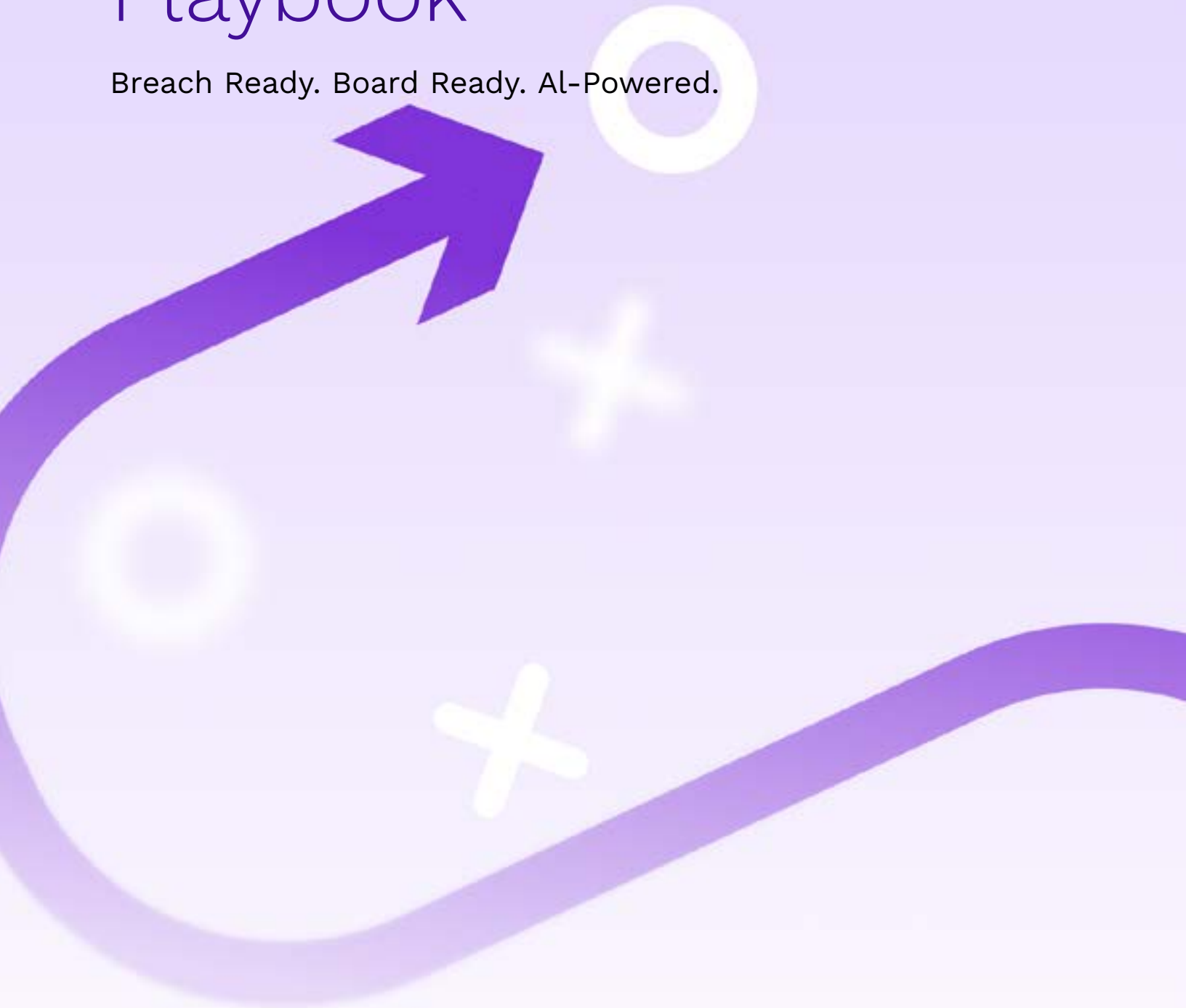
SOC Modernization Playbook

Breach Ready. Board Ready. AI-Powered.



securonix

> Boards no longer ask, 'Are we secure?' They ask, 'Are we secure, efficient, and enabling the business to grow?' CISOs must deliver measurable outcomes that reduce risk, demonstrate ROI, and build enterprise resilience.
>
> - Board Mandate for the Modern SOC

Executive Summary

securonix

Breach Ready. Board Ready. AI-Powered.

Boards now expect CISOs to act as **strategic partners**—leaders who can protect the enterprise and prove measurable ROI. Security leaders face a dual mandate: defend against relentless, AI-powered threats while delivering outcomes the business and board can trust. Legacy SOCs—manual, reactive, and fragmented—are failing both missions.

Modernizing your cybersecurity tech stack isn't about adding more tools. It's about delivering outcomes that matter like faster detection and response, a lower cost to operate, analyst productivity that scales, and compliance confidence with audit-ready visibility.

That’s why SOC modernization must unify AI-driven detection, automation, and compliance reporting into a system that produces outcomes—not overhead.

Securonix is purpose-built to deliver that mission. With a unified, cloud-native TDIR platform, modular Agentic AI, and outcome-based pricing, we help CISOs turn board pressure into business advantage.

The modern SOC is no longer optional. It’s the only way to be breach ready, board ready.

securonix

Why Modernize Now

60%
SOC analysts with alert fatigue

72%
budgets rise only with impact

73%
boards demand ROI updates

Boards are asking CISOs and CIOs how AI will reduce manual workloads, accelerate processes, and enhance decision-making accuracy.

- Deloitte, Future of Cybersecurity 2024

Business risk is accelerating

Adversaries are moving at unprecedented speed, leveraging LLM-powered phishing, identity-based attacks, and supply chain vulnerabilities. With identity misuse now playing a role in 90% of breaches—far outpacing traditional malware—human-only triage can no longer keep up.

Talent is burning out

Over 60% of SOC analysts cite alert fatigue as their top challenge. Too many tools and too much noise are driving attrition and draining effectiveness.

Costs are unsustainable

Ingestion taxes and tool sprawl keep pushing TCO higher without improving detection. The old model isn't scaling. And boards know it.

Boards demand accountability

73% of boards now require ROI reporting, while 72% tie budget approvals to measurable outcomes.

Continuous compliance pressure from global regulations like **SEC, GDPR,** and **DORA** demand proactive reporting, faster breach disclosure, and visibility into third-party risk. Boards expect assurance that the company can detect, contain, and recover from incidents—proving not just security, but **operational rigor and cost discipline.**

