$4.44M average breach cost. 30% of alerts ignored.

2025 reshaped cybersecurity.
2026 will redefine resilience.

Cybersecurity in 2025. Forecast for 2026.

Trends, costs and the role of nextgen cyber platforms

nextgen
Cyber Report
2025/ 2026

Powered by
CYBERQUEST
NETALERT

DECEMBER 2025 © nextgensoftware.eu

Table of contents

Table of contents

Table of contents

CYBERSECURITY FORECAST FOR 2026

From Automation to Autonomy -
What might shape the year ahead

2026 could be the year **cybersecurity shifts from reactive automation to autonomous orchestration**.

The focus for CISOs may move from “detect faster” to “prove trust continuously.”

1.1 Strategic outlook

2026 could be the year when automation begins to act, not just react.
For over a decade, SOCs have relied on rule-driven logic and conditional playbooks that accelerated tasks but still depended on constant human curation.

The next phase might see **orchestration engines that evaluate risk, prioritize cases and adjust their own rules within predefined guardrails** - creating a partial shift **from automation to autonomy.**

This would not remove analysts but reposition them as supervisors of machine judgement, verifying exceptions rather than initiating every step.

Possible drivers:

- **AI policy engines** might evolve from recommendation tools into semi-autonomous control layers.
- **Regulatory convergence between DORA, NIS2 and the upcoming EU AI Act** should tighten links between security evidence and compliance proof.
- **Identity-as-Infrastructure** could replace the perimeter firewall as the defining control surface.
- **Data-sovereign architectures** are likely to dominate European SOC design as localisation rules mature.

At board level, attention may also drift from the speed of detection to the credibility of evidence. A faster alert no longer satisfies regulators or insurers if the underlying data trail cannot be verified.
"Proving trust continuously" could therefore become the key differentiator between compliant and non-compliant organizations. ***Systems able to timestamp, sign and correlate events automatically - while maintaining auditability for DORA, NIS2 and soon the EU AI Act - would define operational maturity*** more effectively than traditional metrics such as mean time to detect (MTTD).

These trends suggest a convergence of **technology and governance**.

Identity, policy and architecture may blend into a single control layer where every event carries both security context and legal provenance.

In that sense, **2026 might not simply extend cybersecurity - it could begin to redefine what operational resilience means** inside a regulated digital economy.

1.2. Forecast Indicators for 2026

The challenge: coherent integration of technologies, owning automation and governing it.

The outlook for 2026 points to sharper divides: costs may edge higher overall, but **organisations that fuse automation with verifiable evidence** could outpace others in both speed and credibility.

Efficiency alone won't define maturity, yet governed autonomy will.

Breach economics in 2026 might stabilize nominally yet hide growing divergence between well-automated and legacy environments.

The global average cost per breach could edge upward to around USD 4.6 million, a modest rise driven by inflation, ransom payouts and the spread of AI-assisted fraud. However, **automation-led organizations might still see reductions in effective loss per incident**, as faster triage and verified evidence shorten insurance negotiations and regulatory exposure.

Lifecycle duration may continue to compress.
If autonomous pipelines gain traction, the **median containment time could fall below 220 days**, mainly through improved correlation at ingestion and automatic context-building. Yet this gain would depend on sustained investment in validation and model oversight: a **self-optimizing SOC without human calibration might expose itself to silent drift or false confidence.**

Identity-linked attacks are expected to pass 60% of all cases, reflecting the persistence of compromised credentials, misused tokens and cloud privilege escalation.

While many firms report near-total adoption of MFA, adversaries increasingly exploit legitimate identity channels - delegated access, OAuth abuse and cross-tenant impersonation - that traditional controls overlook.

Automation penetration itself could reach 80% of SOCs, though full orchestration will likely remain limited to early adopters.

Compliance workloads should lighten considerably as **DORA-aligned reporting becomes built-in rather than manual**, cutting effort from hours to minutes per case. Analyst turnover might drop accordingly, provided organizations invest in ergonomic tooling and **psychological safeguards against "machine-supervision fatigue."**

In essence, **2026 forecasts point toward a bifurcated landscape**: a small cohort operating near-autonomous, resilient SOCs, and a larger base still struggling to link fragmented telemetry into defensible evidence.

The challenge for most will not be technology acquisition but coherent integration - the difference between owning automation and governing it.

1.3. Forecast comparison: 2025 vs. 2026 Indicators

Key estimates shaping cybersecurity planning for CXOs and SOC leaders:

- **Purpose:** Support strategic and operational alignment for the year ahead.
- **Focus areas:** Cost evolution, detection speed, identity threats, automation, compliance, workforce stability.
- **Use case:** Anticipate impact, adjust budgets, prioritize automation and resilience.

Forecasted KPIs – 2025 vs. 2026

(These figures are directional, not prescriptive, as volatility remains high)

Indicator	2025 baseline	2026 outlook	Observation
Average breach cost	USD 4.44 M	**≈ USD 4.6 M**	Upward drift from AI misuse & inflation
Median lifecycle	241 days	**≈ 220 days**	Autonomy could compress detection cycles
Identity-linked attacks	48%	**60% +**	Privilege escalation trends persist
SOCs using automation	68%	**≈ 80%**	Orchestration may become standard
Manual compliance work	62%	**≤ 25%**	Embedded reporting expected
Analyst churn	25%	**15 % or lower**	Better ergonomics if autonomy succeeds

1.4. Threat evolution

Next year attackers may exploit the same AI advances defenders rely on, turning automation into a contested domain. **Synthetic identities** - complete with fabricated histories, biometric data and behavioral patterns which could undermine traditional verification, forcing SOCs to analyze intent rather than credentials. **Adversarial AI may generate convincing but transient threats**: adaptive phishing written in natural language, polymorphic payloads that evolve mid-campaign, and noise floods engineered to desensitise automated filters.

In parallel, **telemetry poisoning might become a strategic weapon**. By inserting corrupted data into shared ML pipelines, adversaries could distort training baselines for months, subtly degrading model accuracy without tripping alarms. This risk is particularly acute in vendor-managed or federated analytics environments, where poisoned updates propagate widely before validation.

The rapid adoption of password-less authentication and device pairing could introduce new fragility: what analysts call ***credential entropy collapse***. Trust shifts from users to devices, yet devices themselves may lack independent verification, allowing silent impersonation. As machine-to-machine interactions multiply, proving identity could depend as much on contextual telemetry and cryptographic attestation as on human oversight.

Taken together, these developments suggest that 2026 might redefine the adversarial landscape: **not simply attackers breaching defenses, but algorithms probing the credibility of other algorithms.** Cybersecurity could become a contest of model governance rather than malware signatures.

Threats in 2026 could become less about code and more about **corrupted context**, where **adversaries target the data and models defenders depend on**.
Resilience will hinge on validating trust itself - of identities, devices and the algorithms interpreting them.

Key Takeaways:

- **Synthetic identities** could erode traditional trust anchors; attribution may depend on intent analysis rather than credentials.
- **Adversarial AI** is expected to mature, producing adaptive phishing, obfuscated payloads and false-positive floods.
- **Telemetry poisoning within shared ML supply chains** might distort behavioral baselines for months before detection.
- **Credential entropy collapse in password-less ecosystems** may expose unverified device pairings as unseen weak points.

1.5. Regulation & Governance

Regulation in 2026 might evolve from static compliance to continuous assurance.

