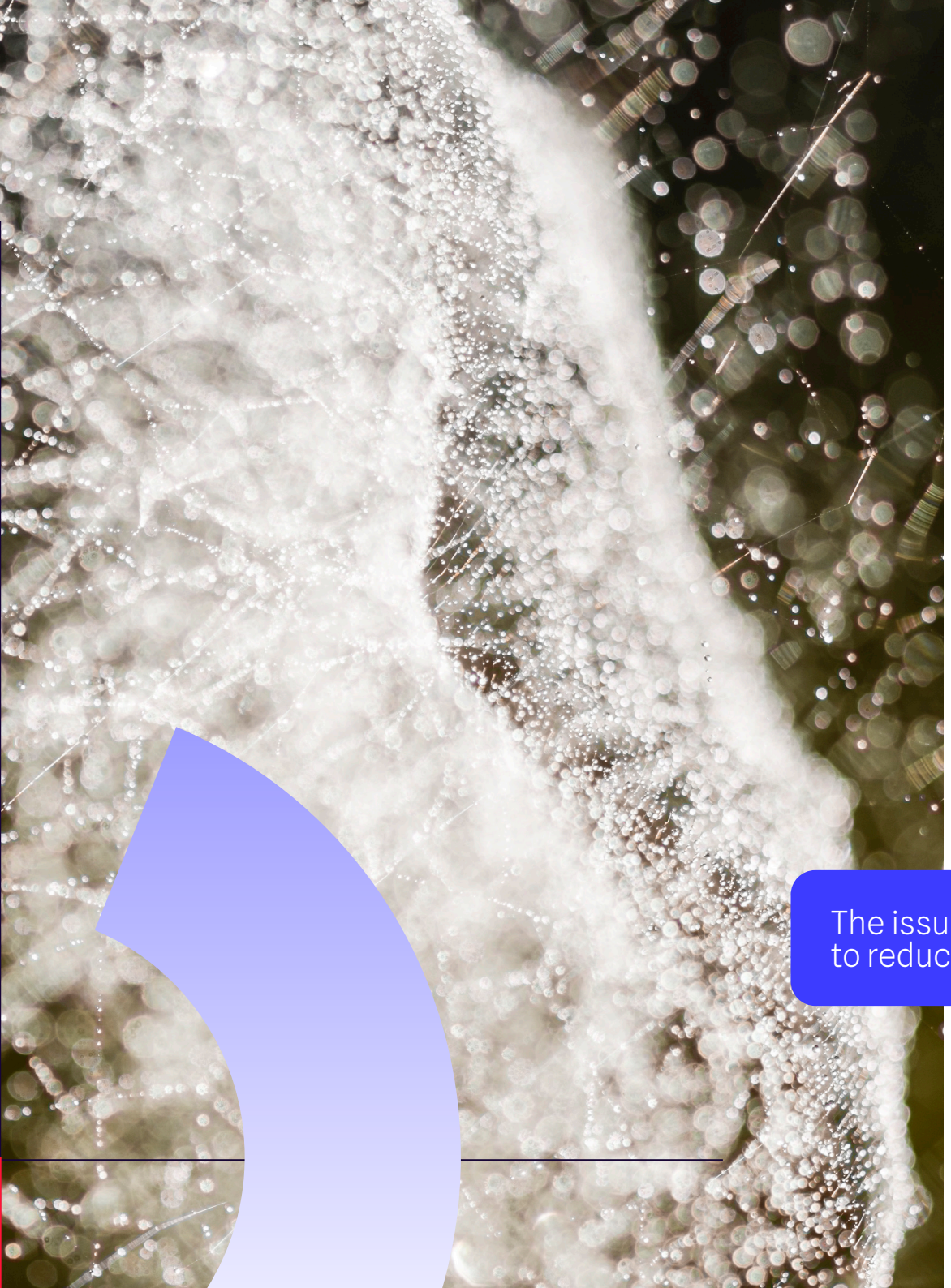
With **instant decision-making**, the aircraft could have made it back to LaGuardia**.** The gap is simple: **human decision time**.

Sully did exactly what a human must do: interpret, doubt, validate. Those seconds of understanding, or time of confusion, made a difference that day.

Now imagine reducing that time. Not replacing the pilot, but **compressing the path to clarity.** With immediate, structured insight, the decision could have come faster. And the outcome might havebeen not just safe lives, but a saved aircraft.

That is the role of modern cybersecurity: not detecting faster, not responding faster, but **deciding faster with confidence.**





4. The expert dependency trap

Today's SOC model relies heavily on a small number of highly experienced analysts.

This creates systemic fragility:

- Decisions depend on individuals, not systems
- Outcomes are inconsistent
- Knowledge is hard to scale
- Talent shortages become critical risks

In some cases, two analysts presented with the same alert will reach opposite conclusions.

The issue is not to replace humans but to reduce dependence on human scarcity.

5. The illusion of visibility

Organizations often equate more tools with better security. In reality,

> Visibility without interpretation can quickly become just noise.

And the data backs this up. Recent industry findings* show that:

> **78% of organizations operate with dispersed and disconnected security tools**
> **69% say this fragmentation creates moderate to significant operational challenges**

This isn't a visibility problem. It's an **operational coherence problem** and there's a second-order effect:

> More tools don't just add noise, they dilute data quality where it matters: indecision-making.

In practice, this fragmentation directly impacts performance:

57% of analysts lose valuable investigation time due to data gaps and poor integration

Adding more detection layers often leads to:

> Redundant alerts
> Conflicting signals
> Increased cognitive load
> Fragmented and inconsistent data context

4 pairs of glasses *won't fix your vision.*

If someone has multiple vision issues, you don't give them four pairs of glasses. You give them one that integrates everything.

Because stacking lenses doesn't improve clarity, it distorts it.

In cybersecurity,
More visibility ≠ More security
More visibility = More responsibility to interpret

*Global State of Security Report Reveals Critical Need for ConnectedSecurity Operations, Splunk, 2025.

Without structured decision-making, visibility becomes a liability_

6. *A new gap: Machine speed vs human cognition*

With the rise of automation and AI, detection is becoming faster and more scalable than ever.

But this creates a new gap:

> Machines generate signals at machine speed
> Humans must interpret them at human speed

This **velocity gap** is widening and it is unsustainable.

The following comparison reflects consistent observations drawn from internal SOC operations and long-term field experience across multiple organizations.