The Board-Level Mandate

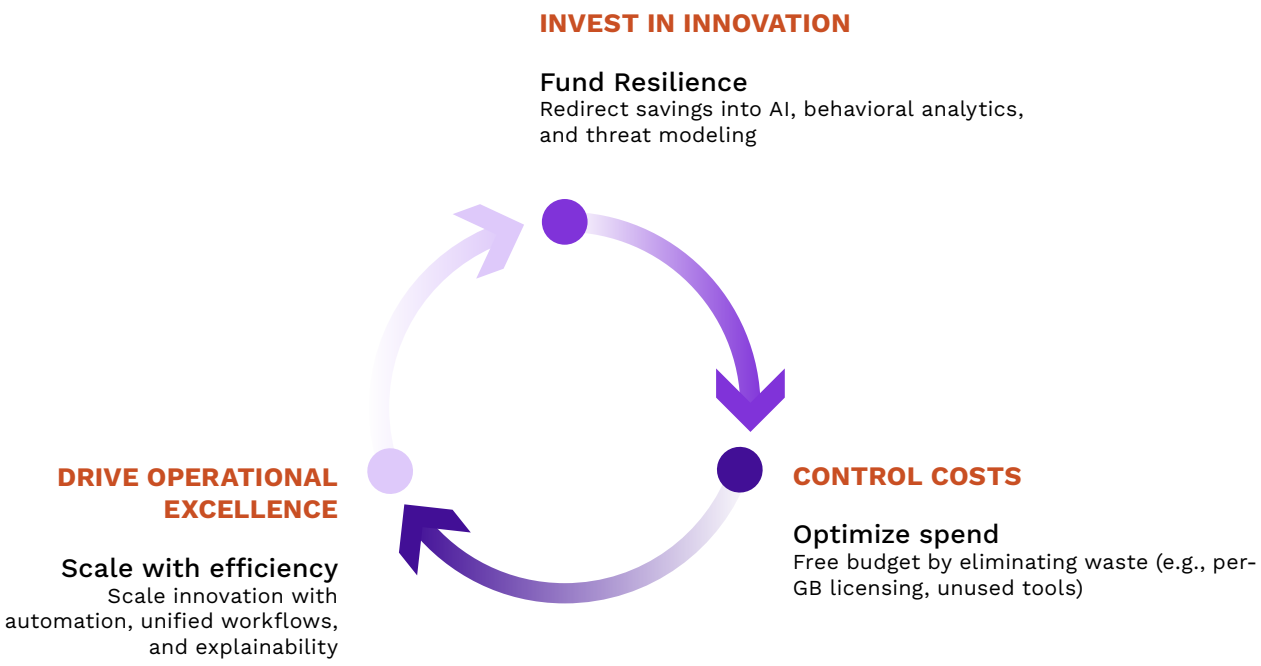
Boards no longer ask, “Are we secure?” They now expect SOC teams to drive efficiency and enable business growth. Meeting that expectation requires unifying three mandates into a single system:

- **Control Costs →** Eliminate waste, and free up budget.
- **Invest in Innovation →** Redirect savings to advanced analytics, AI, and threat modeling.
- **Drive Operational Excellence →** Scale securely with automation and integrated workflows.

When treated as a connected system, these mandates fuel one another: optimize spend → fund resilience → scale with efficiency.

The System-Level Play: Do All Three, Together

When you treat cost, innovation, and operations as siloed initiatives, progress stalls. But when treated as an interconnected system, one fuels the next: This is the flywheel of the modern SOC: Optimize spend → fund resilience → scale with efficiency.



The Securonix Approach

Securonix enables this system-level modernization with a unified, cloud-native TDIR platform that delivers:

- Agentic AI to triage, enrich, and respond in real time
- Outcome-based licensing that breaks the cost-volume trap
- Data Pipeline Manager for intelligent telemetry routing
- Unified SIEM, SOAR, UEBA, and TIP to eliminate tool fragmentation

This is how CISOs turn pressure into progress and security into strategic advantage.

This isn't about upgrading your tools.

It's about transforming security with AI to eliminate noise and safeguard the business.

Securonix modernizes the SOC by unifying threat detection, investigation, and response with AI-driven automation, curated threat intelligence, and a modular architecture built for scale..

CISO Outcomes: What “Modern” Should Deliver

This Isn’t About Tools. It’s About Transformation.

The mandate to modernize your SOC isn’t a shopping list. It’s a scoreboard. Boards and business stakeholders care less about which platform you’ve bought and more about **what it’s doing for the business**.

The modern SOC must deliver tangible, measurable outcomes across detection, response, resilience, and efficiency. Below are the **10 north-star outcomes** every CISO should expect from a truly modernized SOC strategy.

Top 10 Outcomes of a Modern SOC

securonix

1 Reduced MTTD and MTTR

AI-driven enrichment and unified workflows cut detection and response times by **60-70%**.

2 3x Analyst Productivity

Automated triage and enrichment free analysts for higher-value work. **2-3 hours saved per analyst, per day.**

3 Hybrid Visibility

Unified telemetry across cloud, SaaS, endpoint, and identity sources eliminates blind spots and accelerates investigations.

4 Operationalized AI

Explainable, policy-controlled AI agents embedded in workflows drive trust and adoption.

5 End-to-End Detection to Response

One pipeline combining SIEM + UEBA + SOAR + TIP) replaces swivel-chair operations for faster, cleaner resolutions.

6 Outcome-Based Cost Optimization

Smart ingestion, tiering, and outcome-aligned pricing deliver **30-50% TCO savings.**

7 Behavioral Threat Detection

Identity and peer analytics cut noise and expose anomalies. **Up to 90% fewer false positives.**

8 Compliance-Ready Forensics

Federated search across hot and cold tiers ensures **audit-ready visibility**-without storage bloat.

9 Cloud-Native Zero-Ops Scale

Elastic, SaaS delivery eliminates infrastructure overhead and enables on-demand scaling.

10 Continuous Innovation

Modular AI agents and detection packs evolve with threats delivering ongoing improvements without costly re-platforming.

What This Means for CISOs

CISOs are no longer just defenders. They're transformation leaders.

To deliver on board mandates, modernize your SOC to *produce outcomes,* not just *operate technology.*

Because when you measure what matters, you build what lasts.

SOC Maturity Model: Where Are You Today?

Modernization Is a Journey. Know Your Starting Point.

CISOs often ask, *"How modern is our SOC, really?"*
This self-assessment model helps answer that question by mapping your current state against the key outcomes your SOC should deliver.

It's not just about what tools you've deployed.
It's about the **value your SOC produces**, day in and day

How to Assess Your Current State

securonix

Modernizing the SOC starts with an honest look at where you are today. The right tools alone don't guarantee progress, outcomes do. To gauge where your SOC is delivering measurable value, begin by asking yourself:

- Are my analysts spending more time on triage than on true threat hunting?
- Do I have clear visibility into MTTR across both cloud and on-prem assets?
- Can I demonstrate how AI is improving SOC productivity right now?
- Are we investing more in storing logs, or in enriching and acting on them?
- Does innovation often require re-platforming or lengthy vendor negotiations?

If your answers point to friction, fragmentation, or lack of measurable outcomes, you may be stuck between stages or missing a system-wide modernization effort.

Risks of Stagnation

Failing to modernize your SOC carries real consequences. Instead of driving resilience and efficiency, the SOC becomes a source of risk, rising costs, and board-level scrutiny.

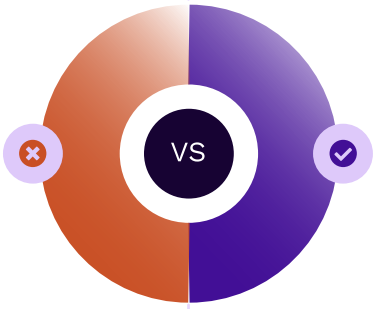
- **Technical debt:** Point solutions without orchestration create workflow gaps and rising costs.
- **Human fatigue:** Burnout accelerates when detection is noisy, and tooling is disconnected.
- **Executive scrutiny:** Boards want outcome metrics, not justification.