The **EU AI Act** is set to formalize requirements for transparency and human oversight in security algorithms, compelling SOCs to document not only what their AI decides but why.

DORA could mature into coordinated digital resilience exercises that test financial and ICT providers as ecosystems, rather than isolated entities, while **NIS2 audits** may shift focus from incident summaries to reproducible, time-stamped evidence.

Compliance may no longer be about reporting after disruption but **proving resilience while operating**.

Those who build transparency into the pipeline from the outset should navigate tightening oversight with minimal friction.

Governments are also expected to **pilot real-time compliance interfaces**, allowing regulators to query anonymized telemetry streams directly instead of waiting for post-incident submissions.

For many organizations, this will demand architectural readiness: **evidence capture and signing at source** long before any alert is raised.

1.6. Architectural trajectories

Architectural thinking in 2026 could move decisively toward local intelligence, global assurance. **As sovereignty and energy efficiency reshape digital infrastructure, Lean + Local SOCs may become the dominant model** - compact, modular deployments capable of analyzing encrypted data in place rather than exporting it to central clouds. This approach not only satisfies residency mandates but also reduces latency and exposure, creating faster and more accountable detection loops.

The principle of zero-copy telemetry and so bringing analytics to the data rather than data to analytics - might emerge as the technical standard for cross-border collaboration. In parallel, autonomous pipelines could begin managing their own feedback cycles, adjusting enrichment, correlation and prioritization dynamically while flagging anomalies that fall outside defined tolerances. Human analysts would intervene only for validation or policy exceptions, turning oversight into a quality-assurance role rather than a manual bottleneck.

Platforms like CYBERQUEST 2.x might represent the practical frontier of this movement. Their embedded policy agents could justify every AI-assisted decision, produce **AI Act-ready evidence chains** and maintain auditability without increasing overhead: transforming compliance from an add-on into a structural property of the architecture itself.

SOC design in 2026 should prioritize sovereignty, explainability and self-correction.

The winning architectures will be those that **think locally, prove globally and waste nothing.**

1.7. Sector outlook

Sector dynamics in 2026 may reflect both regulatory expansion and technological saturation. In finance, the **integration of algorithmic trading and high-frequency platforms into DORA testing regimes could redefine operational risk**, requiring near-real-time attestation that trading engines remain resilient under cyber or infrastructure stress. The focus may shift from breach prevention to continuity of execution, where seconds of downtime translate directly into financial exposure.

Healthcare is expected to accelerate its digital transformation through connected medical devices and remote diagnostics. This surge in IoT telemetry will demand contextual filtering, ensuring that cybersecurity controls do not interrupt care delivery. Success here will likely rely on automated prioritization, where the system distinguishes between safety-critical and administrative alerts in real time.

In manufacturing, predictive maintenance data could merge with cybersecurity telemetry to form unified resilience dashboards. OT and IT teams might finally share a common language of uptime, anomaly and compliance, blending performance metrics with threat indicators to anticipate both mechanical and digital failures.

The public sector may continue to migrate toward sovereign clouds, choosing jurisdictional clarity over global scalability. Governments could favour EU-native providers that guarantee data residency and enforceable accountability, turning sovereignty into a procurement baseline rather than a differentiator.

Meanwhile, **energy and utilities might adopt digital-twin grids**: virtual replicas of physical systems in order to test resilience against cyber and environmental disruptions before they occur. These simulations could evolve into regulatory

Across all sectors, cybersecurity in **2026 should blur the line between defense and operations**.

Resilience will be measured not by the number of alerts blocked but by the **continuity of essential services under stress**.

1.8. Economic & Geopolitical variables

Cybersecurity economics in the year ahead may depend less on increased investment and more on how effectively budgets translate into measurable resilience.

Automation and lean design could widen the gap between modern and legacy SOCs by over USD 2 million per incident, as simplified architectures reduce investigative drag and licensing sprawl. Compact, energy-efficient infrastructures may continue **saving EUR 100–150 K** per refresh cycle, helping organizations maintain security posture even amid tighter financial climates.

However, **geopolitical turbulence threatens to skew every projection**. Energy shocks, sanctions and **state-sponsored cyber campaigns could inflate breach costs regionally by 10–15 %**. At the same time, supply-chain disruptions, semiconductor shortages and diverging privacy regimes might stall automation projects or fracture data-flow strategies across borders. Fluctuating currencies and differing national **implementations of DORA and NIS2 could further complicate cost modelling** and compliance planning.

Efficiency may deliver savings, but uncertainty will test endurance. **The most resilient organizations will budget for change, not for calm.**

Given these variables, forecasts should be viewed as scenario bands rather than fixed outcomes. Financial and operational resilience will hinge on the ability to adapt: **deployments that stay lean, interoperable and transparent will weather volatility far better than those optimized only for stability.**

1.9. Strategic takeaway and the Road to 2027

The next chapter in cybersecurity might not be written by those with the largest budgets or the most powerful algorithms, but by **those who learn to simplify without surrendering depth**. Complexity has long been mistaken for progress, yet as the digital landscape tightens under new regulations, finite energy and shifting geopolitics, the strongest systems will likely be the ones that do less, faster, and explain every decision they make. Architecture becomes the new intelligence: correlation before ingestion, evidence as a by-product of analysis, and automation that knows when to pause rather than when to act.

The world's defenders may find themselves in a **new discipline altogether: not cybersecurity, but cyber integrity - a space where every log, signature and AI conclusion carries its own chain of trust.** SOCs that can produce this kind of verifiable narrative will gain something rarer than speed: credibility.

Regulators may tighten their grip, but transparency will turn compliance into an ally rather than a burden. Autonomy will matter only if it can prove its reasoning; **AI that explains itself will outlast AI that merely performs**.

This evolution could also mark a cultural shift. The next generation of analysts may work less like firefighters and more like historians - curating context, validating truth and deciding what deserves to endure in the permanent record of digital events.

Platforms like CYBERQUEST stand at this inflection point: not promising omniscience, but offering the humility of systems that know when to show their work.

If the past proved that architecture beats spending, the years ahead could show that **understanding beats automation**. **The future of cybersecurity may belong not to the loudest systems, but to the clearest ones.** And in that clarity lies something revolutionary: a world where proof replaces promise and trust stops being a slogan and becomes a feature.

Key Takeaways:

- **Integrity will outlive speed:** fast is no longer enough; evidence must be self-explanatory.
- **Simplicity becomes strategy:** the fewer moving parts a defence has, the harder it is to break.
- **Autonomy earns trust only through transparency:** machines that justify decisions will redefine assurance.
- **Resilience is now cultural:** it lives in how teams think, not just in what tools they deploy.

2. 2025 Executive summary

Accelerating Resilience: Cyber insights 2025

In 2025, cybersecurity balances progress and pressure: **automation and AI have cut breach times** to record lows, yet the cost of attacks remains high.

True resilience now depends on speed - detecting and containing threats before they escalate.

Cyber risk in 2025 is defined by two opposing curves: **cost and complexity remain high**, yet detection and containment times are falling where organizations adopt automation and lean, integrated workflows.

- **The global average cost of a breach is USD 4.44M**, while the United States hit a record USD 10.22M.
- **The average breach lifecycle has dropped to 241 days** - the fastest in nine years.
- **Organizations using security AI and automation extensively save about USD 1.9M per breach and cut lifecycle time by ~80 days** compared with those that do not.