It highlights a structural shift: as decision-making becomes more automated and contextualized, the time required per alert decreases, reducing analyst workload and, as a result, improving operational efficiency and cost control at the organizational level.

Evolution of Operational Paradigms

Metric	*Detection-centric SOC*	*Decision-driven SOC (AI-SOC)*
Primary metric	Alert processed and detection	Decisions made
Detection	**Up to months** (high dependence on manual correlation)	**Seconds** (automated correlation and context building)
Alert volume	Tens of thousands (depending on scale), largely unprioritized. **Between 40% and 60% of alerts are never acted upon.** That creates just as many opportunities for an adversary to gain access quickly and easily to the targeted systems.	Similar volume, **but 100% of alerts are analyzed, prioritized and contextualized**, with a significant reduction inactionable noise. All alerts generated from multiple sources are aggregated, inspected, deduplicated, and analyzed holistically. This is based on acomplete understanding of behaviors across identity, endpoint, network, cloud, and perimeter layers.
Decision & Remediation	**~ 28 days** (industry average, depends on SOC maturity) formaterial remediation. Up to months for economic remediation.	**< 5 minutes** depending on the complexity of the attack and the data sources available, both the analysis and the response can be fully automated by AI (accelerated analysis and prioritization).
Consistency	Varies by analyst	96% consistent decisions
Outcome clarity	Often implicit/undocumented	Explicit: block/step-up/allow

Metric	*Detection-centric SOC*	*Decision-driven SOC (AI-SOC)*
Analyst time allocation	70–80%: triage, data collection, context building. 20–30%: decision-making. The number and complexity of the tools in use can create some variation in the evaluation of the Mean Time To Investigate (MTTI). Nevertheless, the average time required to qualify an incident can be **estimated at between 20 and 40 minutes per alert.**	20–40%: supervision and validation. 60–80%: decision-makingand response. AI integrates natively and seamlessly across the entire technical and business ecosystem. The investigation is automated, delivering analysis results in less than one minute.
Productivity	Limited by human capacity to absorb alert volume, which require ~ **1h/alert.**	Measurably increased (more decisions per analyst, faster execution). Initial results observed inproduction show that the end-to-end handling of a security incident can now be **reduced to just 15 minutes of analyst work**. **This represents a 4x reduction in analyst workload.**
Annual SOC budget (order of magnitude)	~ €20k (SMEs, outsourced) to €15M+ (large enterprises), depending on sector and maturity.	Similar cost structure, but **observed 20–40% efficiency gains** (human time saved).
ROI model	Indirect, difficult to quantify (coverage and detection: number of alerts/incidents detected).	More tangible: **reduced time-to-decision translates into operational cost savings.**
Executive communication and auditability (C-level / board)	Delayed, fragmented, reactive, often lacking context/ comprehension.	Reduced: standardized, traceable, auditable decisions.

Underlying *economic logic*

Traditional SOCs scale with alert volume and therefore headcount. Decision-driven SOCs scale with the ability to **reduce time-to-decision per alert**_

Less human time per decision → More capacity
→ Lower marginal cost

Teams can now :

- Absorb volumes
- Reduce alert fatigue
- Improve decision quality

How & why your *ROI becomes measurable ?*

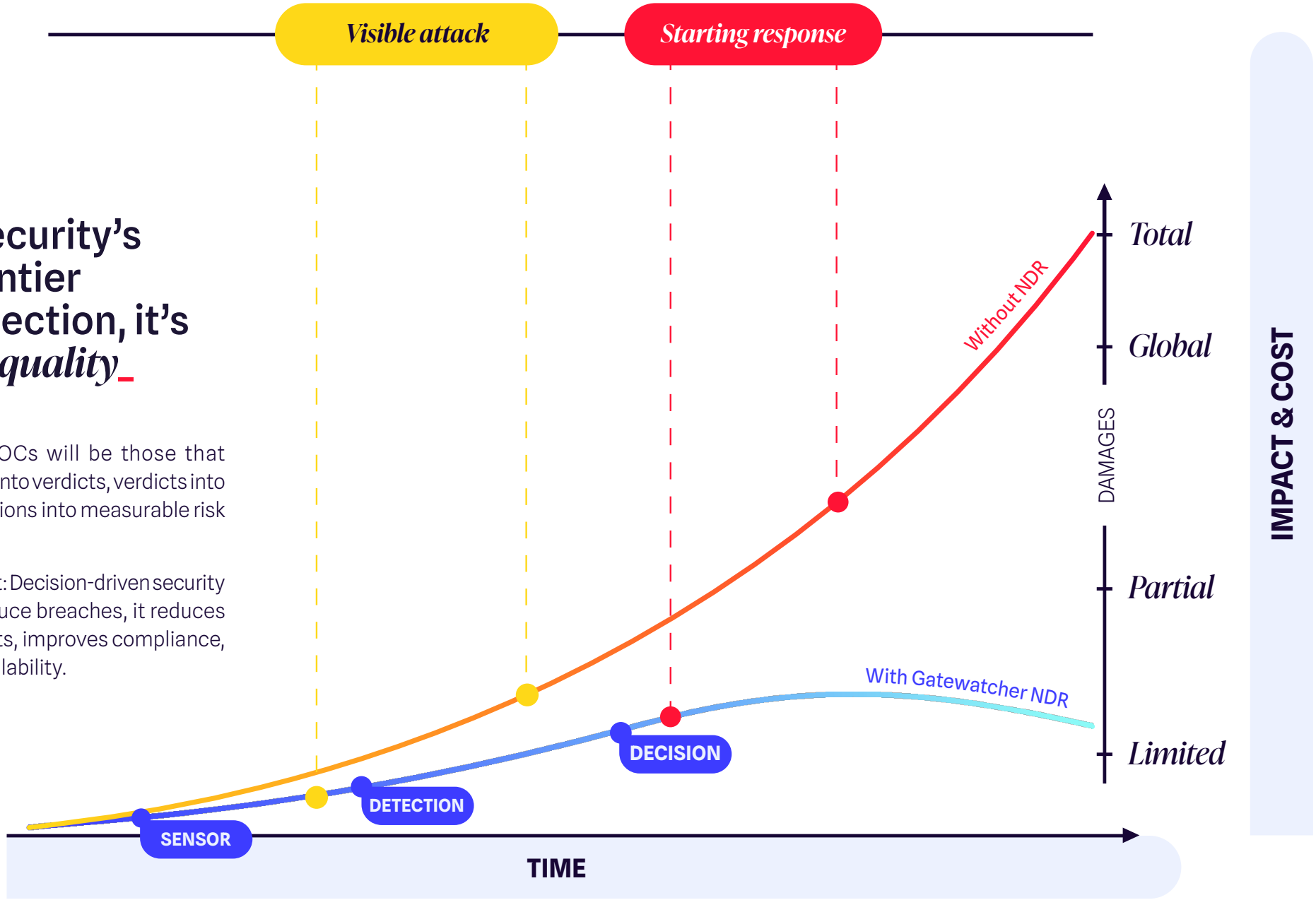
Historically, the ROI of EDR, SIEM, and SOAR platforms was primarily measured through **visibility and detection coverage**.