The Risk of Staying Still

Legacy / Alert-Driven SOCs drain resources and frustrate analysts.

Outcomes:

- Alert fatigue & analyst burnout
- High TCO with limited ROI
- Poor visibility & rising breach risk



The Reward of Moving Forward

Behavior-Based / Agentic AI SOCs create resilience and efficiency.

Outcomes:

- Unified detections & fewer false positives
- 3x analyst productivity with AI augmentation
- Measurable ROI, continuous innovation, and board confidence

securonix

SOC Maturity Model

This Is Your North Star

Modernization is about **system-level maturity** that unlocks:

- Better threat outcomes
- Lower operational drag
- Cost-optimized innovation

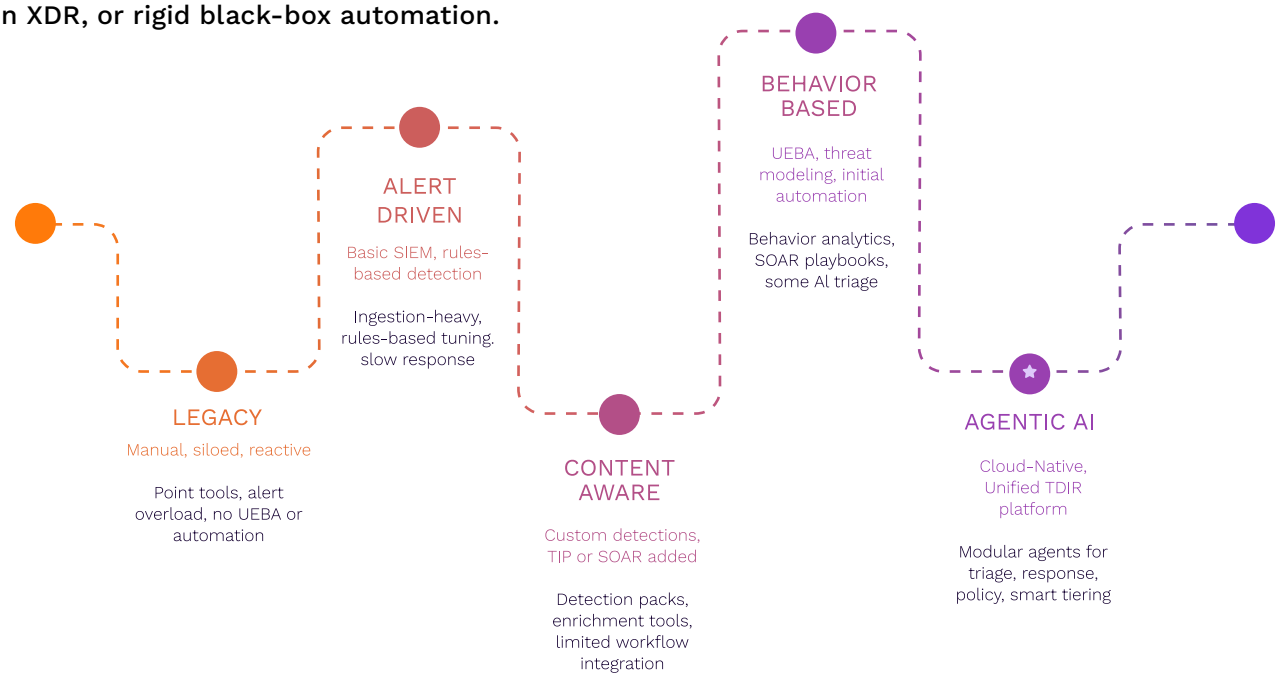
Where are you today? And what outcomes are you leaving on the table?

- Moving from **Content Aware** to **Behavior-Based** unlocks unified detections, fewer false positives, and sharper incident fidelity.
- Moving from **Behavior-Based** to **Agentic AI** delivers 3x analyst productivity, continuous AI-driven innovation, and a cost-aligned telemetry strategy.
- With **Agentic AI**, your SOC achieves measurable ROI, strategic agility, and sustained operational excellence.

Your North Star: The SOC Maturity Model

Modernization is about achieving system-level maturity that unlocks better threat outcomes, lower operational drag, and cost-optimized innovation. The question is: where are you today and what outcomes are you leaving on the table?

The Securonix Unified Defense SIEM platform is purpose-built to power this journey, enabling modern threat detection, investigation, and response without the limitations of legacy SIEMs, bolt-on XDR, or rigid black-box automation.



securonix

SecOps Efficiency

Achieving efficiency in the SOC means working smarter, not harder. Securonix improves operations by cutting through alert noise, automating repetitive tasks, and surfacing the insights that matter most. Analysts spend less time on triage and more time on proactive threat hunting, improving both speed and precision. And with optimized workflows resulting in lower overhead, the SOC responds faster, scales seamlessly, and supports business growth without adding complexity or headcount.

70-90%

False Positive Reduction

False positives are the leading cause analyst burnout. Reducing noise increases focus on real threats.

- AI-powered triage and suppression agents in action
- Shift from static rule-based alerts to behavior-driven detections
- More analyst time spent on response, not review

2-4x improvement

High Fidelity Detections

Increasing precision improves threat coverage and decision confidence.

- AI-powered triage and suppression agents in action
- Shift from static rule-based alerts to behavior-driven detections
- More analyst time spent on response, not review

60-70% reduction

MTTR & MTTD

These are core metrics for board reporting, cyber insurance, and operational performance.

- Agentic AI handling triage, classification, and escalation
- Unified workflows that replace swivel-chair investigations
- Enrichment pipelines cut time-to-context

2-3x increase

Analyst Efficiency

Analyst fatigue is growing and hiring can't keep pace. Now more than ever, efficiency is critical.

- Repetitive tasks moved to AI agents
- Investigations run in a single, enriched timeline
- Detection logic continuously improved via natural language