Sector highlights & SOC realities:

Healthcare remains a pain point:

o 54% of incidents are ransomware.

o Nearly half involve data theft.

o Median major incident cost: EUR 300,000.

SOC realities:

o One large dataset in 2024 distilled ~93,000 confirmed threats from 308 PB of telemetry.

o Identity attacks rose 4×, and VPN abuse emerged as both widespread and difficult to investigate.

Strategic response:

- The most effective change is architectural, not financial.
- **Success comes from**:
  - o Moving correlation and enrichment earlier in the pipeline.
  - o Collapsing duplicate signals into single, enriched cases.
  - o Applying UEBA to rank risk.

o Embedding compliance reporting into the same pipeline as investigations.

Platforms built on lean architecture - including European options such as CYBERQUEST, designed by Nextgen Software (nextgensoftware.eu) - demonstrate how to:

- Reduce “swivel chair” effort.
- Turn repetitive detection into defensible resilience

2.1. INTRODUCTION - THE CYBERSECURITY LANDSCAPE IN 2025

The cybersecurity story in 2025 is a tale of contrasts. On the surface, global averages suggest modest relief: breach costs inched downward and containment times improved. Yet beneath the averages lie structural divides that decide whether an organisation faces a manageable setback or a crippling disruption.

Speed has emerged as the silent multiplier. **When incidents are discovered and contained earlier, attackers have less room for lateral movement, fewer chances to stage exfiltration, and less opportunity to destabilize operations**. In practice, this advantage comes from methodical triage and the consolidation of signals into coherent cases - **not from drowning in duplicate alerts**.

2.2. WHAT PUSHES COSTS UPWARD

While average breach costs hover in the mid-single millions, certain patterns make incidents consistently more expensive:

- **Malicious insiders** and **third-party/supply-chain** compromise remain the highest-cost categories, each nudging towards the five-million mark.
- **Phishing** is still the most common way in, responsible for around one in six breaches globally.
- Exposed **customer PII** and stolen **intellectual property** generate the steepest per-record losses, underscoring why data type matters as much as breach size.

The environment also shapes the outcome. Breaches spanning **cloud, SaaS and on-prem simultaneously** take longer to untangle and cost more than strictly on-premises incidents, largely due to coordination delays and visibility gaps.

2.3. IDENTITY AND CLOUD DEFINE THE FRONTLINE

The past year made it clear that defenders now fight primarily in the identity and cloud domains. Telemetry sets from 2024 show identity-driven techniques quadrupling, with three of the top five attack vectors tied to cloud or identity abuse. VPN misuse sits at the centre of this shift: difficult to investigate, often masquerading as routine administration, but frequently a precursor to ransomware or insider theft.

Without correlation at ingestion, SOCs are forced to handle these events as disjointed alerts. The result is the same narrative repeated across different consoles, with analysts doing manually what the architecture should have solved upstream.

2.4. HEALTHCARE AS A CASE STUDY IN STAKES

The healthcare sector illustrates why alert fatigue is more than an annoyance. European data shows ransomware is present in more than half of sector incidents, often paired with data exfiltration. The financial median for a major incident sits near **EUR 300,000**, but the true cost emerges in **disrupted treatments, diverted ambulances and delayed surgeries.** Here, every redundant alert is not just wasted time but a risk to human safety.

2.5. ARCHITECTURE BEATS SPENDING

What consistently changes outcomes is not bigger budgets but smarter pipelines. Organizations that move correlation and enrichment to the front end of their workflows, rank anomalies with UEBA and push analysts' cases rather than atomized events are the ones bending both curves: **lower cost and lower dwell time.**

The market is responding with leaner platforms that embed compliance and audit-ready evidence into the same workflow. Instead of treating reporting as a separate afterthought, **these systems turn investigative timelines directly into regulator-ready artefacts.**

2.6. MAIN 3 TAKEAWAYS FOR 2025

Faster is cheaper.

The lifecycle curve is consistent: incidents wrapped up in under 200 days cost over a million less than slower cases. The lever is design - correlation, automation and standardised playbooks.

Context is king.

Identity and SaaS metadata, along with agentless visibility in non-agent environments, must be treated as first-class telemetry. Analysts need an attack story, not a dump of raw logs.

Compliance is operational.

Under regimes like NIS2 and DORA, the ability to produce regulator-ready evidence automatically is as vital as stopping the breach itself.

3. BREACH COSTS & LIFECYCLE TRENDS

Headline averages often hide the structural differences that decide whether a breach costs a few million or spirals into systemic disruption. In 2025, the conversation is less about the global mean and more about **where the money goes, how long breaches last, and what kind of environments and industries carry the heaviest burden.**

3.1. WHERE THE MONEY GOES

The largest slice of cost in 2025 remains detection and escalation, accounting for roughly a third of total impact at about **USD 1.47 million per breach**. Encouragingly, that figure has fallen by around 10% year over year, but the improvement is uneven:

- **Automated SOCs** have trimmed investigative overhead substantially.
- **Manual-heavy teams** still spend at similar levels as last year.

By comparison, **legal and regulatory response sits steady around USD 1.3-1.5 million**, while **lost business varies sharply by sector**. This distribution shows where savings are most achievable: cutting downtime is difficult, but trimming investigative overhead is operationally within reach.

3.2. THE LIFECYCLE DIVIDE

Time is the most reliable predictor of cost. In 2025:

- Breaches **under 200 days** averaged **USD 3.87 million.**
- Those stretching **beyond 200 days** averaged **USD 5.01 million.**

The difference is more than statistical. **Longer dwell times mean attackers have space to pivot laterally, persist across systems and stage exfiltration.**

Progress is visible: organizations are spotting anomalies earlier, but many still struggle with escalation and resolution. The culprit is often fragmentation - alerts arriving separately instead of as unified cases. Analysts lose weeks reconstructing what should have been visible at ingestion.

3.3. ENVIRONMENTS MATTER

The operating environment dictates complexity and cost:

- **Multi-environment breaches** (cloud, SaaS, and on-prem combined) averaged **USD 5.05 million**, with a lifecycle close to **276 days**.
- **On-premises-only incidents** were cheaper and faster, averaging **USD 4.01 million** and **217 days.**

Although the share of multi-environment cases fell slightly (to 30%), they remain disproportionately expensive. Hybrid estates multiply investigative complexity unless telemetry is normalised and correlated from the outset.

3.4. INDUSTRY- SPECIFIC PRESSURES

Different sectors absorb breach costs in different ways:

- **Healthcare is still the costliest**, averaging USD **7.42 million per incident** and taking **279 days** to contain. Beyond the financial toll, downtime here disrupts patient care.
- **Finance faces a dual hit**: **fines and fraud**. In 2025, "**shadow AI**" misuse appeared as a measurable cost driver, adding an average of **USD 670,000** to breaches where staff used unsanctioned tools.
- **Manufacturing and energy suffer most from downtime**, where every halted production line or disrupted grid can cost millions per day. With **NIS2 enforcement beginning in 2025**, downtime also doubles as a compliance failure.

3.5. AUTOMATION AS THE COST EQUALISER

The gulf between automated and manual responders continues to widen:

- Organizations with **extensive automation** reported **USD 1.9 million lower average breach costs**.
- They also **shortened breach duration by around 80 days**, reducing losses in detection, escalation and lost business.

