Five Tips for Modernizing Security Operations

Security operations teams face growing pressure to work efficiently, reduce investigation time, and show measurable improvement in threat detection, investigation, and response (TDIR). Many CISOs begin their role with a security operations program that functions but lacks consistency, or one that depends heavily on manual practices that slow analysts down. Modernizing your security operations no longer requires a disruptive overhaul. Instead, practical improvements, introduced at the right pace, strengthen how your team works and create lasting gains in performance.

This guide gives you a clear, five-step framework for understanding your current environment, identifying where improvements will have the most impact, and selecting technology and workflows that replace repetitive manual work with connected, predictable processes. The goal is simple: Help your team move from reactive, manual processes to a more consistent and efficient way of working using modern TDIR practices and platform capabilities.

1. Audit Your Security Operations

A strong modernization effort begins with a clear view of how your security operations team functions today. Before choosing new tools or changing workflows, review the systems, processes, and data sources your analysts rely on. Look closely at alert queues, triage steps, and how long it takes to assemble context during an investigation.

Focus your audit on the essentials:

- Current data sources and coverage gaps
- Detection reliability and noise levels
- Manual touchpoints in investigations
- Escalation paths and where delays occur
- Whether existing runbooks reflect daily practice
- The time it takes to complete a standard investigation

This foundational work helps you see which improvements will create immediate, team-wide benefits.

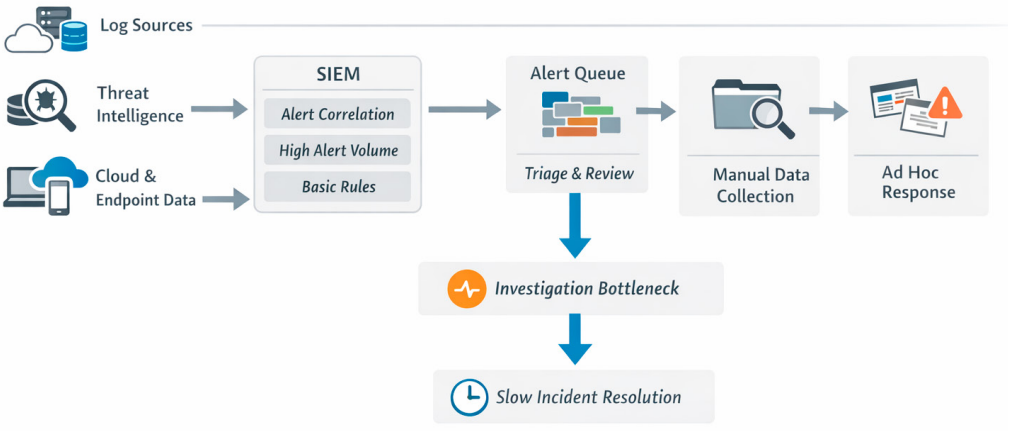

Figure 1. A high-level view of how alerts enter the SOC, how analysts gather information, and where investigation work slows down.

2. Identify What Needs Modernization and What Can Wait

Once you understand how your team works day to day, the next step is learning where analysts feel the most friction. Their insights reveal which tasks consume time without moving investigations forward and which processes break down under pressure.

Useful questions include:

- Which alerts require the most manual validation?
- When investigations stall, what information is usually missing?
- Which tools require repetitive data gathering?
- Which tasks repeat across every shift?

Clear patterns will appear. Many security operations teams point to challenges involving repeated event lookups, difficulty connecting identity-related behavior, or limited visibility into activity across multiple systems. Capture these findings and group them into themes that reflect both small wins and more strategic program needs.

3. Analyze Your Findings and Prioritize Improvements

Use the information gathered from your audit and team discussions to establish a modernization roadmap. The goal is not to fix everything at once. Instead, focus on changes that reduce manual effort, improve detection accuracy, and help analysts complete investigations in less time.

Common high-impact focus areas include:

- Strengthening identity-centric detections
- Reducing the manual steps needed to assemble context
- Improving visibility by onboarding missing log sources
- Standardizing response tasks to reduce variation across analysts
- Shifting from static rule maintenance to behavioral detection approaches

Organize each opportunity by effort and impact. This makes it easier to choose improvements that demonstrate early results while preparing your team for more advanced capabilities later.

Challenge	Root Cause	Opportunity to Improve
Analysts spend too much time validating low-value alerts.	Analysts face a high volume of alerts and have limited context available during triage.	Introduce behavioral analytics and prioritization to surface meaningful activity earlier.
Investigations stall while analysts gather data.	Event details live across multiple tools and require manual lookup.	Use automated timelines to assemble relevant activity into a single view.
Repeated steps slow investigations.	Processes differ between analysts and depend heavily on personal experience.	Standardize investigation and response workflows with guided steps.
Key identity-related activity is difficult to trace.	Gaps in user, device, and cloud data limit availability.	Expand data onboarding and apply dynamic risk scoring to highlight unusual behavior.
Tuning rules consumes more time than investigating real threats.	Static detections require ongoing adjustments and still miss important signals.	Shift to behavioral detection approaches that learn normal activity.
Escalations happen inconsistently.	Missing context forces analysts to escalate prematurely.	Provide enriched event details and recommended next actions at each investigation step.
Reporting progress is difficult and time consuming.	Metrics are gathered manually and aren't tied to daily work.	Track operational metrics like investigation time and throughput with built-in dashboards.