100% visibility into business-critical services

Cloud & SaaS Telemetry

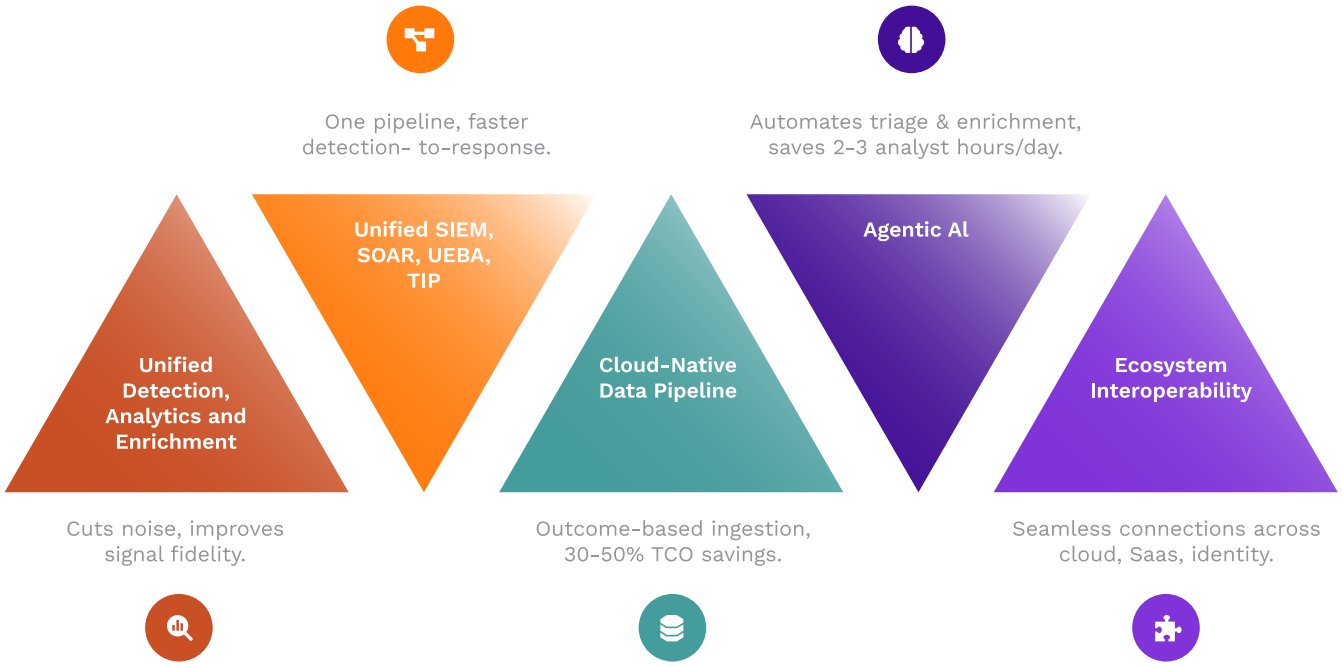
Threat actors thrive in blind spots-especially in your laas and Saas environments.

- % of business-critical cloud assets monitored (AWS, Azure, GCP
- % of Saas behavior analytics (M365, SFDC, GitHub, Okta)
- Gaps between telemetry ingested and actual threat detection value

Architecture Blueprint: The Future SOC Stack

securonix

A Modern SOC Needs a Modern Foundation



CISOs increasingly understand why SOC modernization is critical—regulatory pressure, rising costs, and AI-powered threats have made that clear. The real challenge now is the how: designing and building a SOC that's not just future-ready, but also resilient, efficient, and focused on measurable outcomes. What does a modern SOC look like beneath the surface, and which architectural decisions set high-performing organizations apart from the rest?

Modernizing your SOC requires more than stitching together point solutions. It demands a strategic blueprint for long-term success. This architectural model offers a clear framework for the capabilities, integrations, and design principles needed to achieve:

- Accelerated detection and response
- Effective AI operationalization
- Cost-efficient scalability
- Streamlined analyst experiences

This isn't a rip-and-replace strategy. It's a modular reference model designed to integrate with your current investments while minimizing complexity, eliminating redundancy, and bringing cohesion to previously fragmented tools.

Core Layers of the Future SOC Stack

The future SOC is built on a modular, intelligence-driven architecture designed to adapt, scale, and respond in real time. At its core are foundational technology layers that enable seamless integration, AI operationalization, and unified analyst experiences. These layers work together to deliver a resilient, high-performing SOC aligned with modern threat landscapes and business outcomes.

Unified Detection, Analytics and Enrichment Core

At the heart of the modern SOC is a real-time engine that ingests telemetry, correlates signals, enriches context, and scores risk.

Must-haves:

- Cross-domain telemetry ingestion (cloud, endpoint, identity, network, SaaS)
- Real-time behavioral analytics and threat modeling
- Built-in enrichment with identity, asset, threat intel, peer group context
- Risk-based alerting with dynamic scoring

Why it matters: Analysts need actionable insights—not raw data. Contextual correlation and risk scoring cut through the noise, improve signal fidelity, and drive faster, more informed investigations.

Unified SIEM + UEBA + SOAR + TIP

Instead of stitching together disconnected tools, the modern SOC converges these once-siloed functions into a single, integrated operational layer.

Must-haves:

- Native or tightly integrated modules for SIEM, UEBA, SOAR, and TIP
- Unified data layer and shared risk engine powering all functions
- Seamless orchestration of detections, playbooks, and threat intelligence
- Policy-based automation that operated within analyst-defined guardrails

Why it matters: Detection, investigation, and response should operate as a single continuous flow. Integration isn't just a feature—it's the foundation of modern SOC architecture.

Open, Cloud-Native Ingestion and Data Pipeline Strategy

In modern detection, data is fuel. But not all data is equal. A flexible, cloud-native pipeline is critical for balancing visibility, cost and performance.

Must-haves:

- Ingest from any telemetry source (e.g., Microsoft Sentinel, CrowdStrike, Zscaler, Okta, Palo Alto)
- Bring-your-own-cloud (AWS, Snowflake) for cost efficiency and data sovereignty
- Intelligent routing and tiering (hot/warm/cold) based on detection relevance
- Real-time stream filtering and enrichment at the point of ingest

Why it matters: A modern SOC doesn't just collect more —it collects smarter. Data should be prioritized, enriched, and stored based on value, not volume.

Agentic AI Layer for Triage, Detection, and Response

While traditional SOC tools offer automation in theory, modern SOCs operationalize it through modular, explainable AI agents that act with precision and context.

Must-haves:

- Specialized agents for triage, threat hunting, IOC correlation, response, and detection engineering
- Natural language input for rule creation and detection tuning (via policy agents)
- Risk-based prioritization and automated enrichment to streamline investigations
- Human-in-the-loop controls to ensure transparency, auditability and oversight

Why it matters: AI must be trusted, explainable, and directly actionable. Modular agents boost analyst efficiency while maintaining control, context and confidence.

Interoperability and Ecosystem Alignment

The modern SOC doesn't operate in a vacuum —it must seamlessly connect with the broader security and IT ecosystem to maximize speed, consistency, and reuse.

Must-haves:

- Native integrations with EDR (e.g., CrowdStrike), firewalls (e.g., Palo Alto), CASB/SWG (e.g., Zscaler), IAM (e.g., Okta), and cloud-native SIEMs (e.g., Microsoft Sentinel)
- Support for open standards (STIX, TAXII, Sigma, JSON)
- Extensible APIs for data ingestion, enrichment, and automated response workflows
- Ecosystem or marketplace support for rapid deployment of integrations and content

Why it matters: A future-ready SOC is built for interoperability. Tight integration across tools and platforms enables faster response, shared context, and scalable security operations.