Automation at scale now means more than scripted responses. It includes **UEBA scoring, automated forensic enrichment** and **compliance-ready workflows** that generate regulator-aligned reports as a by-product of incident handling.

European platforms like **CYBERQUEST (Nextgen Software)** demonstrate this in practice with **270+ pre-built connectors** and **1,200+ automated actions**, ensuring that dozens of fragmented alerts arrive as a single enriched case, complete with audit evidence.

3.6. THE STRATEGIC VIEW

The real story is variance.
While global averages suggest a downward trend, the gap between leaders and laggards is widening:

- **Manual-heavy SOCs** continue to face breaches **over USD 5 million**.
- **Automation-led teams** consistently shave millions off exposure.

The takeaway isn't to spend more indiscriminately, but to spend differently - prioritizing architectural efficiency over module sprawl. In 2025, resilience is measured not just in money saved but in **days cut from the lifecycle, alerts collapsed and regulator-ready evidence produced automatically.**

4. ALERT FATIGUE & DETECTION BURDEN

Every breach cost statistic hides a more human reality: **security operations centres are drowning in alerts.** For many SOC teams, the daily flood of notifications has become as dangerous as the breaches themselves. It erodes focus, fuels burnout, and creates direct blind spots where threats slip through.

4.1. THE SCALE OF THE PROBLEM

Industry telemetry in 2025 quantifies the overload.

- **308 petabytes of telemetry** across **4 million+ identities, endpoints and cloud assets** produced **nearly 30 million investigative leads**.
- From this mountain, analysts confirmed only **~93,000 real threats** - a hit rate of just **0.3%.**
- Of these, **25,000 incidents** were high-severity enough to require escalation.

This inefficiency means analysts are forced to wade through irrelevant or redundant data for every genuine compromise they uncover. **The imbalance between volume and value is at the core of modern alert fatigue.**

4.2. HUMAN COSTS

The operational toll on analysts is measurable:

- Studies show SOC teams **ignore or dismiss up to 30% of incoming alerts**, not through negligence, but necessity.
- Burnout drives **churn rates above 25% annually - among the highest in IT.**
- Replacing a trained analyst typically **takes 6-12 months**, compounding the cost of every resignation.

Every redundant alert pushes skilled staff closer to the door, undermining resilience not only at the system level but within the team itself.

4.3. SECTOR EXAMPLES OF FATIGUE

The **healthcare sector** demonstrates the risks of unchecked noise. ENISA's dataset of **215 incidents (2021-2023)** revealed:

- **54% involved ransomware**, often paired with exfiltration.
- **43% of ransomware cases** included confirmed data theft.
- Patient data was the top target in **30% of incidents.**

The consequences are not just financial. Hospitals reported **diverted ambulances, delayed surgeries and cancelled treatments** - outcomes directly tied to stretched staff and clogged detection pipelines.

In this context, **alert fatigue becomes a clinical hazard**, not just an IT problem.

4.4. WHY VOLUME MULTIPLIES RISK

Identity-driven attacks illustrate the challenge:

- **Malicious cloud account creation** and **suspicious email forwarding rules** surged in 2024, ranking among the **top five MITRE techniques globally**.
- These appear superficially like routine admin activity, generating **ambiguous alerts that require context to validate**.
- **Without correlation at ingestion, SOCs drown in lookalike notifications** or miss them altogether.

Attackers exploit this ambiguity. The more defenders are forced to sift manually, the longer adversaries enjoy undetected dwell time.

4.5 BREAKING THE CYCLE

The solution lies less in hiring more analysts and more in redesigning pipelines:

- **Deduplicate at source**, collapsing repetitive alerts into enriched cases.
- **Apply UEBA scoring to rank anomalous identities** and assets by risk.
- **Shift toward case-centric timelines** that give analysts context rather than fragments.

When correlation is performed upstream, analysts see the attack narrative once, instead of piecemeal across consoles. This reduces noise, preserves analyst focus, and accelerates decision-making.

The lesson of 2025 is stark: sheer data volume will only increase, but the teams that succeed are those who treat correlation and enrichment as architectural necessities, not optional add-ons. Without that shift, alert fatigue will remain the breach vector no adversary ever needs to exploit directly.

5. COMPLIANCE PRESSURES - DORA & NIS2

Cybersecurity in 2025 is not only about defending data but **proving resilience under regulatory scrutiny.**

The twin forces of the **Digital Operational Resilience Act (DORA)** and **NIS2 Directive** have transformed compliance from a back-office chore into a strategic, board-level obligation. **Fines, investigations and even personal liability for executives mean compliance** is now inseparable from security architecture.
Organizations no longer ask "how secure are we?" but rather "**can we demonstrate it to regulators within hours?**"

5.1. DORA - RAISING THE BAR IN FINANCIAL SERVICES

DORA came into force across the EU in January 2025, with a sharp focus on banks, insurers, investment firms, and ICT service providers. **Unlike GDPR, which centered on personal data, DORA reframes the conversation around operational resilience during severe IT disruptions.**

DORA's five core pillars are:

1. **ICT Risk Management** - full lifecycle controls for digital risk.
2. **Incident Reporting** - initial, intermediary, and final reports on major incidents in standardised templates.
3. **Digital Operational Resilience Testing (DORT)** - periodic testing, including red-team style assessments.
4. **Third-Party Risk Oversight** - contractual and operational supervision of ICT providers, particularly in cloud outsourcing.
5. **Information Sharing** - structured collaboration across financial entities for threat intelligence exchange.

The reporting requirement is the most disruptive. Institutions must submit incident reports within hours, backed by **forensic, audit-grade evidence** - not just narrative summaries. Logs must be **digitally signed and time-stamped** to survive regulator's scrutiny months later.

For **global financial groups**, the complexity multiplies. A single breach may require **simultaneous reporting under DORA, GDPR and national frameworks**, each with different formats and deadlines.

5.2. NIS2 - EXPANDING THE NET

NIS2, transposed into national law across Europe in 2024-2025, expanded the regulatory perimeter from 7 sectors to 18 essential and important sectors. It now covers industries as diverse as manufacturing, healthcare, energy, transportation and digital infrastructure.

In Romania, NIS2 was transposed as Law 124/2025, validated on 7 July 2025 and entering into force on 10 July. **This explicitly named manufacturing as a regulated sector, forcing production facilities - previously outside the perimeter - to adopt compliance frameworks on par with hospitals and banks.**

THE OBLIGATIONS INCLUDE:

- **Incident Reporting** - notifying national CSIRTs of significant cross-border incidents.
- **Risk Management Measures** - adopting appropriate technical and organizational controls, often aligned with ISO 27001.
- **Governance Responsibility** - **boards of directors are directly accountable, with penalties including fines and disqualification from holding directorships in the EU.**
- **Supply Chain Oversight** - regulated entities must assess and enforce resilience standards with providers.

5.3. THE OPERATIONAL CHALLENGE

The regulatory aims are clear, but implementation is difficult. Obstacles include:

- **Siloed visibility** - IT, OT, and cloud logs remain fragmented, making regulator-ready reports hard to produce.
- **Manual reporting burdens** - under older regimes, compliance meant CSV exports, log parsing, and manual narrative assembly. This is unsustainable under DORA/ NIS2 timelines.
- **Module sprawl** - many SIEM/ SOAR systems require bolt-on compliance modules, each adding cost, latency, and integration effort.