Table 1. A summary of common investigation challenges, what causes them, and where you can improve daily workflows.

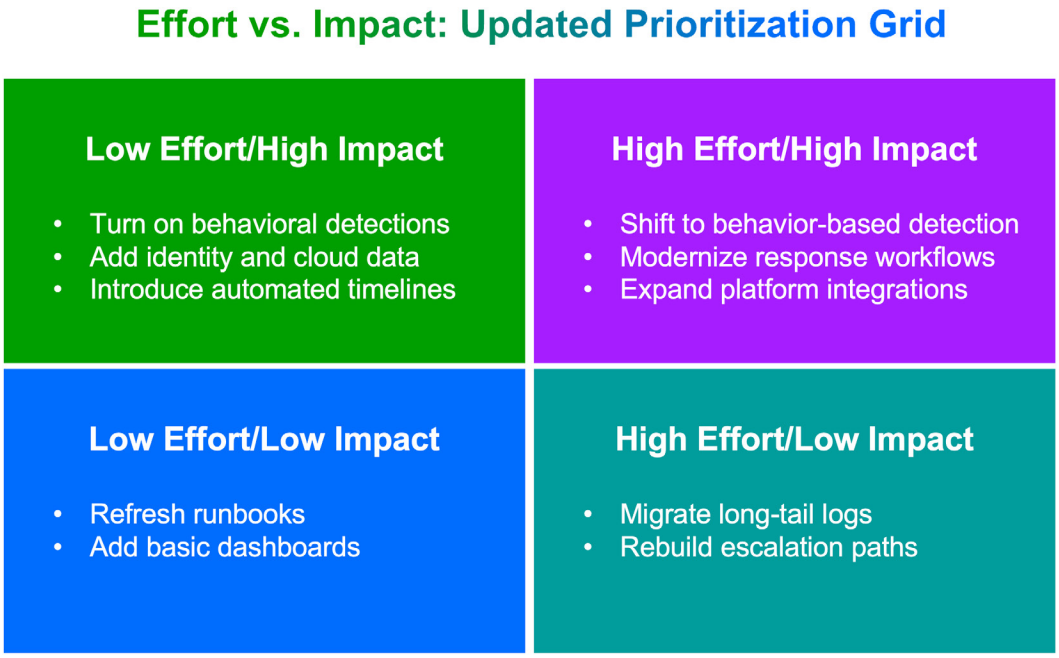

Figure 2. Identify which improvements move the team forward without major disruption.

4. Evaluate Technology Options That Support Your Target Outcomes

Your modernization work is most effective when your technology supports how analysts actually investigate and respond to threats. Instead of piecing together disconnected tools, look for a platform that connects collection, detection, investigation, and response in a single workflow.

As you compare options, prioritize capabilities that improve daily operations:

- Behavioral analytics for more accurate detections
- Automatic timeline assembly that organizes events into clear sequences
- Flexible data onboarding that removes delays
- Guided investigation steps that reinforce consistent processes
- Automated actions that reduce repetitive tasks
- Unified visibility across users, devices, and cloud assets

A connected platform such as the New-Scale Security Operations Platform creates a straightforward path from alert to decision. Analysts spend less time gathering data and more time evaluating what happened.

Standardize Investigation and Response Workflows

Modern security operations teams depend on workflows that guide analysts through each step of detection, investigation, and response. Consistent workflows improve efficiency, reduce variation, and help new team members become productive faster. They also protect your program from skill gaps by making critical tasks easier to follow.

Workflow standardization supports your modernization efforts by:

- → **Reducing repeated data gathering**
- → **Improving triage accuracy**
- → **Supporting consistent processes across shifts**
- → **Strengthening handoffs and review cycles**

Exabeam Threat Timelines help analysts understand what happened by organizing relevant events into a clear, ordered narrative. Recommended actions then guide next steps, reducing guesswork and improving outcomes.

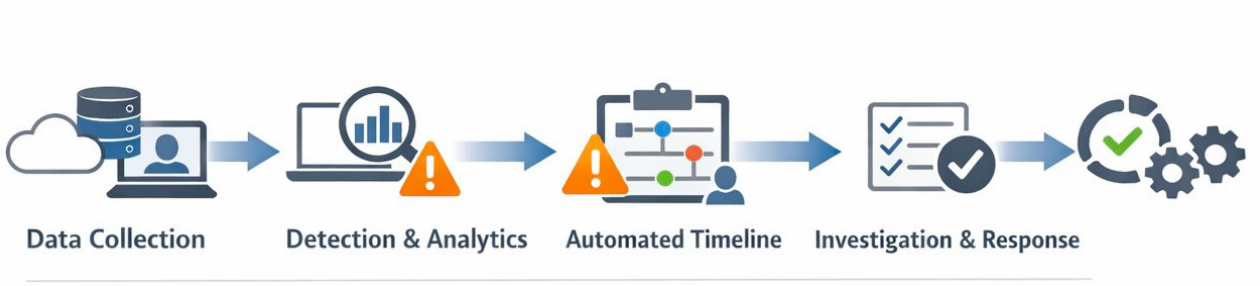

Figure 3. A unified sequence help analysts complete their work with fewer manual steps.