Today, the ROI of a decision-driven SOC is increasingly defined by operational outcomes: the time saved by analysts, the ability to make faster and more confident decisions, and the capacity to contain threats earlier in the attack lifecycle.

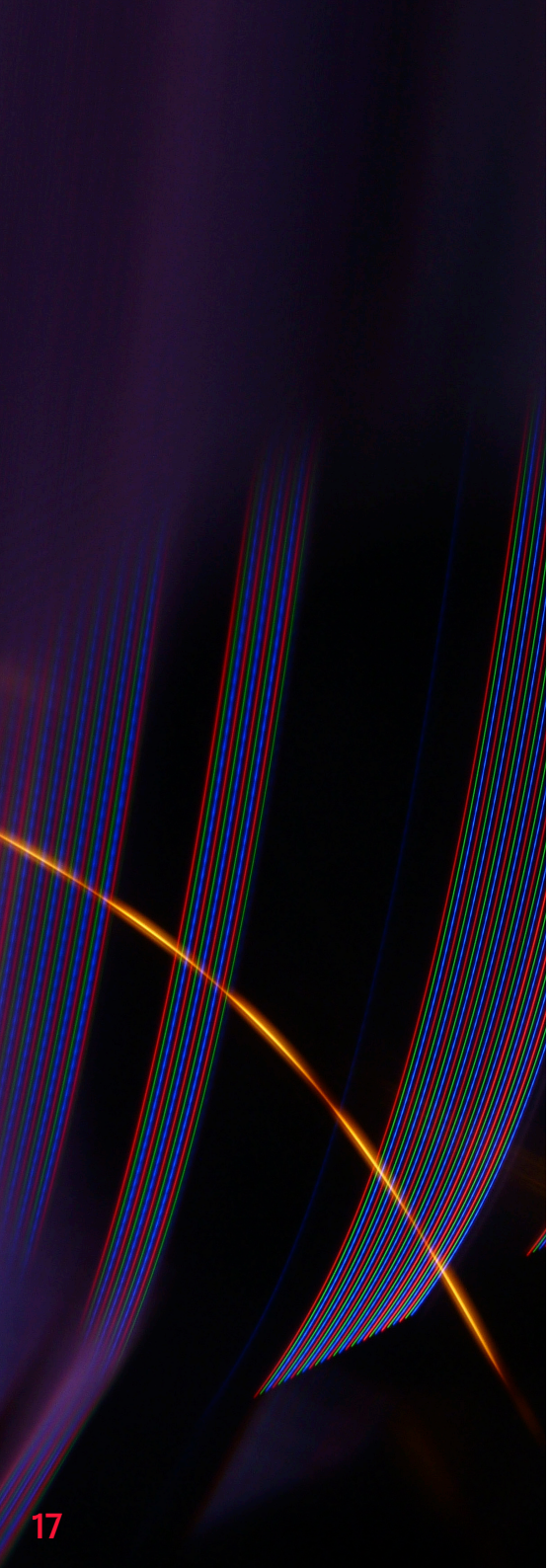
Cybersecurity's next frontier isn't detection, it's *decision quality*_

The winning SOCs will be those that convert signals into verdicts, verdicts into actions, and actions into measurable risk reduction.

Business impact: Decision-driven security doesn't just reduce breaches, it reduces operational costs, improves compliance, and enables scalability.



The Economic Impact of NDR Detection & Response vs. No NDR



02

REDEFINING THE OBJECTIVE OF CYBERSECURITY_

If the detection paradigm created a **visibility revolution,** the next phase of cybersecurity will be a **decision revolution**.

An alert is not an outcome.
A recommendation is not an outcome.
A decision is the outcome.

From a business perspective, an alert has no intrinsic value. Organizations are not looking for more alerts, they are looking for *less uncertainty*_

1. From signals to decisions

In most security operations centers today, the operational model follows a linear process:

Signals → Alerts → Investigation

But this model leaves the most important step largely unstructured: then what?

Most alerts are **technical signals, not actionable evidence.**

Decision-driven cybersecurity is a model where every signal is transformed into a structured, actionable outcome.

Each decision includes:

A verdict: What is happening?
Evidence: Why this conclusion is valid?
Context: Why it matters?
Confidence level: How sure we are?
Recommended action: What to do next?

This transforms security operations from reactive interpretation to **structured judgment.**

The human remains the final decision-maker, crossing the finish line *without having to run the entire marathon alone.*

2. The shift: From volume to impact

One of the most counterintuitive aspects of decision-driven security is that it does not necessarily reduce detection signals.

Historically, many SOCs attempted to control alert fatigue by reducing detection sensitivity.

This approach lowers alert volumes, but it also reduces visibility. Decision-driven security adopts the opposite philosophy.