The net result is that **many firms remain "willing but unable": committed to compliance but slowed by tooling gaps, raising both regulatory and cyber risk.**

5.4 EMERGING SOLUTIONS

To close this gap, the industry is shifting toward compliance-by-design architectures.

KEY INNOVATIONS INCLUDE:

- **Digitally signed logs** that preserve evidentiary integrity for years.
- **Case-driven reporting**, where analyst investigation timelines double as audit trails.
- **Multi-framework mappings**, with detections aligned directly to ISO 27001, PCI DSS, GDPR, DORA, and NIS2.
- Automated report generation, triggered the moment a case is escalated, complete with timestamps and enrichment.

European vendors are at the forefront of this model. For example, Nextgen Software's **CYBERQUEST platform integrates compliance-ready reporting into the incident lifecycle: encrypted and signed logs, automated templates for DORA/ NIS2, and OT visibility via NETALERT.** Manufacturers and utilities can now feed industrial telemetry into compliance reports without deploying intrusive agents.

5.5. WHY LEAN ARCHITECTURES MATTER

The architecture itself determines viability.

- **Under DORA**, initial reports may be due within hours.
- **Under NIS2**, CSIRTs expect rapid cross-border notifications.

In a lean design, every case becomes both a security artefact and a compliance artefact. Analysts investigate once, and the system produces both operational outputs and regulator-ready reports.

This avoids duplication, reduces errors and saves dozens of analyst hours per major incident. In practice, it is the only way to keep pace with the accelerated timelines regulators demand.

5.6. STRATEGIC IMPLICATIONS

The rise of DORA and NIS2 signals a structural shift:
CYBERSECURITY IS NOW A REGULATED BOARD-LEVEL FUNCTION.

- **Boards** must recognize compliance as fiduciary duty.
- **SOC leaders** must ensure tooling outputs regulator-ready artefacts without extra work.
- **Regulators** now enforce resilience, not just reporting compliance.

The organizations that succeed will demonstrate resilience as a **market advantage** - winning customer trust and regulatory goodwill. Those that fail face **financial penalties, reputational damage and leadership sanctions.**

5.7. COMPLIANCE PRESSURE WILL ONLY INTENSIFY

The EU has already signalled intent to extend DORA-style resilience requirements into adjacent industries, while member states may adopt stricter interpretations of NIS2.

The winners will be those who view compliance not as an overhead but as an **opportunity to integrate governance, security and continuity**.

Platforms that deliver **audit-ready evidence as a natural output of operations** - as lean architectures increasingly do - will set the new standard.

6. INDUSTRY SCENARIOS SECTOR-SPECIFIC PRESSURES AND PRACTICES

Cybersecurity challenges manifest differently across industries. While ransomware, supply chain compromise, and insider threats are recurring themes, the cost, operational impact, and regulatory environment vary sharply depending on the sector.

6.1. FINANCE - FRAUD AND REGULATORY EXPOSURE

The financial sector remains one of the **most scrutinized industries - by both regulators and adversaries. Breaches here average USD 5.9M - 6.5M**, with fines, litigation and reputational loss accounting for much of the gap across regions.

TWO 2025 TRENDS SHARPENED THE EXPOSURE:

- **Shadow AI misuse**: Staff using unsanctioned generative AI tools to process sensitive data added an average of USD 670,000 per breach where present. This is the first year "shadow AI" became a measurable cost category.
- **Sophisticated fraud campaigns**: Credential theft, insider collusion and supplier compromise now blend into multi-stage attacks. Unlike ransomware, fraud unfolds quietly, accumulating financial loss over weeks or months.

Under DORA, financial institutions must file initial, intermediary and final incident reports, each supported by forensic evidence. This forces analysts to fight active fraud while documenting it for regulators.

Platforms that merge investigative timelines directly into compliance-ready reports - such as **European solutions like Nextgen Software's CYBERQUEST** - show how regulatory and operational demands can be aligned.

6.2. HEALTHCARE - DATA SENSITIVITY AND SERVICE CONTINUITY

Healthcare continues to be both the costliest and slowest-to-contain industry:

- **Average breach cost: USD 7.42M**.
- **Average lifecycle: 279 days**.
- **Ransomware prevalence: 54% of incidents**, nearly half of which also involved data theft.
- **Top target: patient data**, making up 30% of stolen assets.
- **Median cost in Europe: EUR 300,000 per major incident**, with outliers over **EUR 10M** when downtime compounded.

The consequences reach far beyond balance sheets. Breaches have forced:

- **Cancelled chemotherapy appointments.**
- **Diverted ambulances.**
- **Delayed emergency surgeries.**

These operational impacts show why ransomware in healthcare is uniquely severe - **downtime threatens lives.**

Regulatory layers (GDPR fines, national health obligations) intensify pressure. For this sector, **digitally signed, encrypted logs and compliance-ready audit trails are no longer optional** - they are prerequisites for trust and continuity in healthcare.

6.3. MANUFACTURING - IT MEETS OT

With NIS2 expansion, manufacturing has entered the regulated perimeter, facing the same legal scrutiny as banks and hospitals.

The unique cost driver here is downtime:

- **A single day offline** in a high-throughput plant **can cost millions of euros** in lost production and contractual penalties.

Adversaries increasingly target ICS (Industrial Control Systems) and SCADA networks, often by pivoting through IT networks or poorly segmented VPNs.

Challenges include:

- **Agent limitations:** OT systems often cannot host endpoint agents or tolerate intrusive monitoring.
- **Hybrid visibility gaps**: separating IT and OT telemetry delays detection.

Solutions such as agentless monitoring modules (e.g., NETALERT integrated into lean SIEM architectures) provide continuous oversight of OT communications without disrupting machinery.

Under NIS2, boards are personally accountable for ensuring resilience across both IT and OT - forcing manufacturers to unify telemetry and deliver cross-domain incident reports regulators can trust.

6.4. GOVERNMENT & PUBLIC SECTOR - ACCOUNTABILITY AND STANDARDS

Governments hold the **most sensitive citizen data & face high-value threats** from nation-state adversaries and malicious insiders. Insider breaches average **USD 4.92M per event**, but the deeper cost is **erosion of public trust** in democratic institutions and services.

Challenges include:

- **Fragmented legacy systems**.
- **Procurement-heavy SOCs** & multiple tools for SIEM, SOAR, compliance and forensics.
- **Long dwell times and inconsistent regulator reporting**.

Frameworks such as **ISO 27001, NIS2 and national strategies** now require public agencies to p**rove not only containment but also compliance** - often within hours.

ATT&CK-mapped detections & prebuilt compliance templates are transformative, allowing ministries to present regulator-ready evidence that withstands **parliamentary or judicial scrutiny** without doubling analyst effort.

6.5. RETAIL & ECOMMERCE - FRAUD AND PCI DSS

Retail and eCommerce face a distinct mix of threats:

- **Payment card fraud** and **account takeover** dominate.
- **Breaches often involve customer PII** (53% of global cases), costing USD 160 per record.
- **Distributed carding operations**, where stolen cards are tested at scale, are particularly hard to detect without high-correlation analytics.

Compliance pressure here comes from **PCI DSS**, which demands strict controls over cardholder data. Non-compliance leads to fines, chargebacks, and reputational loss that can cripple online retailers.

Key enablers in this sector:

- **UEBA to spot anomalies** like a single account making purchases from multiple geographies in minutes.
- **PCI DSS dashboards** embedded into monitoring platforms to align detection with audit requirements.