securonix

Reference Model Summary

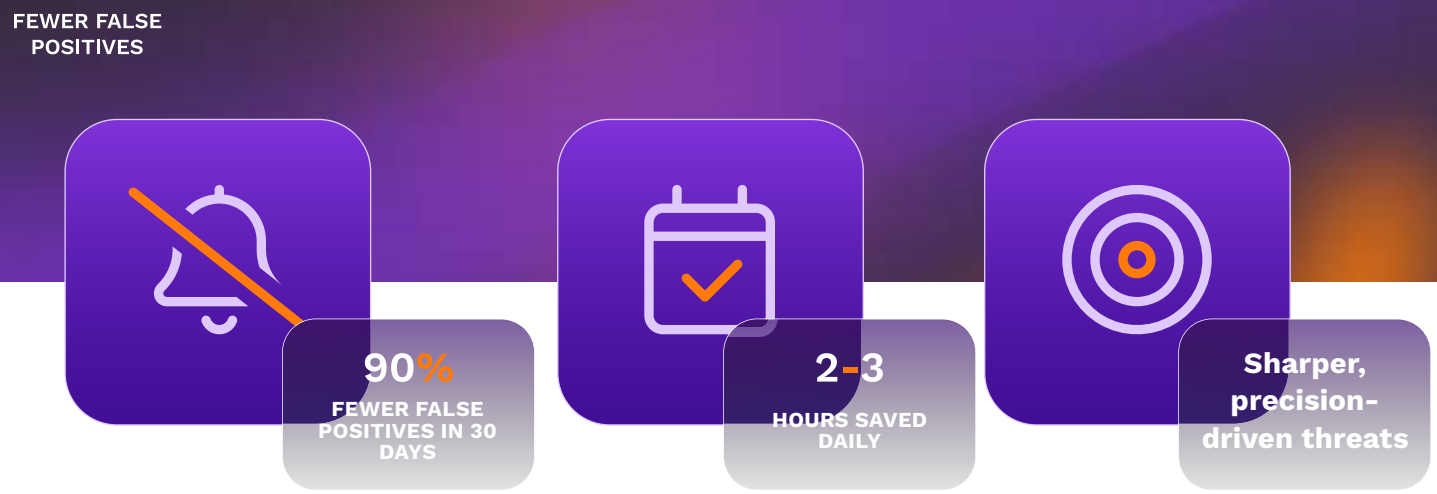
LAYER	CAPABILITY	VALUE
Detection Core	Analytics + Enrichment	High-fidelity alerts, less noise
TDIR Stack	SIEM + UEBA + SOAR + TIP	Unified response loop
Data Pipeline	Ingest + Tiering	Cost control, signal quality
Agentic AI	Triage + Policy + Response Agents	Analyst productivity, faster MTTR
Ecosystem Interop	API + Integrations	Protects existing investments

Built for Now. Ready for What's Next.

This isn't a conceptual model, it's a **practical roadmap** for CISOs to design a SOC that's:

- Agile enough to handle today's fast-moving threats
- Scalable enough to manage tomorrow's data demands
- Efficient and measurable enough to gain and maintain board confidence
- Because modern security isn't just about what's in your stack, it's about how your stack adapts, responds, and delivers outcomes at scale.

90-Day Modernization Plan: From Vison to Value



SOC Transformation Shouldn't Take a Year—It Should Deliver in a Quarter

CISOs don't have the luxury of drawn-out security overhauls. A modern SOC must show value fast, scale without disruption, and generate measurable ROI from day one.

This 90-day roadmap **accelerates outcomes** by layering high-fidelity analytics and automation **on top of your existing infrastructure**. Designed for low-friction deployment, it meets you where you are—then elevates detection, triage, and response through three phased, outcome-driven stages.

Phase 1 Days 1 - 30	Phase 2 Days 31 - 60	Phase 3 Days 61 - 90
		
## Unified Detection, Analytics and Enrichment	## Correlation, Context and Identity	## AI-Augmented Response
Modernization starts with measurable outcomes, not heavy integrations. The first 30 days focus on rapidly enhancing threat detection accuracy through curated detection content, agentic triage, and cost-optimized telemetry strategies.	With detections in place and alert noise under control, the next phase focuses on enriching investigations by linking user identity, behaviors, and threat intelligence for faster, more accurate insights.	The final phase turns your SOC into a force multiplier, by using modular AI agents to automate triage, orchestrate response, and accelerate detection engineering with precision and scale.
• Deploy the analytics and enrichment layer in your cloud environment (e.g., Snowflake, AWS) • Connect to existing telemetry sources—no rip-and-replace required • Implement curated detection packs targeting high-risk threat vectors • Activate triage agents and false positive suppression to cut noise early • Route telemetry through an intelligent data pipeline with automated tiering • This approach overlays your current SIEM, extending its capabilities with advanced behavioral analytics, curated threat intelligence, and identity-based correlation—without disrupting existing workflows	• Activate behavioral correlation and dynamic risk scoring • Integrate internal and external threat intelligence into detection logic • Add identity context through peer group analytics and account activity profiling • Set unfederated search across hot, warm, and cold data tiers • Launch contextualized investigations within a unified investigation console	• Deploy response automation agents for policy-based, SOAR-driven containment • Use natural language policy agents to convert analyst intent into detection rules • Automate IOC correlation, enrichment, and escalation workflows • Implement GenAI-powered simulation to validate detection logic and coverage • Launch outcome-focused dashboards showing alert reduction, hours saved, and TCO gains
In 30 days: sharper detections, fewer alerts, faster triage.	Deeper visibility, enriched context, and precision driven threat detection-all while significantly reducing investigation time.	AnAI-augmented SOC that speeds containment, scales analysts and proves value, with measurable impact.

Fast-Start Wins (Days 1—30)

Modernization starts with measurable outcomes, not heavy integrations. The first 30 days focus on rapidly enhancing threat detection accuracy through curated detection content, agentic triage, and cost-optimized telemetry strategies.

Deliverables:

- **Deploy the analytics and enrichment layer in your cloud environment (e.g., Snowflake, AWS)**
- **Connect to existing telemetry sources—*no rip-and-replace required***
- **Implement curated detection packs targeting high-risk threat vectors**
- **Activate triage agents and false positive suppression to cut noise early**
- **Route telemetry through an intelligent data pipeline with automated tiering**
- **This approach overlays your current SIEM, extending its capabilities with advanced behavioral analytics, curated threat intelligence, and identity-based correlation—without disrupting existing workflows**

Outcome: In 30-days or less: higher-fidelity detections, reduced alert volume, and accelerated triage across your existing SOC infrastructure.

Phase 1 (Days 1—30): Detection and Enrichment Foundation

FOCUS AREA	WHAT'S DEPLOYED	WHY IT MATTERS
Cloud-Native Core	Analytics + Enrichment Layer	Rapid value delivery with zero infrastructure overhead
Curated Content Packs	500+ behavior-based detections	Minimizes manual tuning and reduces false positives
Smart Ingestion	Tiered routing + stream filtering	Lowers ingestion andstorage costs while preserving detection quality
Agentic Triage	Autonomous triage + noise suppression agents	Automatically highlights high fidelity, actionable threats

Phase 2 (Days 31—60): Correlation, Context, and Identity

With detections in place and alert noise under control, the next phase focuses on enriching investigations by linking **user identity, behaviors, and threat intelligence** for faster, more accurate insights.

Deliverables:

- Activate behavioral correlation and dynamic risk scoring
- Integrate internal and external threat intelligence into detection logic
- Add identity context through peer group analytics and account activity profiling
- Set unfederated search across hot, warm, and cold data tiers
- Launch contextualized investigations within a unified investigation console

Outcome: Deeper visibility, enriched context, and precision-driven threat detection—all while significantly reducing investigation time.

Phase 3 (Days 61—90): Automation and AI-Augmented Response

The final phase turns your SOC into a **force multiplier,** by using modular AI agents to automate triage, orchestrate response, and accelerate detection engineering with precision and scale.