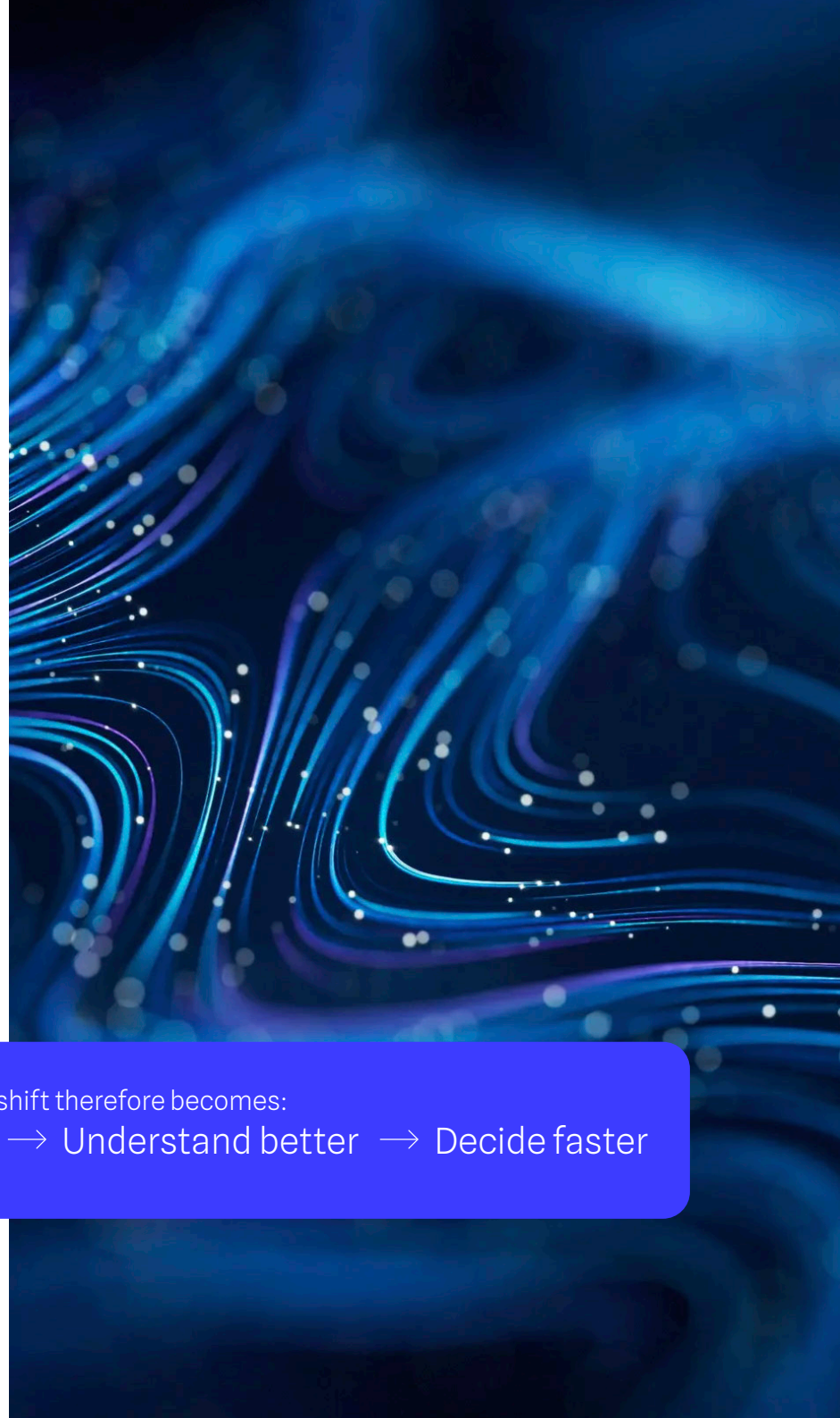
Rather than attempting to see less, the objective is to understand more effectively.

Traditional SOCs operate on a logic of volume:

- Number of alerts processed
- Number of logs ingested
- Number of detections triggered

Decision-driven SOCs operate on a logic of impact:

- Number of decisions made
- Quality of those decisions (triage, prioritization)
- Business outcomes of those decisions

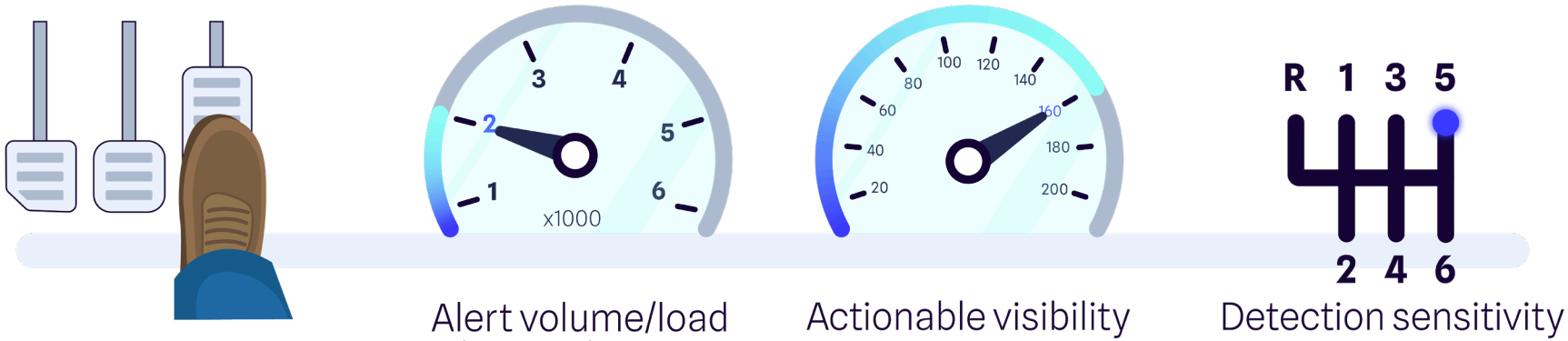


The strategic shift therefore becomes:
See more → Understand better → Decide faster

Sensitive increases volume, *Triage determines values*_

Increasing detection sensitivity is like pushing the engine to higher RPM: Alert volume spikes on the tachometer. But without an efficient gearbox, that power doesn't translate into speed, and visibility stays low. AI-augmented triage acts as a high-performance transmission, converting alert volume into actionable visibility.