Retailers are also heavily exposed to **supply chain compromise**, especially through point-of-sale software and third-party eCommerce plugins. **Without integrated monitoring, these attacks are often detected late** - after losses have accumulated.

6.6. ENERGY & UTILITIES - CRITICAL INFRASTRUCTURE RISKS

The energy and utilities sector faces a unique convergence of **critical infrastructure risk and regulatory accountability**. Breaches here are less about data loss and more about **operational disruption**.

Key pressures include:

- **Third-party/supply chain compromises**, averaging **USD 4.91M per incident**.
- **OT manipulation attempts**, such as interference with wind turbines or grid distribution systems, flagged by both ENISA and Red Canary.

Energy systems are globally distributed, making attackers prone to exploit the weakest regional link to pivot into wider networks.

Under NIS2, boards are directly accountable for resilience. Energy providers must prove both **rapid detection and operational recovery under regulatory oversight.**

Agentless monitoring and **sector-specific incident templates** enable utilities to meet both operational and compliance obligations.

Lean architectures that collapse IT and OT anomalies into unified narratives become especially valuable these days.

6.7 CROSS-SECTOR OBSERVATIONS

Despite different environments, **three themes repeat across industries:**

- **Compliance is operational.** Reporting cycles are short, fines are substantial, and audit readiness must be a daily output, not an ad-hoc exercise.

- **Agentless and hybrid monitoring are critical**. Healthcare manufacturing, and energy cannot rely on universal endpoint agents.

- **Lean architectures reduce burden**. Platforms that embed correlation, enrichment, automation and compliance reporting into one flow reduce duplicate effort and analyst fatigue.

Across the board, resilience is measured in millions of dollars lost, hundreds of dwell-time days saved and hours of compliance work avoided.

The organizations best placed to succeed are those that detect early, collapse duplicates and produce regulator-ready evidence without overloading their teams.

7. AUTOMATION & AI - FROM PROMISE TO PRACTICE

In 2025, automation and AI are no longer optional enhancements. They have become the **decisive levers that shape breach economics**, changing how SOCs detect, investigate and report incidents.
What once required armies of analysts is now achievable with leaner teams supported by machine-driven workflows. The evidence from across industries is clear: **automation is altering both the cost curve and the human experience of cyber defence.**

7.1. REAL-WORLD IMPACT METRICS

Surveys and operational benchmarks highlight the widening gap between manual-heavy SOCs and automation-led ones:

- **60% of SOC teams using AI** report **investigation times reduced by at least 25%**.
- **73%** have **fully automated alert triage & prioritization**, while **68% rely on automation for enrichment tasks** like threat intelligence lookups and asset correlation.
- Despite **82% of SOCs now running 24/7**, **69%** still compile metrics manually, and **62% struggle with analyst retention.**

The numbers underscore a structural shift. **Automation is not a "nice-to-have"** for efficiency - it is the only way to sustain SOC operations at scale while keeping staff engaged and effective.

69% of SOC teams

report investigation times

reduced by at least 25%

82% of SOCs

now running 24/7

69%

still compile metrics manually

62%

struggle with analyst retention

7.2. HOW AI RESHAPES DETECTION

AI and behavioral analytics are most impactful where human attention is most strained: **in separating noise from signal.**

- SOCs routinely process on **average 4,000+ alerts per day**, the majority of which are false positives.
- Deployments of **UEBA (User and Entity Behavior Analytics)** reduce noise sharply, with around **41% of irrelevant alerts dismissed automatically**.
- Organizations that embed UEBA report **mean time to respond (MTTR) improvements of 50-70%**, because analysts receive risk-ranked entities instead of atomized alerts.

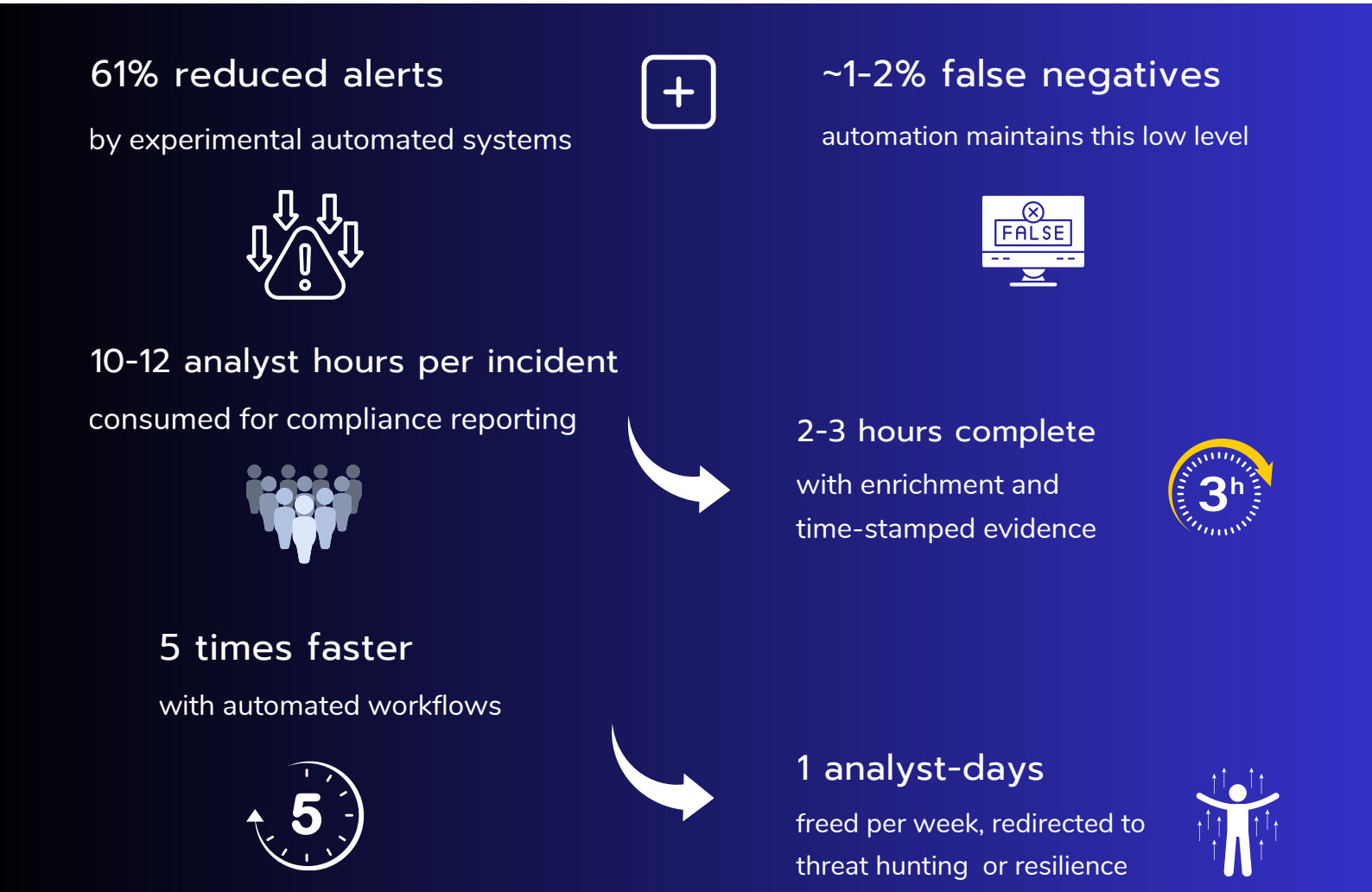
This shift matters because fatigue is as dangerous as any external adversary. AI reduces the cognitive load, **allowing human analysts to focus on the incidents that genuinely threaten the business.**

7.3. OPERATIONAL GAINS: TRIAGE TO REPORTING

The reach of automation has now extended beyond filtering alerts:

- Experimental systems have **reduced alerts** presented to humans **by 61%**, while **maintaining false negatives at just ~1-2%**.
- Compliance reporting that once consumed **10-12 analyst hours per incident** can now be **completed in 2-3 hours**, complete with enrichment and time-stamped evidence.
- Security reviews, such as vendor risk assessments and questionnaires, can be processed **up to 5 times faster with automated workflows**.