Deliverables:

- Deploy response automation agents for policy-based, SOAR-driven containment
- Use natural language policy agents to convert analyst intent into detection rules
- Automate IOC correlation, enrichment, and escalation workflows
- Implement GenAI-powered simulation to validate detection logic and coverage
- Launch outcome-focused dashboards showing alert reduction, hours saved, and TCO gains

Outcome: A self-optimizing, AI-augmented SOC that enables faster containment, scales analyst output, and proves its value through measurable operational impact.

90-Day Milestones

METRIC	EXPECTED IMPROVEMENT
MTTD/MTTR	60—70% faster
Analyst Time Saved	2—3 hours per analyst/day
False Positives	Up to 90% reduction
Ingest/Storage Costs	30—50% reduction
Detection Coverage	500+ high-fidelity use cases

What Makes This Plan Work

Adopting a 90-day plan to transform your SOC works because it's built around your needs, not someone else's roadmap. You keep the tools you already use, avoid new infrastructure headaches, and start proving value right away with curated detections and AI-powered workflows. As you grow, the approach grows with you eventually expanding into full detection, triage, and response at your pace. Its modernization made simple: faster, smarter, and delivering outcomes from day one.

- **Non-Disruptive**: Enhances existing tools—no rip-and-replace required
- **Cloud-Native**: Runs in your environment with zero infrastructure overhead
- **Outcome-Driven**: Delivers rapid ROI with curated detections and AI-powered workflows
- **Scalable**: Grows into full-spectrum detection, triage, and response at your pace

This is modernization on your terms. **Faster, smarter, and aligned to value from day one.**

Sample Use Cases: Before and After SOC Modernization

From Noise to Precision. From Tool Sprawl to Unified Defense.

It's one thing to talk about the benefits of a modern SOC. It's another to see those benefits in action. The following use cases show how legacy detection methods compare to outcomes achieved with a unified, AI-augmented architecture.

Each before-and-after scenario is rooted in real-world operational challenges and shows how enriched telemetry, agentic automation, and integrated TDIR pipeline translate into faster response, reduced noise, and smarter resource utilization.

Insider Threat Detection

BEFORE	AFTER
Static rule-based alerts on file access or large data transfers	Behavioral baselines detect deviations from peer group norms
No context on user role, tenure, or device activity	Enriched with identity, asset, location, and risk scoring
High false positives from legitimate admin activity	Noise reduction agents filter normal behavior; focus on true anomalies
Disconnected tools for access logs, HR data, and SIEM analysis	Unified view combining SIEM + UEBA + identity analytics

Result: **Insider threats are identified up to 10x faster—with fewer false positives and greater context for investigation.**

Credential Misuse (Account Compromise)

BEFORE	AFTER
Detection based on basic rules like login failures or geolocation mismatch	Identity enrichment connects failed and successful logins across all assets and applications
No detection slow, stealthy compromise patterns	Peer group analysis and frequency modeling detect subtle behavioral shifts
Response dependent on manual triage and escalation	Agentic AI scores risk in real-time and triggers automated response based on policy thresholds
Logs siloed across active directory, VPN, and endpoint systems	Correlated identity telemetry within unified platform, queryable via federated search

Result: Credential misuse is identified and contained in minutes, stopping lateral movement before it starts.

Lateral Movement

BEFORE	AFTER
High alert fatigue from port scans and off-hours logins	Chain-of-activity analytics detect suspicious patterns across multiple assets
Manual correlation required across EDR, firewall, and Active Directory	Unified timeline links behaviors across telemetry layers in a single view
No historical context for recurring suspicious entities	Dynamic risk scoring escalates based on cumulative behavior over time
Response only initiated after multiple alerts stack up	Agentic response agent auto-isolates user or triggers MFA based on risk confidence

Result: Accurate detection of lateral movement across cloud and on-prem environments—reducing MTTR by 60—70% and enabling proactive containment.

SaaS Abuse / Data Exfiltration

BEFORE	AFTER
Visibility limited to basic firewall logs; minimal insight into SaaS activity	Direct cloud API integrations with identity context expose risky behavior in apps like Box, GITHub and Google Drive
No way to differentiate between normal sync and malicious exfiltration	Peer group analytics detect abnormal data transfer volumes and usage patterns
Alerts triggered only after large data transfer thresholds are exceeded	Behavior analytics proactively flag unusual SaaS actively (e.g., off-hours access or atypical file sharing)
No automated response to prevent ongoing exfiltration	Agentic response agent can revoke OAuth tokens, trigger DLP actions, or isolate the user session automatically

Result: **Sensitive SaaS abuse is detected and contained proactively— before data is exfiltrated, without disrupting normal business operations.**

Threat Hunting with Enriched Telemetry

BEFORE	AFTER
Threat hunting limited by siloed date in hot storage	Federated search spans both live (Snowflake) and archive (S3) data tiers seamlessly
Requires complex SQL queries and custom scripts	Natural language-driven hunting with inline enrichment simplifies the process
Threat intel feeds must be manually parsed and integrated	Built-in TIP layer seamlessly embeds threat intelligence into hunt queries and detection logic
Rehydrating historical data for investigation is costly and time-consuming	Full-text search across hot and cold storage with no performance or cost penalties

Result: **Threat hunters gain speed, depth, and precision—unlocking advanced detections and faster investigations without the burden of manual overhead or expensive data retrieval.**

Threat Intelligence Fusion

BEFORE	AFTER
Threat intel is siloed across third-party TIPs, spreadsheets, and unstructured feeds	Internal observables and external intel are unified into a **single pipeline** with shared enrichment across detection, investigation, and response
Analysts manually copy/paste IOCs into queries	Indicators and TTPs are automatically mapped to detection logic with explainable AI and behavioral correlation
Intel remains static limited to reports or dashboards	Threat intel fuels curated detections, real-time enrichment, and automated response playbooks
TIP, SIEM, and SOAR operate as separate tools	Threat intel and behavioral analytics run natively **within one platform** closing the integration gap

Result: Threat intelligence becomes fully **operationalized**; detecting, enriching, and triggering responses in real time, without manual overhead or fragmented workflows.

What This Means for CISOs

Every "after" scenario shows the real impact of SOC modernization: precision instead of noise, context instead of chaos, speed instead of sprawl, and outcomes instead of overhead. When detection, enrichment, and response work as one, the SOC stops being a cost center and becomes a true strategic asset driving measurable value for the business. Every "after" scenario demonstrates the true impact of SOC modernization:

- **Precision replaces noise**
- **Context replaces chaos**
- **Speed replaces sprawl**
- **Outcomes replace overhead**

When detection, enrichment, and response are fully integrated, **the SOC doesn't just improve—it becomes a strategic asset that drives measurable business value.**

securonix

Metrics That Matter: The CISO Scorecard for SOC Modernization

Modernization Without Measurement Is Just a Rebrand

Today's CISOs are expected to go beyond detecting threats—they must demonstrate measurable progress. Boards want performance. Finance wants predictability. The business demands resilience. That requires more than dashboards and alerts; it calls for a **clear, outcome-driven scorecard** that shows how SOC modernization reduces risk, improves efficiency, and delivers ROI.

Below are five essential KPIs every modern SOC should track—mapped directly to modernization levers like agentic AI, behavioral analytics, smart ingestion, and unified detection-to-response workflows.

90%

Noise Cut (False positive reduction target 70—90%)

4X

Better Detections (High-fidelity detection lift)

1. False Positive Reduction

TARGET: 70—90%

Why it matters: False positives are the leading cause of alert fatigue and analyst burnout. Reducing noise increases focus on real threats.