AI-Augmented SOC

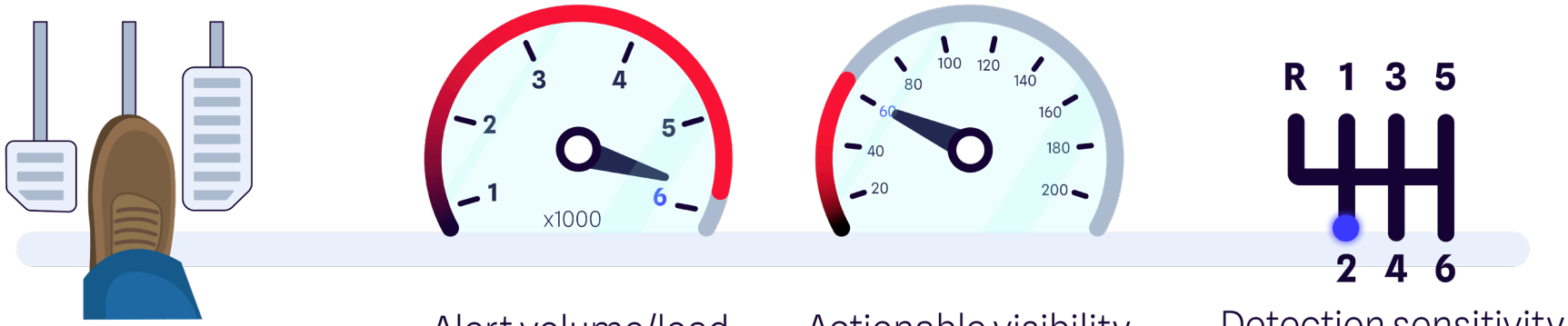


Alert volume/load
with AI-powered triage

Actionable visibility

Detection sensitivity

Most current SOCs



Alert volume/load
with manual triage

Actionable visibility

Detection sensitivity

From Raw Power to Performance: The Driving Force of AI

3. Context is what makes decisions possible

Most alerts are context-blind.
They don't answer:

- Is this asset critical?
- Is this behavior expected?
- What is the business impact?

Without context, prioritization is guess work.
With context, prioritization becomes **deterministic**.

Context beats volume

You don't need more alerts. You need more context per alert. Context is what turns:

Activity → Behavior → Risk → Decision

In practice, making an alert actionable means systematically **attaching the minimum set of business and technical context** required to take a decision without escalation.

For each alert, this includes:

- **Asset criticality**
  production system, revenue-generating asset, internal tool, testenvironment
- **User context**
  role, privilege level, typical behavior, current activity pattern
- **Threat context**
  known attack technique, reputation, similarity with past incidents
- **Exposure level**
  internet-facing vs internal, lateral movement potential
- **Business impact**
  revenue risk, operational disruption, regulatory exposure
- **Historical baseline**
  is this activity normal, rare, or unprecedented for this entity

When this context is present upfront, three things change immediately:

> **Prioritization becomes automatic**
→ critical asset + abnormal behavior = immediate escalation

> **Decisions are faster and consistent**
→ analysts don't need to reconstruct the situation manually

> **Actions are clearer**
→ contain, monitor, or close, without ambiguity

Operationally, this reduces:

> Investigation time per alert
> Unnecessary escalations
> Decision variability between analysts

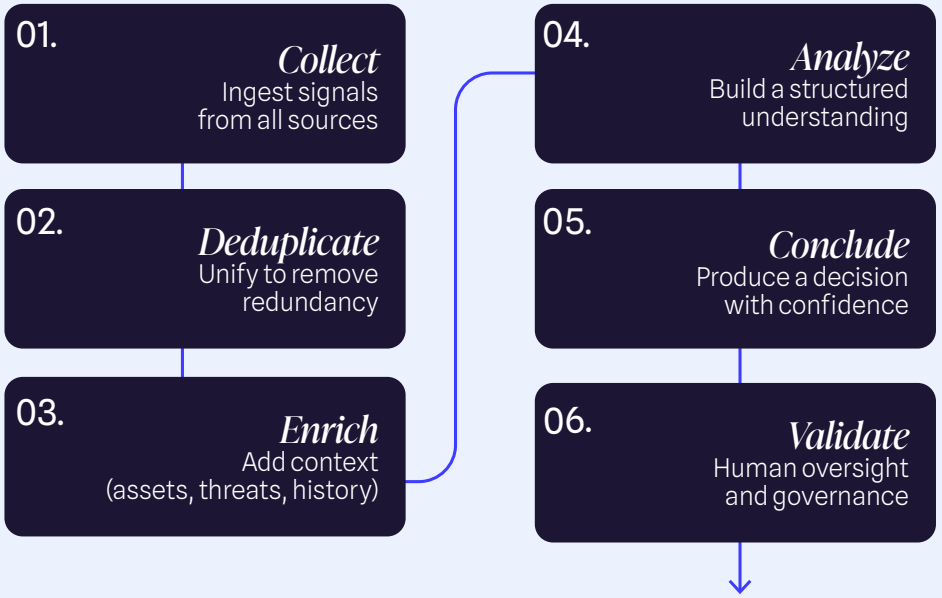
And most importantly, it shifts the unit of work from:

> *From "An alert to investigate"*
>
> to "A situation ready to act on"