5. Deploy Improvements and Track Results Over Time

Choose one high-value use case to begin your modernization rollout. Identity misuse, suspicious authentication patterns, or cloud misconfigurations often provide strong early results because they benefit directly from behavioral analytics and automated timelines.

As you deploy improvements, check whether:

- Detection quality improves
- Analysts spend less time assembling context
- Triage paths become more predictable
- Response steps follow a consistent pattern
- Investigation throughout increases

Expand to additional use cases once your first scenario stabilizes. Track progress regularly so you can show meaningful improvements in how your team investigates and responds to events.

Exabeam helps security operations teams:

- Gain visibility of internal and external threats like compromised credentials, lateral movement, ransomware, and phishing
- Speed threat detection and response through automation and turnkey playbooks
- Meet regulatory compliance and audit requirements

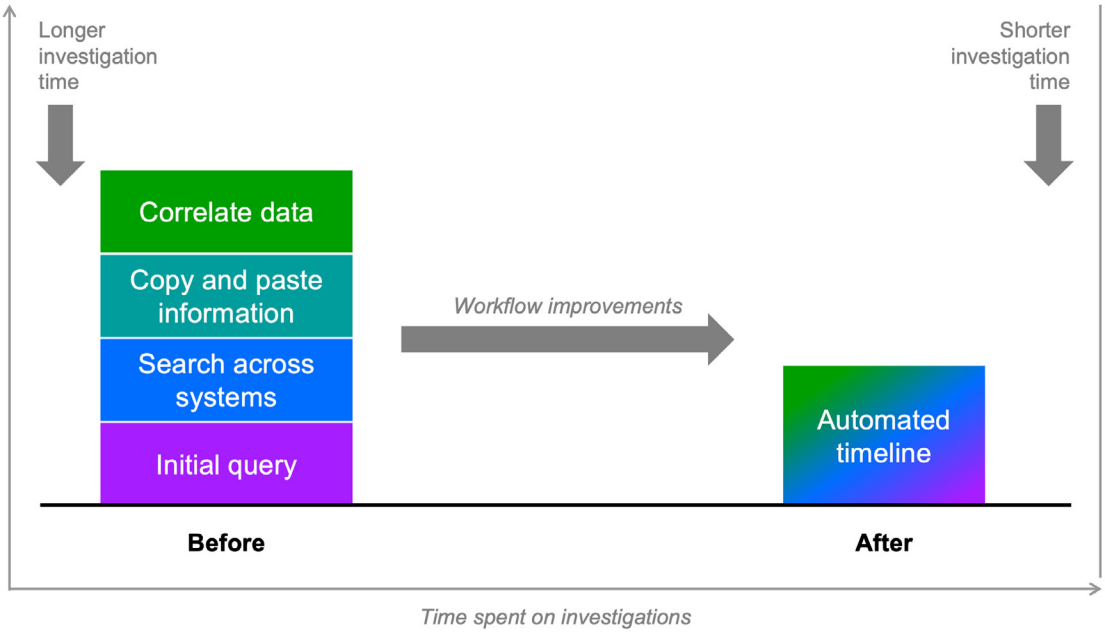

Figure 4. Track how modernization reduces repetitive manual tasks and shortens investigative cycles.

Conclusion

Modernizing security operations doesn't require dramatic restructuring. Instead, steady improvements to how your team detects, investigates, and responds to threats create meaningful, sustained performance gains. By focusing on this structured five-step approach and supporting it with standardized workflows and clear measurement practices, you create an environment where analysts work more effectively and your program moves toward stronger, more predictable outcomes.

Measure, Optimize, and Communicate Impact

Measuring progress is essential to maintaining momentum. Use metrics that show how modernization improves daily work and supports your broader security objectives.

Useful security operations metrics include:

- **Time required to assemble context for investigations**
- **Time to confirm whether alerts are actionable**
- **Investigation throughput per analyst**
- **True-positive to false-positive ratios**
- **Mean time to detect and respond (MTTD and MTTR)**
- **The number of repeated tasks reduced through automation**

Translate these operational findings into clear improvements such as faster decision making, fewer unnecessary escalations, or more consistent results across analysts. These indicators help you communicate progress to leadership and refine your roadmap over time.

About Exabeam

Exabeam is a leader in intelligence and automation that powers security operations for the world's smartest companies. As a global cybersecurity innovator, Exabeam provides industry-proven, security-focused, and flexible solutions for faster, more accurate threat detection, investigation, and response (TDIR).

exabeam

Learn more at www.exabeam.com →