Signals of success:

- AI-powered triage and suppression agents in action
- Shift from static rule-based alerts to behavior-driven detections
- More analyst time spent on response, not review

2. Increase in High-Fidelity Detections

TARGET: 2—4X IMPROVEMENT

Why it matters: High-fidelity alerts are those your team investigates—and acts on. Increasing precision improves threat coverage and decision confidence.

Driven by:

- Correlation across identity, behavior, and telemetry
- Integration of curated threat intelligence and peer analytics
- Risk scoring that prioritizes meaningful threats

3. Mean Time to Detect (MTTD) / Mean Time to Respond (MTTR)

TARGET: 60—70% REDUCTION

Why it matters: These are core metrics for board reporting, cyber insurance, and operational performance.

- Improvements driven by:
- Agentic AI handling triage, classification, and escalation
- Unified workflows that replace swivel-chair investigations
- Enrichment pipelines that cut time-to-context

4. Analyst Productivity per Headcount

TARGET: 2—3X INCREASE IN COVERAGE

Why it matters:

Analyst burnout is real, and hiring isn't keeping up. Efficiency matters more than ever.

Improves when:

- Repetitive tasks (e.g., IOC analysis, log pivoting) are offloaded to AI agents.
- Investigations run in a single, enriched timeline
- Detection logic is continuously improved via natural language, not manual scripting

5. Cloud and SaaS Telemetry Coverage

TARGET: 100% VISIBILITY INTO BUSINESS-CRITICAL CLOUD AND SAAS SERVICES

Why it matters: Threat actors thrive in blind spots—especially in your IaaS and SaaS environments.

Track:

- % of business-critical cloud assets under monitoring (e.g., AWS, Azure, GCP)
- % of key SaaS platforms under behavior analytics (e.g., M365, Salesforce, GitHub, Okta) Gaps between telemetry ingested and actual threat detection value

Bottom Line:

SOC modernization isn't just about adopting AI or consolidating tools—it's about improving outcomes. This scorecard helps CISOs prove that modernization efforts are paying off in the metrics that matter most: faster response, smarter coverage, reduced noise, and greater resilience.

Bonus KPIs for Board Reporting & Budget Justification

securonix

Use these supplemental metrics to demonstrate business value, justify investment, and showcase the operational impact of your SOC modernization efforts.

METRIC	WHAT IT SHOWS
Ingestion/Storage Cost per Alert	Cost efficiency and signal-to-noise ratio across your data stack
% of Alerts Auto Triaged by AI	Analyst time saved and maturity of AI adoption
Detection Coverage per $ Spent	ROI on detection investment and budget effectiveness
Time to Onboard New Detection Content	Operational agility and threat readiness
% of Use Cases Covered by Unified Platform	Tool consolidation, TCO reduction and platform efficiency

Pro Tip: These KPIs resonate with CFOs and board members by linking technical outcomes to business value, cost control, and operational scale.

How to Use This Scorecard

- **With the Board:** Demonstrate clear ROI through improved resilience, broader coverage, and increased operational efficiency
- **With the CFO:** Tie modernization investments to reduced TCO and higher performance per dollar
- **With the Security Team:** Prioritize resources towards high-impact areas and identify opportunities for continuous improvement.

What gets measured, improves. What improves, earns continued investment.

securonix

Modern SOC Partner Checklist: What to Look For—and What to Avoid

Every Vendor Says “Modern.” Few Deliver It.

In a crowded security tech market, nearly every vendor promises AI, cloud-native architecture, and automation. But many platforms simply rebrand legacy tech with new labels. **CISOs need outcomes, not buzzwords.**

This checklist helps you cut through the noise and identify platform partners that can truly accelerate your SOC modernization **without adding integration debt, operational drag, or unexpected costs.**

Must-Have Capabilities for a Future-Ready SOC Platform

Cloud-Native by Design, Not Retrofit

Built for the cloud, not patched for it.

What to Look for:

- Saas-native architecture with decoupled compute and storage
- Elastic scaling and multi-region deployment
- Zero infrastructure to manage

Why it matters: “Lift-and-shift” platforms come with hidden infrastructure burdens, limited scalability, and slow upgrades. True cloud-native platforms eliminate those headaches—**saving time, cost, and effort.**

Fully Integrated Detection, Analytics, and Response

One system, clearer insights, faster action.

What to Look For:

- Native SIEM, UEBA, SOAR—not stitched-together tools Unified risk scoring, correlation, and timeline views
- One content pipeline from detection to playbook execution
- Policy-driven automation with real-time response triggers

Why it matters:

Many vendors claim “integration” but deliver siloed UIs, separate ingestion engines, and fragmented policies. Real integration means:

- One timeline from alert to remediation
- One source of truth across alerts, users, assets, and behaviors
- One platform for managing policy, risk, and content. One experience for analysts—not five tabs and a swivel chair

Customer impact: Faster workflows, fewer tools, lower TCO—and more time spent solving threats, not managing platforms.

Curated Detection Content + Modular AI

Stop hand-coding detections from scratch.

Curated content meets modular AI so you can detect faster, respond smarter, and scale without the guesswork.

Look for:

- 500+ behavior-based detection rules curated by threat experts
- Built-in threat intel fusion (TIP engine)
- Modular agents for triage, enrichment, response, and rule generation
- Explainable AI that analyst’s control (not a black box)

Why it matters: Some platforms dump data and expect you to build everything yourself. Others use opaque models that can’t be validated. Neither approach scales or satisfies board-level accountability.

Fast Time to Value

You should see outcomes in weeks—not quarters.

Look for:

- Cloud deployment in your tenant within days
- No dependency on professional services for core use cases
- Overlay analytics that runs alongside your existing SIEM
- First value in <30 days (e.g., alert suppression, detection uplift)

Why it matters: 12-month deployment are obsolete. Your board wants progress this quarter, not next year.

Outcome-Based Pricing Model

Don't pay to store noise.

What to Look For:

- No per-GB ingestion tax
- Licensing aligned to outcomes, not data volume
- Smart tiering and stream filtering to reduce TCO
- Customer-owned cloud support to preserve data sovereignty and avoid cloud markups

Why it matters: Volume-based pricing penalizes scale. Outcome-aligned pricing supports growth and focuses spend on what truly delivers value.

Evaluation Summary: What Separates True Modern Platforms

FEATURE	WHAT TO LOOK FOR	WHY OTHERS FALL SHORT
CloudArchitecture	SaaS-native, elastic, zero infra	Most require on-prem-style maintenance
Unified Detection/ Response	SIEM, UEBA, SOAR, TIP in one core	Most vendors bolt on SOAR/TIP
AI + Detection Content	Modular, curated, explainable,	DIY rules or opaque black-box models
Integrated Architecture	Single timeline, shared policy engine	Disconnected tools = operational complexity
Time-to-value	Up and running with impact in <30 days	Legacy vendors take 6—12 months
Pricing Model	Use-case aligned, no ingestion tax	Volume-based models inflate cost and reduce ROI

Choose Partners That Match Your Mandate

Your board doesn't want another dashboard—they want results. That means measurable threat reduction, faster response, greater analyst efficiency, and lower cost per detection. When evaluating vendors, focus on partners who can align with those mandates and prove real outcomes, not just add more tools to your stack.

securonix

Case Studies & Customer Wins

Proven Outcomes. Powered by Securonix.