4. The decisions pipeline

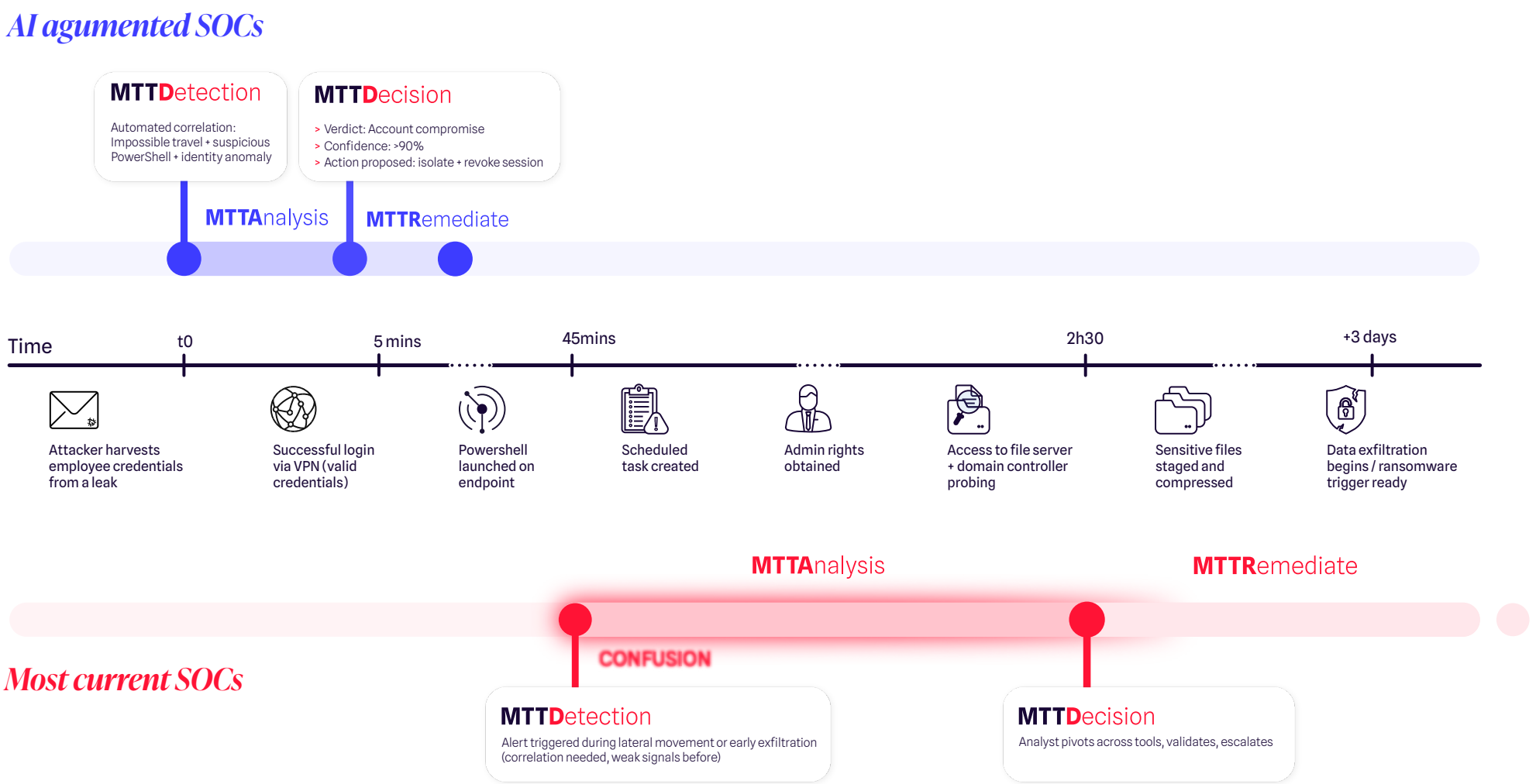
To operationalize this, security workflows must evolve from alert pipelines to **decision pipelines**.

Modern decision-centric workflow:



The ability to transform signals *into fast, high-confidence decisions_*

A SOC Autonomy Level (SAL) operationalizes this by correlating multi-domain telemetry in real time, dramatically compressing time-to-decision and enabling earlier, more decisive response. The result is a measurable shift from late-stage remediation to proactive containment, reducing both operational cost and business risk.



Faster Response and Reduced Risk: The SAL Maturity Model

The goal is to **scale analysts' expertise**, not to replace them

5. *Industrializing judgment*

Today, expert reasoning lives in people's heads.

It is inconsistent, hard to transfer and impossible to scale. Decision-driven security turns this into **structured, repeatable logic.**

Results:

- Junior analysts perform at a higher level
- Decisions become consistent across teams
- Expertise becomes an **organizational asset,** not an individual bottleneck for future refrences or for board feedbacks.

In effect:

Your best analyst becomes *your operating model*_

6. Closing the structural gaps of detection-centric SOCs

Introducing a decision layer resolves the core limitations of traditional SOCs:

> The context gap_

Context is embedded directly into analysis, no more manual reconstruction.

> The evidence gap_

Raw signals become **structured proof chains** linking events, behaviors, and threats.

> The governance gap_

Each alert should produce a **Decision Contract**: a standardized, business-readable output that turns analysis into a clear, accountable decision, so that every decision becomes a **traceable artifact**:

- **Verdict** (What decision was made?)
- **Evidence and reasoning** (Why it was made?)
- **Rationale and confidence** (What evidence supported it?)
- **Action plan** (What was done?)
- **Governance and validation** (Who validated it?)

Aligned with frameworks like **NIS2, DORA, ISO 27001** that require explainability, auditability, traceability.

You don't fail audits because you lack tools. You fail because you cannot explain your decisions.

