Automated Investigation Experience

Security operations teams fail due to the limitations of legacy SIEM. Legacy tools don't provide a complete picture of a threat and compel slow, ineffective, and manual investigations and fragmented response efforts. Meanwhile, attacks are becoming increasingly sophisticated and hard-to-detect, and credential-based attacks are multiplying.

Whether it's phishing, ransomware, malware, or another external threat, valid credentials are now the adversaries' primary target. And for insider threat attacks, the adversary already has access to valid credentials. This demands a shift in investment from legacy on-premises, rule-based detection to cloud-native SIEM platforms designed to automate the entire threat detection, investigation, and response (TDIR) workflow.

Exabeam offers automated investigation that changes the way analysts do their jobs. Automate and modernize the entire TDIR workflow to gain a complete picture of a threat, reduce manual routines, and simplify complex work.

Key Features:

- **Enrichments such as threat intelligence, geolocation, and user-host-IP mapping**
- **Risk scores assigned to anomalous event or alerts and aggregated within a timeline to escalate the highest-risk users and assets for analyst review**
- **Automated prioritization of third-party security events and Exabeam alerts with machine learning that understands the rarity of an alert and how often it was fired, among other factors**
- **Customizable, outcome-driven steps for analysts to guide them through to mitigation or resolution of incidents**
- **Automate repeated workflows for investigation into compromised credentials, malware, or malicious insiders**

Automate and modernize TDIR

Fully automate the entire threat detection, investigation, and response (TDIR) workflow; accelerate and streamline security operations

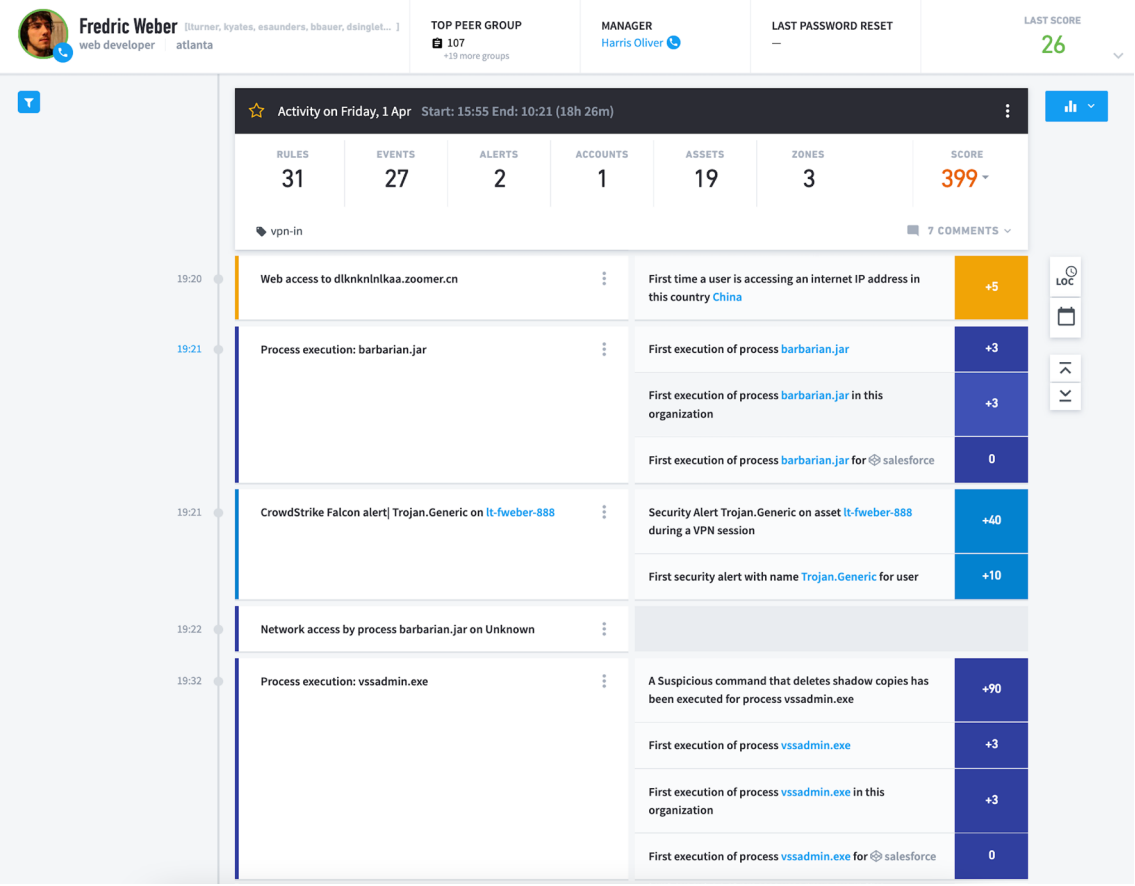
Exabeam automates the entire TDIR workflow to help your security team focus on meaningful work, not tedious, manual tasks. Automatic reconstruction of incident timelines accelerates and streamlines security operations resulting in faster response times and more thorough investigations. Automation of threat detection, investigation, and response activities from a single, centralized control plane turbocharges analyst productivity and reduces response times.