The effect is cumulative. Hours saved in triage, enrichment, and reporting translate into **whole analyst-days freed per week**, which can be redirected to threat hunting, red-teaming, or resilience planning.



7.4. ARCHITECTURE: AUTOMATION AS THE BACKBONE

The decisive change in 2025 is architectural. Automation has moved from the edges of the SOC to the center:

- Incidents that once generated **dozens of overlapping alerts** now appear as single enriched cases, complete with context, attack timelines and mapped MITRE ATT&CK techniques.
- Analysts investigate once and the **platform automatically generates both operational evidence and compliance-ready artefacts**.
- Cost analyses show that **embedding automation** directly into the pipeline allows SOCs to **avoid hiring additional headcount, saving USD 100K-150K annually in staffing**.

Automation has become the backbone of SOC design, ensuring that complexity is handled by the platform rather than by human repetition.

7.5. TOWARD PROACTIVE AND TRUSTED AI

The next horizon is proactivity. SOCs are beginning to:

- **Run continuous adversary simulations**, validating that pipelines detect pivots and lateral movement before attackers arrive.
- **Deploy dynamic detection logic**, where AI adapts rules in near real time as attacker behavior evolves.
- **Adopt human-AI teaming frameworks**, where analysts remain the decision-makers but rely on AI to build context, suggest next steps, and assemble evidence.

Trust is crucial. These models are not replacing human analysts but amplifying their reach, ensuring human judgment is applied where it matters most.

7.6. SUMMARY - AI & AUTOMATION

Automation and AI are now reshaping SOC performance along three fronts:

Cycle Time Compression - response and escalation times **shortened by 25-70%**, turning multi-day processes into hours.

Analyst Enablement - alert floods reduced, false positives nearly halved, compliance reports assembled in hours rather than days.

Architectural Evolution - automation is embedded into ingestion, correlation and reporting, ensuring every case doubles as **both a security artefact and a compliance artefact.**

The lesson of 2025 is straightforward: **automation doesn't just cut costs. It redefines resilience, enabling lean teams** to defend complex environments at a pace and scale that manual operations can no longer match.

8. COST, LICENSING AND SCALABILITY

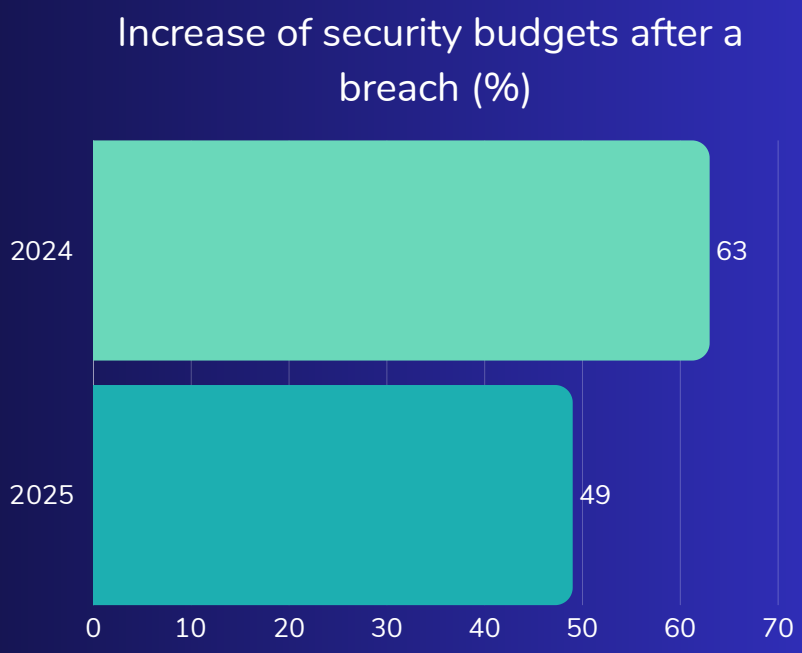
Beyond the immediate costs of breaches, there is a quieter but equally decisive factor: the **economics of running a security platform itself**. Even before a single alert is investigated, the choice of architecture, licensing model and infrastructure footprint can determine whether security remains sustainable - or whether it quietly drains budgets year after year.

8.1. THE HIDDEN WEIGHT OF LEGACY APPROACHES

Traditional SIEM and SOAR deployments often grow heavy over time.

- **Up to 30% of total SIEM** spend in large enterprises now goes to **auxiliary modules and marketplace add-ons** - correlation engines, UEBA, or compliance packs bolted on at premium cost.
- **Infrastructure adds another layer**. A single high-throughput environment may demand **hundreds of gigabytes of RAM and dozens of cores** simply to keep ingestion stable.
- **Over a three-year refresh cycle**, oversized infrastructure and module licensing can **consume six-figure sums** in hardware and energy costs alone.

This is the "second bill" of cybersecurity: **not the incident itself, but the platform needed to watch for it**.



8.2. LICENSING TRANSPARENCY

The market is now shifting toward transparent, all-in pricing models.

Instead of treating UEBA, MITRE ATT&CK mapping, or compliance templates as separate products, **newer platforms include them in the base license.**

This matters for two reasons:

- **In 2025, 49% of organizations increased security budgets after a breach**, down from **63% the year before**. Boards are asking harder questions about where the money goes.
- **Transparent licensing** ensures that every dollar spent translates into **capability on day one, not hidden costs six months later.**

The difference is more than accounting - it directly affects trust between CISOs, boards and vendors.

8.3. INFRASTRUCTURE EFFICIENCY

Resource efficiency is another silent differentiator.

• **Next-generation platforms can now operate full-scale SOC environments** on as little as **32 GB RAM and 8 CPU cores**, while still supporting horizontal scaling.
• Legacy deployments may **require 2-3x those resources** for similar throughput, driving both direct hardware spend and indirect energy costs.
• Across a medium enterprise, the difference can translate to **EUR 100K+ saved** per refresh cycle.

In an era of tight budgets, **efficiency** is not cosmetic. It is the **difference between maintaining resilience and being forced to trim coverage**.

8.4. LEAN ARCHITECTURES IN PRACTICE

This is where lean architectural philosophy becomes visible. Instead of layering modules, platforms like **CYBERQUEST (CQ) integrate ingestion, correlation, enrichment, automation and reporting into a single streamlined pipeline.**

• **NO COSTLY ADD-ONS**: UEBA, ATT&CK mapping and compliance-ready reporting are part of the core.