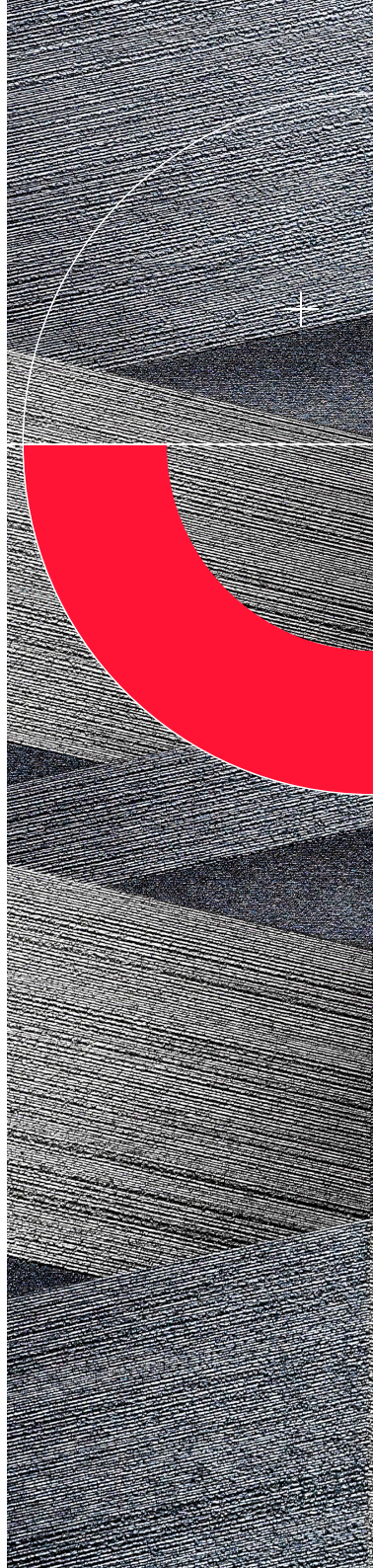
> The scalability gap_

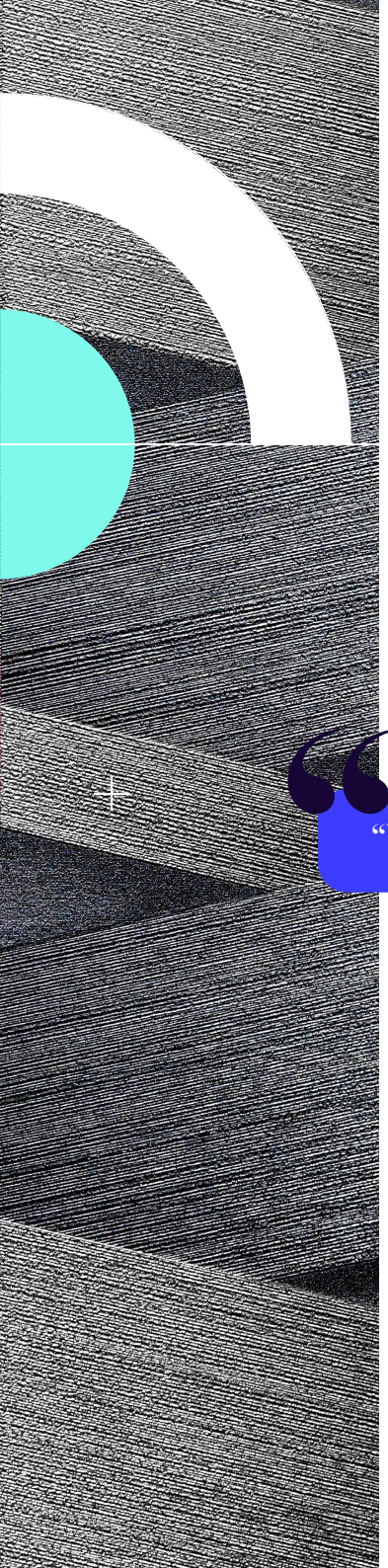
Expertise is systematized, reducing dependence on scarce senior analysts.

> The integration gap_

This does not replace SIEM, EDR, NDR, or SOAR. It sits above them and intergrates seemlessly.

A **decision layer** that translates fragmented signals into coherent judgment.





A new operating model:
Measuring what actually matters

This shift is not just technical. It's operational.

Traditional SOC:
Optimized to process alerts

Decision-driven SOC:
Optimized to produce decisions

This changes how performance is measured.

"*We processed 10 000 alerts*"

"We reduced risk exposure by 30%"

New metrics emerge, business-critical questions:

TIME TO DECIDE (not just detect)
The time required to turn a signal into avalidated decision.
How fast can we decide?

DECISION QUALITY AND CONSISTENCY
The accuracy and repeatability of outcomes across similar situations.
Can we trust our decisions?

ACTIONS EXECUTED
The proportion of decisions that lead to concrete remediation or response.
Are decisions actually executed?

RISK REDUCTION PER DECISION
The measurable impact of each decision on the organization's exposure.
Do the decisions reduce risk?

REDISTRIBUTING TIME AND ATTENTION WHERE IT CREATES VALUE
The ability toprioritize high-impact signals over low-value noise.
Are we focusing on what truly matters?

Economic impact
(the missing layer today)

Security spend becomes **partially measurable**

- → Time saved per alert
- → Decisions accelerated
- → Incidents contained earlier

Ability to translate into concrete numbers

- → Hours saved per week
- → Incidents handled per analyst
- → Reduction in escalation time

This creates something most SOCs lack today:

A direct link between security operations and financial efficiency_

Immediate benefits

95% Reduction in alert noise + 10x Faster triage + 60% Cost reduction = Reduce Ambiguity and SOC Fatigue + Average decision time (*MTTD*) < 5 min

Strategic impact

Budget goes where it matters

→ from alert processing to risk reduction.

Investment decisions become rational

→ based on time, capacity, and impact, not just tooling.

Security aligns with business performance

→ faster decisions = lower exposure window = lower cost of incidents.

This is not a tooling improvement.
It is a shift from spending on detection...*to investing in decision speed*_

Real-world scenario: *The anatomy of a decision*

ENTERPRISE SOC - DECISION AUTOMATION AT SCALE_

Your challenges.

SOC teams are confronted with a continuous and growing flow of security signals generated by multiple, often siloed tools. Each alert requires **analysis, contextualization, and decision-making,** creating a strong dependency on human intervention.

This results in slower response times, increased cognitive load, and ultimately a model that struggles to scale while maintaining consistency.

Your needs.

Moving beyond this limitation requires a shift toward a **decision-driven SOC model.** This starts with the ability to centralize and structure signals, unifying data across tools, removing redundancies, and rebuilding a coherent view of each situation.

On this foundation, organizations can accelerate decision-making by reducing the time between detection andaction, while automating analysis and contextualization to produce **actionable outcomes in real time.**

Scalability then becomes achievable: the SOC can handle increasing volumes without proportional growth in resources, while significantly **reducing analyst cognitive load.**

At the same time, ensuring reliable and consistent decisions remains critical, through impact-based prioritization, homogeneous response strategies, and full **traceability of decisions.**

In this context, **decision automation becomes essential.** By combining multi-source correlation, behavioral analysis, and **AI-driven investigations**, it becomes possible to generate contextualized attack scenarios and deliver structured decisions, including a recommended verdict, a confidence score,and a clear action plan. These decisions can then be automatically executed or orchestrated across the security ecosystem.