- Automate Threat Detection: automation drives risk scoring, surfacing notable users and activity so your security teams know the most important events to investigate.
- Automate Alert Triage: Exabeam offers automated risk prioritization, identifying and prioritizing the alerts which require the most attention.
- Automate Investigation: contextual Smart Timelines™ automatically reconstruct hundreds of security data points into clear chronologies of security incidents, accelerating investigation.
- Automate Response: build repeatable investigation and response playbooks, or deploy pre-built Turnkey Playbooks automating response to common security scenarios.

Automatically reconstructed security incidents

Reconstruct the chain of incidents using built-in timelines; reduce the time and specialization required to detect, investigate, and respond to security incidents

For all anomalies detected by Advanced Analytics, Exabeam's machine-built incident timelines, called Smart Timelines, stitch together both the normal and abnormal behavior for users and machines. These timelines include all information you need to perform a rapid investigation, including: normal and abnormal behavior, as well as the surrounding context, like what happened before and after an alert, or if this alert maps to a MITRE ATT&CK® tactic, technique, or procedure. Smart Timelines allow security teams to easily investigate event details with minimal technical expertise and without repeatedly querying multiple systems — automating investigation and improving SOC productivity.

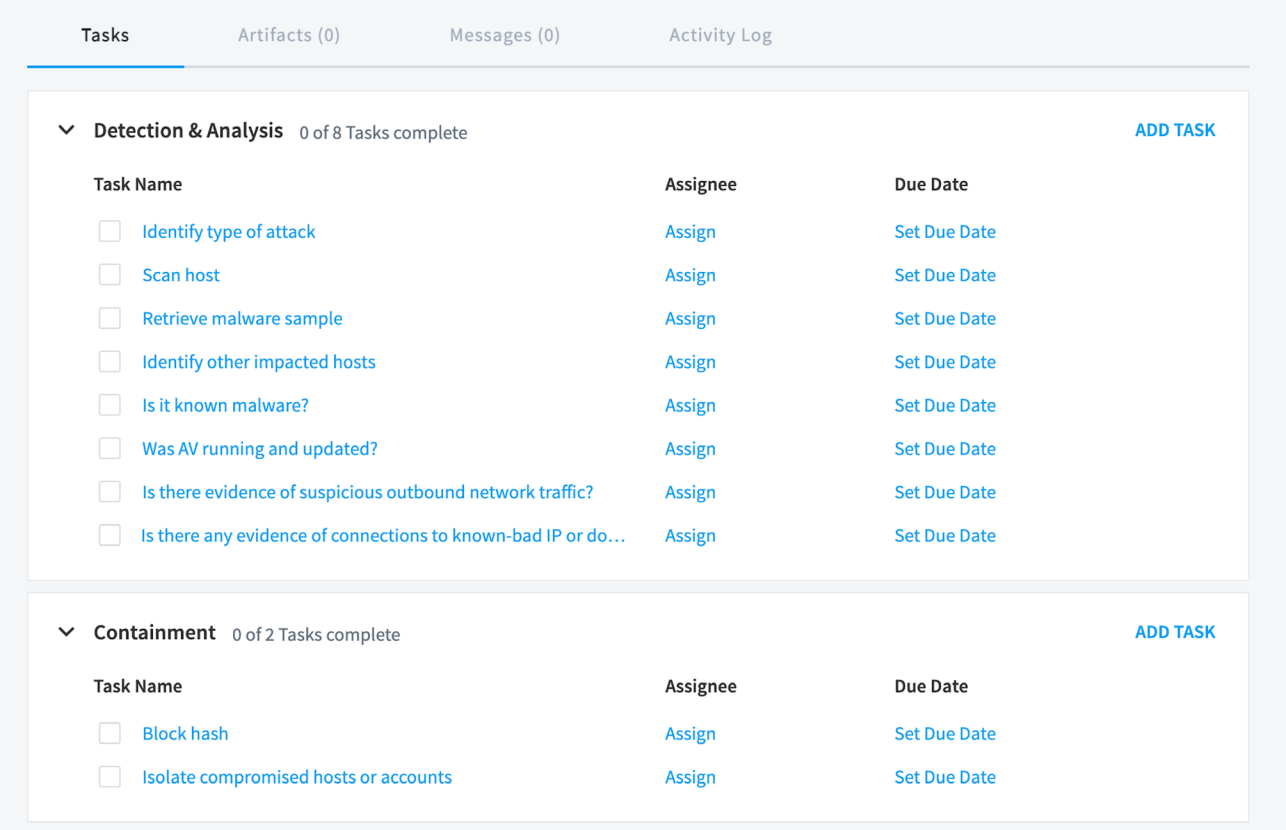


Contextual, built-in response

Quickly see and act on meaningful alerts with automated case enrichment with relevant context, followed by scripted response actions

Alert and Case Management lets analysts organize alerts from Exabeam and other security tools into incidents requiring further investigation or response. Alert and Case Management helps the analyst sort incoming events at volume, making it easy to see the most crucial alerts and cases that correspond to anomalies or high-value signatures. You can manually or automatically sort events into incidents for focused investigation and/or escalation — or export into other third-party workflow solutions.

