Three Essentials for Modern Threat Detection and Response

Security operations teams handle more data, tools, and alerts than any human can realistically review by hand. Implementing or replacing a SIEM can take months or even years. During that time, analysts often split their time between deployment tasks and day-to-day investigations, which reduces their ability to improve detection and response.

Modern security leaders need a way to strengthen threat detection, investigation, and response (TDIR) without waiting for a complete platform overhaul. That means improving how teams use the tools they already have, then introducing automation, behavioral understanding, and better workflows where those changes deliver the most value.

The New-Scale Security Operations Platform supports this approach. It combines cloud-native SIEM, behavioral analytics, dynamic risk scoring, and guided workflows so analysts can see identity-driven activity, investigate faster, and coordinate response from a single workbench.

This guide explores three essentials for modern detection and response, and how a solution like the New-Scale Platform can help.

Essential 1: Detect Threats Your Point Products Miss

Attackers rarely use a single account or system. They move between VPNs, SaaS applications, endpoints, and servers. They use valid credentials, abuse trusted access, and mislead users through social engineering.

The 2025 Data Breach Investigations Report (DBIR) shows that around 60% of breaches involve a human element, such as phishing, credential misuse, or user error. When activity looks legitimate in isolation, point products and simple rules often fail to connect the dots.

At the same time, many organizations have only partial detection coverage. Research on the state of SIEM detection risk found that typical SIEM deployments include detections for roughly 22% of MITRE ATT&CK® techniques, leaving many adversary tactics unaddressed or under-monitored.

Behavior-Based Detection Closes Visibility Gaps

Static rules and isolated alerts aren't enough when attackers can quickly change infrastructure, tools, and tradecraft. Teams need a way to understand how accounts, hosts, and services behave over time so they can spot unusual activity, even when it doesn't match a known signature.

The New-Scale Platform addresses this by:

- Collecting and normalizing data from identity systems, endpoints, cloud infrastructure, applications, and network sources into a Common Information Model (CIM)
- Building behavioral profiles for users, service accounts, devices, and other entities
- Assigning multi-layer, dynamic risk scores when behavior deviates from normal patterns, peer groups, or business expectations
- Automatically generating timelines that show the full sequence of relevant events, including logins, configuration changes, and access activity

Recommendation

Use a detection platform that supports behavioral analytics and dynamic risk scoring across your existing telemetry, not just new tools. Look for capabilities that:

- Model users and entities over time
- Correlate activity across on-premises and cloud environments
- Present findings through visual timelines rather than isolated alerts

These capabilities give analysts a more complete picture of what's happening and reduce the chances that high-risk behavior gets lost among routine events.

By the Numbers: Detection and Coverage

- **Around 60% of breaches involve a human element, such as credential misuse, social engineering, or error.**
- **Typical SIEM deployments include detections for about 22% of MITRE ATT&CK techniques.**

Essential 2: Increase the Efficiency of Triage and Investigations

Strong detections still generate alerts that must be reviewed. Analysts have to decide which alerts to investigate, gather context from different tools, and reconstruct what happened. When this work is mostly manual, teams face alert fatigue and slower investigations.

The average security operations team receives about 4,484 alerts per day, and analysts spend nearly three hours per day manually triaging those alerts. Even more concerning, 83% of the alerts turn out to be false positives, which means a large share of effort goes into work that does not reduce actual risk.

Automated Triage Reduces Noise

Modern triage workflows should group related events, enrich them with context, and prioritize them based on risk and business impact. In the New-Scale Platform, Threat Center provides this type of triage experience by:

- Grouping behavioral detections and rule-based detections into alerts and cases
- Applying multi-layer risk scoring so the most urgent issues appear first
- Enriching alerts with user and device details, historical activity, and threat intelligence
- Allowing analysts to acknowledge, dismiss, or escalate alerts in place, with changes automatically reflected in case records

Automated Investigation Creates a Complete Story

Instead of manually reconstructing incidents across several tools, analysts should be able to see everything in one timeline. The New-Scale Platform supports this through automated timelines, which:

- Organize events in chronological order for a user, device, or case
- Highlight unusual behavior and high-risk actions
- Include both suspicious and normal actions so analysts can understand context
- Update as new events are ingested or new detections fire

These features reduce the time analysts spend gathering data and increase the time they spend interpreting findings and recommending or executing response actions.