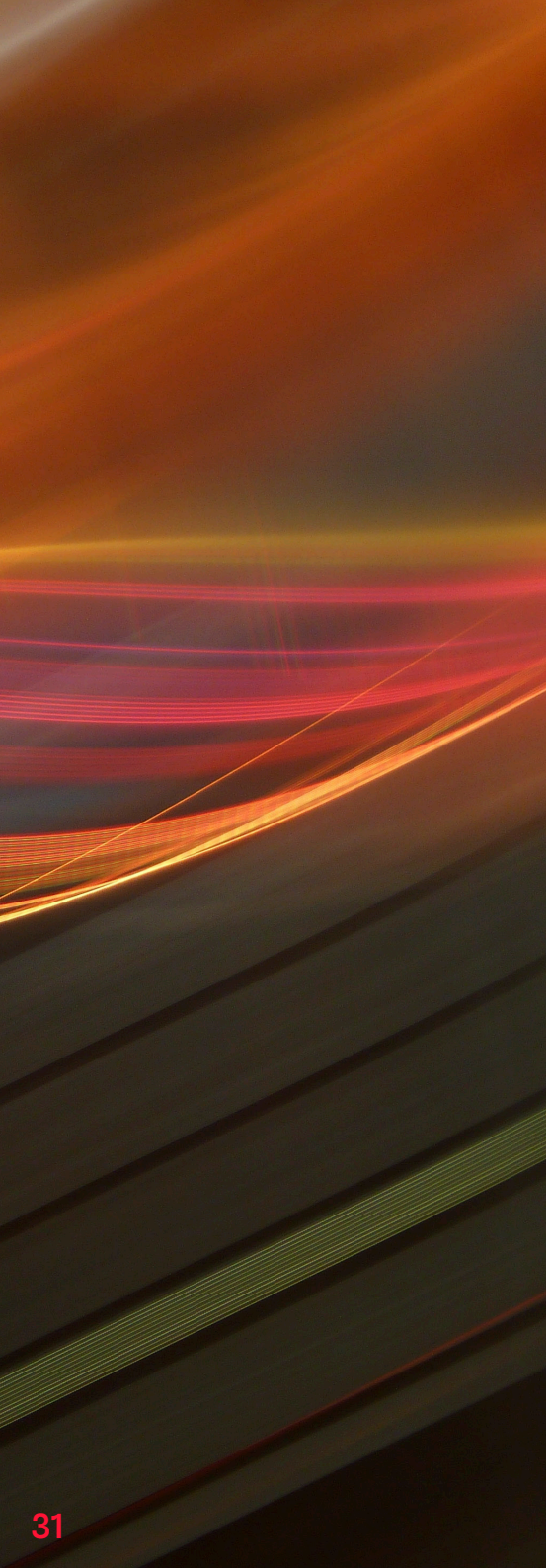
> *"As signal volumes continue to grow, decision automation becomes essential.*
>
> With the **Decision Center**, the SOC evolves toward a model where decisions are structured, contextualized, and generated in real time."

Our approach.

Gatewatcher's technology is based on four key capabilities: **structuring, qualifying, deciding, and executing.**

It unifies signals from NDR, SIEM, EDR, and cloud environments, reconstructs context (assets, users, behaviors), and consolidates alerts into structured cases. Incidents are then intelligently prioritized to reduce reliance on manual analysis and ensure consistent decision-making. Automated correlation and anomaly detection support AI-led investigations, producing contextualized attack scenarios.

Finally, decisions are formalized with a **recommended verdict, confidence score, and action plan,** and can be automatically executed or orchestrated across the security ecosystem, ensuring scalable and consistent response.



03

MAKING DECISION-DRIVEN SECURITY REAL_

If the objective of security shifts from detecting threats to making decisions,then the question is no longer what tools to add, but **how to redesign operations around decisions.**

This can be expressed operationally:

$$\textit{Decision Velocity} = \frac{\textit{Context} \times \textit{Automation}}{\textit{Cognitive Load}}$$

In concrete terms:

More context	→	faster understanding, less ambiguity
Better automation	→	less manual enrichment and stitching
Lower cognitive load	→	more consistent, higher-quality decisions

The question is no longer conceptual. It becomes operational: **What needs to be put in place to increase decision velocity in day-to-day workflows?**

1

Start with augmentation, *not replacement*

Decision-driven security is not a rip-and-replace model.

It:

- Integrates with existing tools (multi-source)
- Enhances current workflows
- Progressively restructures operations

2

Combine AI and human governance

The future is not full automation. It is **decision acceleration with human control.**

- Machines structure and analyze
- Humans validate and arbitrate

At the core sits a **Trust Score**:
A business-facing confidence indicator that tells you how reliable a decision is before you act.

It reflects four simple questions:
Is the evidence strong? Is it complete? Does it agree across sources? Does it make sense in context?

The score rises when multiple high-quality signals align (e.g., identity, endpoint, behavior) and drops when data is incomplete or contradictory, automatically triggering a **human review threshold** to ensure critical decisions remain controlled.

Trust requires control
Automation without explainability creates risk.

Decision systems must be:

- Explainable
- Auditable
- Controllable

3

Build around five *core capabilities*

- Signal unification
- Asset-centric prioritization
- Evidence enrichment
- Confidence scoring
- Human validation

4

Change what *you measure*

Move from:

- Alerts processed
- Events ingested

To:

- Decisions made
- Decision time
- Decision consistency
- Business impact

5

Evolve the role of the SOC

From:
Alert processing center

To:
Decision engine of the organization

*Conclusion*_

The momentum of cybersecurity *starts now*

> For 20 years, cybersecurity has asked:
> *"How do we detect more threats?"*
>
> The next 20 years will ask:
> *"How do we accurately decide faster?"*

Cybersecurity is entering a new phase of maturity. Detection has become abundant, scalable, and increasingly commoditized.

What differentiates organizations now is not what they see, but how fast and how well they decide.

This is why MTTD must evolve.

From Mean Time to Detect, to Mean Time to Decision:

The time it takes to turn uncertainty into a confident, actionable outcome.

This shift is not only operational, it is structural. As attack cycles accelerate and the time to exploit continues to shrink, defenders face a growing asymmetry: machine-speed attacks versus human-speed decisions.

In this context, the real risk lies in the time it takes to understand. Reducing this "time of confusion" becomes essential, as every delay directly increases exposure. Deciding faster is no longer about efficiency, it is about staying within the window where action still matters.

This shift changes how security is built, how it is measured, and how it delivers value:

- From tools to outcomes
- From activity to impact
- From cost centers to decision systems

It also redefines the economic role of security. By accelerating and standardizing decision-making, organizations can **reduce operational inefficiencies, optimize analyst time, and limit the financial impact of incidents:** from containment costs to business disruption.

In this model, security becomes measurable in the only unit that matters to the business:

Faster, better decisions that reduce risk. And do so with greater operational and financial efficiency.

The leaders of this next era won't be those with the most visibility. They will be those who have turned decision-making into a scalable capability.

About us_

A leader in cyber threat detection, Gatewatcher protects enterprise and public-sector networks worldwide – including the most critical. It delivers full network visibility through an AI-driven NDR platform that analyzes activity across cloud and on-premise environments. Its Decision Center transforms security signals into actionable, governed decisions by unifying data from network, endpoint, cloud, and identity sources, improving SOC efficiency and response times.

gatewatcher.com

Explore our solutions.....

contact@gatewatcher.com
+33 (0)1 44 51 03 93
Campus Cyber • Puteaux, France

GATEWATCHER
GATEWATCHER Official
@GATEW4TCHER