Auto-attribution of alerts to users and assets, nearby anomalies, and user and host context provides additional context for more effective triage and investigations. Case Management allows alert and case tagging, task creation with assignment options, and an audit trail for your team's steps through investigation and response. Exabeam provides a guided investigation and response checklist, and response actions for you to take to effectively investigate and remediate an incident. Checklists are pre-built for common threat scenarios, but can also be customized to meet your organization's key challenges.



Elevate human performance

Scale operations and people to focus on more meaningful work — recapture 2/3 of analyst time on detection, triage, and investigations*

Automating TDIR allows analysts to achieve faster response times which in turn helps limit the damage attacks may cause to an environment. Consistent, standardized responses across analysts regardless of skill level can help ensure nothing slips through the cracks. Turnkey Playbooks automate repeated workflows for investigation into compromised credentials, external attacks, or malicious insider use cases, without requiring configuration or investment in additional third-party products. With Incident Responder, analysts can orchestrate and automate repeated workflows with APIs to 65 different vendors and 100 products with 576 response actions, from semi- to fully-automated activity. Analysts can automate gathering key pieces of information about incidents via integrations with popular security and IT infrastructure, and run response playbooks to programmatically perform investigation, containment, or mitigation. Automating TDIR improves SOC productivity. Responding to threats faster means organizations better utilize their existing processes and tools, and drastically improve analyst efficiency.

(*Ponemon Institute)

About Exabeam

Exabeam is a global cybersecurity leader that created the New-Scale SIEM™ for advancing security operations. We Detect the Undetectable™ by understanding normal behavior, even as normal keeps changing – giving security operations teams a holistic view of incidents for faster, more complete response.

Learn more about Exabeam today

Get a Demo Now