Recommendation

When evaluating detection and response tools, prioritize capabilities that:

- Automatically group detections into fewer, more meaningful alerts or cases
- Provide a unified triage queue with consistent risk scoring
- Create and maintain timelines without manual assembly

This reduces repetitive work, accelerates investigations, and helps analysts move faster from "what happened" to "what needs to happen next."

By the Numbers: Triage and Investigation

- **The average security operations team receives about 4,484 alerts per day.**
- **Analysts spend nearly three hours per day manually triaging alerts and 83% of those alerts are false positives, which take up time that could be spent on real threats.**

Essential 3: Strengthen and Automate Incident Response

Once an incident is confirmed, security teams must contain it, remediate the impact, and capture lessons learned. Many organizations still rely on a combination of manual processes, custom scripts, and separate tools for each part of the workflow. This increases the chances of delays, missed steps, and inconsistent outcomes.

Insider-driven incidents are especially costly. The Cost of a Data Breach Report 2025 indicates that malicious insider attacks are among the most expensive initial breach vectors, with an average cost of $4.92 million per incident. These incidents often take longer to detect and contain because they involve trusted identities.

At the same time, broader studies continue to show that many organizations struggle to close incidents quickly because automation is limited and manual tasks slow response.

Coordinated Response From One Workbench

To improve response, teams need a way to take action directly from the same place where they view detections and investigations. In the New-Scale Platform, response is integrated into Threat Center and automation services so analysts can:

- Trigger actions such as disabling accounts, isolating hosts, or blocking IP addresses from a single interface
- Use automation playbooks that encode repeatable response steps for common threat types
- Integrate with case management and ITSM tools so that tickets and cases update automatically as actions are taken
- See which automations ran, which actions succeeded, and where manual review is still required

This moves response from a set of disjointed tasks to a coordinated workflow.

Recommendation

Focus on response capabilities that:

- Are integrated with the detection and investigation experience
- Provide prebuilt, threat-centric playbooks you can adapt to your environment
- Use open APIs so you can connect to your existing tools for identity, endpoint, networking, and ticketing
- Capture a complete record of actions for audit, compliance, and continuous improvement

This approach reduces the likelihood of gaps between detection and containment and helps teams more reliably address high-impact threats like malicious insiders and identity-driven attacks.

By the Numbers: Response and Impact

- **Malicious insider breaches cost $4.92 million on average, making them one of the most expensive incident types to remediate.**
- **Alert fatigue, manual processes, and a global cybersecurity workforce gap of about 3.4 million professionals put significant pressure on security operations teams and slow response.**

Conclusion

Modernizing detection and response doesn't always require ripping and replacing your entire security stack. The most effective programs focus on three essentials:

1. **Behavior-based detection** to catch threats that static rules and point tools often miss
2. **Automated triage and investigation** to reduce manual work and present a clear story of what happened
3. **Integrated response workflows** that connect detection, investigation, and action in one environment

The New-Scale Platform brings these capabilities together. It combines New-Scale SIEM for scalable data collection and search, New-Scale Analytics for behavioral detection and dynamic risk scoring, and Threat Center and Automation Management for coordinated response.

By focusing on these three essentials, security leaders can reduce alert overload, improve investigation quality, and respond to incidents more consistently, all while making better use of the tools they already have.

Use this guide as a starting point to review your own detection, investigation, and response workflows. Identify where behavior-based analytics, triage automation, or integrated response could deliver the fastest improvements, then prioritize those use cases for your next phase of security operations modernization.

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 →