cyderes

WHITE PAPER

Modernizing Security Operations:

Bridging the Gap from Reactive Firefighting to “Everyday Ready” Resilience

In Partnership with Google Cloud

EXECUTIVE SUMMARY:
The SecOps Execution Gap

The current cybersecurity landscape is defined by a paradox:

While **88%** of organizations maintain a Security Operations Center (SOC)

Only **45%** report effectiveness in proactive threat hunting.

70% of professionals surveyed state that high technology investment is failing to translate into operational success.

This "Execution Gap" is driven by four systemic factors:

Alert Fatigue:

Manual triage remains a primary bottleneck. Teams are overwhelmed by false positives, delaying responses to genuine threats.

Visibility Gaps:

69% of organizations increased cloud adoption this year, yet only **49%** feel confident in their security's ability to adapt.

Integration Challenges:

The average SOC manages **10–15** disparate tools, and **52%** of leaders cite poor integration as a top barrier to proactive security.

Staffing Constraints:

Demand for specialized expertise (Cloud, AI/ML) exceeds supply, leading to overextended workloads and burnout.

Modern SecOps must transition from manual, tool-centric triage to an integrated, automated architecture that reduces the cognitive load on personnel.

In 2025, Cyderes partnered with independent research firm SIS International to study the state of enterprise security maturity. The research surveyed 182 director-level and above security leaders across the U.S., U.K., and Europe. The findings focused on the convergence of Identity and Security Operations (SecOps), analyzing how organizations manage access behaviors alongside real-time threat detection.

STRATEGY:
Bridging the Confidence Gap

To move beyond reactive defense, organizations must address “security debt” — the gap where workloads move faster than security controls.

Cloud and Legacy Anchors

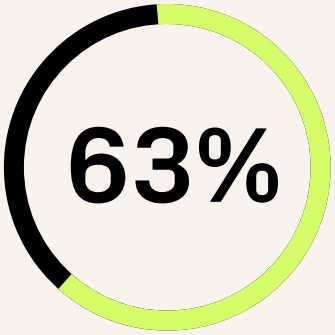
Hybrid complexity forces teams to manage fundamentally different architectures simultaneously. While cloud adoption is a priority, legacy systems in sectors like Healthcare and Finance remain an “anchor.” These older systems often lack API compatibility with modern Zero Trust tools, forcing teams into high-risk workarounds and custom code that creates visibility blind spots.

High-confidence organizations do not retrofit security; they embed it into infrastructure decisions from the outset, focusing on API security and shared responsibility models.

AI: Augmentation Over Replacement

AI is a critical force multiplier for building proactive operations. **70%** of organizations view AI as essential, citing measurable benefits:

Noise Reduction		**66%** see a decrease in false positives
Workload Reduction		**64%** report lower analyst burden
Response Speed		**60%** cite faster incident resolution



The Reality Check:

63% of professionals recognize AI as an augmentation tool rather than a replacement. Human judgment remains indispensable for business context and ethical decision-making.

CASE STUDY:
Solving the “Data Tax”

A global law firm reached a breaking point where rising security costs compromised their posture. Their legacy SIEM utilized a volume-based pricing model, creating a “data tax” that forced them to throttle data feeds to stay within budget — intentionally creating blind spots.

The Solution: The firm migrated to a cloud-native **Threat Detection**, **Investigation**, and **Response (TDIR)** platform to decouple data volume from cost. In just six months, they optimized log feeds, eliminated redundant alerts, and achieved sub-second search capabilities across petabytes of telemetry. By removing the financial penalty for visibility, they restored their defensive posture while freeing internal staff for strategic initiatives.

From The Fragmentation to Integration

Modernizing operations requires shifting from a tool-centric model to a discipline-centric one.

Core Requirements:

Unified Platforms:
Consolidating visibility to overcome the **52%** integration hurdle.

Proactive Posture:
Shifting from incident response to continuous vulnerability management and threat intelligence.

Intelligent Automation:
Handling repetitive triage to free analysts for high-value threat hunting.

24/7 Operational Discipline:
Ensuring monitoring remains reliable every day, not just during crises.

The Philosophy of Maximizing Investments

Rather than a “rip-and-replace” approach, an integration-first model connects existing stacks — Splunk, Microsoft Sentinel, CrowdStrike — into a unified visibility layer. This eliminates vendor lock-in and allows for a coordinated response across multiple platforms simultaneously.

The “Everyday Ready” Standard

The business case for modern SecOps rests on a shift from resignation (“not if, but when”) to prevention. Organizations must build “operational muscle memory” to achieve three core outcomes:

1. **Reduced Risk:**
   Stopping threats before they escalate. Success is measured by reduced dwell time and decreased incident scope via automated containment.

2. **Operational Efficiency:**
   Eliminating tool sprawl to remove the cognitive load of context switching.

3. **Scalability:**
   Utilizing providers that monitor hundreds of environments to recognize attacker behaviors that a single organization might miss.

The Modern Operational Shift

Feature	Legacy Reactive Posture	Modern “Everyday Ready” Posture
Mindset	Acceptance (“Not if, but when”)	Prevention-centric
Focus	Alert volume and triage	Contextual investigation
Availability	Shift-dependent	24/7/365 Continuous discipline
Knowledge	Internal environment only	Broad cross-industry patterns

From Investment To Execution

The execution gap remains stark:

51%
of organizations lack confidence in cloud adaptation

54%
do not feel confident preventing attacks.

These gaps exist despite substantial investment because the operational capability does not yet match the technology.

Bridging these gaps requires a shift toward **continuous operational readiness**. Organizations must prioritize **unified visibility**, strategic automation, and **rigorous operational discipline.** The path forward is not defined by acquiring more technology, but by building better operations on a unified foundation.

Move beyond common secops pitfalls. Access the full data set in our ebook, **How Google Cloud and Cyderes deliver security operations that work** to benchmark your operational maturity and identify your hidden visibility gaps.