Modernizing your SOC doesn't mean starting from scratch. It means delivering faster detection, reducing operational noise, and achieving measurable ROI with minimal disruption. Across healthcare, finance, legal, media, and service provider environments, security leaders are achieving that with **Securonix's Unified TDIR Platform. Cloud-native, analyst focused and powered by Agentic AI, Securonix** unifies **SIEM, SOAR, UEBA, and TIP** into one scalable solution — deployed in **your cloud, on your terms**. It includes **Agentic AI modules** that automate triage, enrich telemetry, reduce false positives, and streamline response, all while maintaining explainability and human-in-the-loop control.

These customer wins highlight what real-world SOC transformation looks like with Securonix at the center.

Alberta Health Services (Healthcare — Canada)

"We got more value in 6 months than in 8 years with our previous SIEM."

The Challenge:

- Legacy SIEM drove high false positives and infrastructure costs
- Analysts spent hours triaging noise with limited behavioral visibility

The Solution:

- Migrated from legacy SIEM to the Securonix Unified Defense SIEM, removing infrastructure and tuning burdens.
- Leveraged behavioral analytics and UEBA to deliver enriched, high-fidelity alerts.
- Used for log management, analytics, and case management, streamlining detection and response.

RESULTS:

- 90% reduction in false positives
- 2—3 analyst hours saved per day
- 3 FTEs refocused on incident response
- Full behavioral analytics and peer group comparisons surfaced subtle threats

Outcome: Streamlined infrastructure, empowered analysts, faster detection.

RAKBANK (Financial Services — UAE)

"We cut investigation time from hours to minutes—and doubled our coverage."

The Challenge:

- Legacy stack couldn't scale storage, delaying investigations by hours
- No behavioral detection or insider threat visibility to catch anomalous activity
- Siloed SIEM stack limited visibility and detection coverage

The Solution:

- Implemented Securonix SIEM with Snowflake for scalable, cloud-native security.
- Enabled UEBA for insider threat detection and behavioral analytics.
- Unified SIEMs into one platform with 1-year hot storage and enriched telemetry.

RESULTS:

- 1-year hot-searchable log retention
- 35% increase in insider threat detection
- Reduced false positives by 15% with enriched telemetry
- Investigation times cut from hours to minutes

Outcome: Search in seconds. Broader coverage. Response accelerated.

NMC Healthcare (Healthcare — UAE)

“We unified 85 facilities and cut audit prep time by a third.”

The Challenge:

- Disconnected systems and no centralized log management
- Compliance audits were manual and time consuming
- Limited visibility into user activity and insider risk

The Solution:

- Deployed Securonix SIEM + UEBA for centralized monitoring and advanced analytics.
- Automated compliance reporting to streamline audit preparation.
- Scalable log ingestion and event processing to support organizational growth.

RESULTS:

- Behavioral analytics flagged suspicious access and policy violations
- Full visibility across facilities with scalable ingestion
- 33% reduction in audit prep time through automation

Outcome: Compliance simplified. Insider risk exposed. Operations scaled.

Media & Production — Global

"False positives overwhelmed our analysts we needed signal, not noise."

The Challenge:

- Limited telemetry (mostly AD and firewall logs)
- No UEBA or insider threat detection • Response efforts bogged down by noise

The Solution:

- Deployed Securonix United Defense SIEM with advance UEBA for behavioral and insider threat detection
- Integrated diverse data sources into a single cloud-native telemetry pipeline
- Enhanced threat detection with threat intelligence integration and customizable use cases

RESULTS:

- Unified telemetry pipeline to enable real-time and end-to-end visibility
- Advanced UEBA and noise cancellation drastically reduced false positives
- Insider threats surfaced quickly with identity-aware detection Outcome: Better signal. Faster response. Less analyst fatigue.

Outcome: Better signal. Faster response. Less analyst fatigue.

Steptoe & Johnson (Legal — U.S.)

"We cut audit prep time by 70% and gained full visibility with minimal staff."

The Challenge:

- Fragmented visibility across 15+ data sources
- No UEBA or SOAR integration for behavior-based detection
- Manual compliance workflows consumed staff cycles

The Solution

- Deployed Securonix Unified Defense SIEM with real-time log aggregation
- Added advanced UEBA for anomaly detection and SOAR Lite for automation
- Seamlessly scaled to ingest 15+ data sources and 65GB logs daily

RESULT:

- 70% reduction in audit prep time
- Continuous threat model tuning improved fidelity and reduced noise
- 10+ critical alerts triaged weekly by a lean security team Outcome: Audit-ready, visibility-rich, and built for scale.

Real Outcomes, Delivered to Real Teams

With Securonix, SOC transformation is a business enabler delivering measurable results without disruption. Customers across industries report:

- Faster detection and reduced false positives
- Analyst efficiency gains of 2-3X
- Full-spectrum visibility across cloud, identity, and network
- Unified analyst workflows across detection, enrichment, and response
- Lower TCO with smart tiering and modular AI
- Seamless, scalable cloud deployment

Real results. From real teams. On a platform built for modern security operations.

securonix

Start Your Modernization Journey with Securonix

From Strategy to Execution: It Starts Here

You've seen what's possible: faster detection, lower noise, better outcomes. You've seen what modern looks like with unified SIEM, SOAR, UEBA, TIP, and Agentic AI in one cloud-native platform.

Securonix offers a low-friction path to SOC modernization that's built for **speed, scale, and measurable results**. Whether you're just starting out or ready to consolidate your detection stack, we'll meet you where you are and help you move fast.

Your 5-Phase Modernization Journey

As introduced in our corporate briefing, these are the pillars of SOC transformation with Securonix:

Modernization Journey

SOC Transformation with Securonix

securonix

Ready to Get Started?

Here are your next steps:

1

Modern SOC Readiness Assessment

Benchmark your SOC maturity and identify high-impact modernization opportunities.
Includes: personalized scorecard, outcome gap analysis

2

Detection & Enrichment Pilot

See high-fidelity detection and AI-powered triage in your environment within 30 days.

Includes: curated content packs, identity analytics, triage agents

3

ROI & TCO Modeling

Project the economic impact of modernization, including false positive reduction, automation gains, and licensing savings via tiered ingestion.

Includes: NPV/ROI forecast, ingestion vs detection cost modeling, SIEM consolidation benefits

4

Partner-Backed Deployment

Deploy with the combined strength of Securonix and our global partner ecosystem. Gain access to architecture experts, workshop facilitation, and implementation support.

Includes: partner-led POCs, joint delivery planning, and CISO-level roadmap consultation

Let's Build Your Modern SOC - Together

Securonix is trusted by global healthcare providers, financial institutions, law firms, manufacturers, and MSSPs to:

- Reduce MTTD and MTTR by 60—70%
- Eliminate 70—90% of false positives
- Increase SOC productivity by 2-3x
- Scale securely, cost-effectively, and on your terms!

We're ready. Your SOC is ready. Let's modernize it together.

Contact us to schedule your SOC Modernization Workshop

To learn more about Securonix, visit **securonix.com**, or follow us on **LinkedIn** and **X**.

securonix