• **OPERATIONAL REACH**: **CQ extends visibility** into OT and ICS through **NETALERT**, without intrusive agents.

• **AUTOMATION EMBEDDED**: rather than scattered scripts, more than a thousand predefined actions cover integration with identity systems, EDRs, and collaboration tools.

• **COMPLIANCE BUILT-IN: outputs aligned with DORA and NIS2 are generated automatically** from the same cases analysts investigate daily.

The point is not to oversell one tool but to illustrate a pattern: **lean design reduces duplication and ensures resilience scales without spiralling cost.**

8.5. STRATEGIC PERSPECTIVE

Economics in cybersecurity are about more than licensing fees. They touch:

- **OPPORTUNITY COST - analysts spend 20-30% of their time** reconciling alerts across fragmented systems in legacy deployments.
- **STAFF TURNOVER** - inefficient platforms fuel burnout, raising the cost of retraining and backfilling talent.
- **BOARD CONFIDENCE** - predictable cost structures make it easier to defend security budgets.

A lean, transparent platform design turns each of these from liabilities into advantages. Analysts reclaim time, boards get clarity, and organisations save money that would otherwise be consumed in hidden overhead.

8.6. THE LESSON FOR 2025

The industry trend is unmistakable: away from fragmented module stacks and toward lightweight, horizontally scalable deployments.

The lesson for 2025 is that resilience is not only about catching threats - it is also about running the platform sustainably.

Architectures like CYBERQUEST demonstrate that scalability can be achieved with modest resources, transparent pricing and compliance capabilities already integrated.

For boards and SOC leaders alike, the takeaway is straightforward: the economics of your detection platform are as critical as its detection rules.

A platform that is lean, transparent and scalable ensures that **resilience is affordable, sustainable and defensible in front of both regulators and auditors**.

9. STRATEGIC TAKEAWAY: FROM COMPLEXITY TO RESILIENCE

The cybersecurity story of 2025 is dominated by two realities:

- breaches remain costly and disruptive
- compliance has become a board-level legal obligation.

What separates organizations that bend these curves from those that break under them is not how much they spend, but **how their security platform is built.**

9.1. THE UNSOLVED PROBLEMS

The direction of travel is clear: threats intensify, regulations harden and traditional heavyweight platforms are no longer enough.

Global average breach cost may stand at **USD 4.44M**, yet in markets like the US, it climbed to **USD 10.22M**.

Average breach lifecycles may have fallen to **241 days**, but attackers need only **hours to exfiltrate data or disable systems.**

SOCs still face **thousands of alerts daily, discarding up to 30%** simply to cope.

Healthcare faces **ransomware in 54% of incidents**, with life-critical services disrupted and **median costs of EUR 300,000**.

Compliance regimes like **DORA and NIS2 now enforce fines**, reputational penalties and even **board disqualifications for failures**.

9.2. WHAT WORKS IN PRACTICE

The data proves that three moves consistently shift outcomes:

Collapse lifecycles - cases resolved **under 200 days save over USD 1M** compared to slower incidents.

Elevate context - **integrating identity, SaaS and OT metadata** cuts through the noise of duplicate alerts.

Automate compliance - regulator-ready reports must be generated as a natural output of incident handling, not an afterthought.

These principles aren't theoretical. They are already visible in the organisations that report faster containment, lower costs, and fewer staff departures.

9.3. THE DECISIVE CHOICE

CISOs and boards are now facing a binary decision:

- **Continue layering complex, expensive and siloed tools**, hoping that integration projects will close the gaps.
- **Or adopt a lean, integrated platform like CYBERQUEST**, designed to cut cost, compress lifecycles and deliver regulator-ready evidence from day one.

The organisations that succeed in the next decade will be those that take the second path.

CYBERQUEST proves that resilience and compliance can scale together, without spiraling costs or analyst burnout.

9.4. WHY CYBERQUEST IS DIFFERENT

Among the platforms on the market, **CYBERQUEST (CQ)** has emerged as a model of how lean architecture changes the equation. CQ does not try to bolt on modules after the fact - it was **built from the ground up to integrate ingestion, correlation, automation and compliance into a single streamlined pipeline**.

Efficiency: Runs full-scale SOC deployments on as little as **32 GB RAM and 8 CPU cores**, avoiding the infrastructure sprawl of legacy SIEMs.

Breadth: 270+ native connectors bring IT, cloud and OT telemetry into one console without costly custom parsers.

Industrial visibility: With **NETALERT, CYBERQUEST** extends coverage into ICS and OT environments without disruptive agents.

Automation: A library of predefined actions and workflows removes repetitive tasks, cutting escalation time from hours to minutes.

Compliance by design: CQ outputs **DORA and NIS2 aligned reports automatically**, turning every case into both an investigative and regulatory artefact.

The result is not an incremental efficiency.
CYBERQUEST is a platform that **redefines what resilience looks like in practice.**

9.5 CONCLUSION

The lesson from 2025 is that complexity is the real enemy. Attackers exploit it. Regulators punish it. Analysts burn out under it.

CYBERQUEST shows how to **replace that complexity with clarity, speed and defensible resilience.**

It is not simply another tool in the SOC stack - it is an architectural reset, one that **turns detection into trust, investigation into evidence and compliance into an outcome achieved automatically**.

For boards, regulators, and SOC leaders, the message is simple: If resilience is the goal, **CYBERQUEST is the platform that delivers it.**

10. REFERENCES

This report draws on a combination of industry benchmarks, regulatory texts and independent research published in 2024-2025. Key sources include:

- IBM Security - Cost of a Data Breach Report 2025 (global and regional breach cost benchmarks, lifecycle durations, cost by vector).
- ENISA (European Union Agency for Cybersecurity) - Threat Landscape for the Health Sector 2021-2023 (ransomware prevalence, data theft in healthcare, sector-specific incident costs).
- Red Canary - Threat Detection Report 2025 (telemetry volumes, confirmed threats, rise of identity-centric techniques, VPN abuse trends).
- European Commission / EU Publications Office - texts of the Digital Operational Resilience Act (DORA) and NIS2 Directive, with national implementations including Romania's Law 124/2025.
- Cloud Security Alliance - Top Security Functions to Automate in 2025 (automation use cases and quantified efficiency improvements).
- Swimlane - Global SOC Survey 2025 (24/7 SOC operation rates, manual reporting burdens, staff retention challenges).
- Gurucul - Pulse of AI-Powered SOC Report 2025 (AI adoption levels, automation in triage, enrichment practices).
- Cybersecurity Insiders - SOC Transformation Survey 2025 (investigation time reductions, automation adoption statistics).
- Torq Security - SOC Automation Benchmarks 2025 (MTTR reduction percentages, cost avoidance through automation).
- Radiant Security - SOC Use Case Benchmarks (alert volumes per day, false positive ratios).
- Splunk - UEBA impact reports (false positive reduction and simplification of investigations).
- Academic Research
  - AACT: AI-Augmented Cybersecurity Triage (2025, arXiv preprint 2505.09843) - reduction of analyst alert loads by 61%, low false negative rates.
  - Trusted Human-AI Collaboration in SOCs (2025, arXiv preprints 2505.23397 and 2508.18947) - frameworks for AI autonomy calibration and LLM-assisted analyst workflows.

nextgen

CYBERQUEST

NETALERT

Questions? Contact us.

www.nextgensoftware.eu
office@nextgensoftware.eu
marketing@nextgensoftware.eu