How Does Exabeam Help Unify Security Operations for OT Environments?

Detect IT-to-OT threats faster with behavioral analytics, automation, and AI-assisted investigations

What Is the Exabeam Solution for OT Security Operations?

Exabeam helps unify security operations visibility and investigations across IT and OT environments using New-Scale Fusion, combining SIEM, behavioral analytics, and automation on a shared data foundation. It prioritizes suspicious behavior with dynamic risk scoring and supports faster investigations with Threat Timelines and Exabeam Nova AI agents, while accommodating cloud and self-hosted deployment needs.

Why OT Security Operations Is Hard

Healthcare providers, energy and utility companies, and other critical infrastructure operators face outsized operational impact when OT incidents occur. Disruptions can interrupt patient care, halt power generation or distribution, and affect public safety. Downtime often lasts longer in OT environments, where systems are designed for availability and safety rather than rapid recovery.

Many OT incidents begin in enterprise IT through phishing, compromised credentials, or abused service accounts. Attackers then move laterally into operational networks and segmented OT VLANs that enforce strict data locality and access controls. In healthcare, this can involve connected medical devices or clinical systems. In energy and utilities, it often includes industrial control systems and substations. When IT and OT telemetry lives in separate workflows, detection slows and investigations become manual and reactive.

OT environments also impose architectural constraints. Data residency requirements, segmented VLAN-based networks, and uptime expectations limit where log data can be stored and how it can move outside operational systems. Security operations teams still need shared visibility into user activity, device behavior, and system interactions across IT and OT environments without disrupting operations or violating locality requirements.

Products & Features

New-Scale Platform

Product: New-Scale Fusion

Relevant Capabilities:

- UEBA
- ABA
- Dynamic risk scoring
- Threat Timelines
- Automation Management
- Playbooks
- Exabeam Nova

LogRhythm SIEM Platform

Product: LogRhythm SIEM

When Used: For organizations that require OT telemetry and logs to remain fully on-prem or within specific VLANs due to regulatory, architectural, or operational constraints

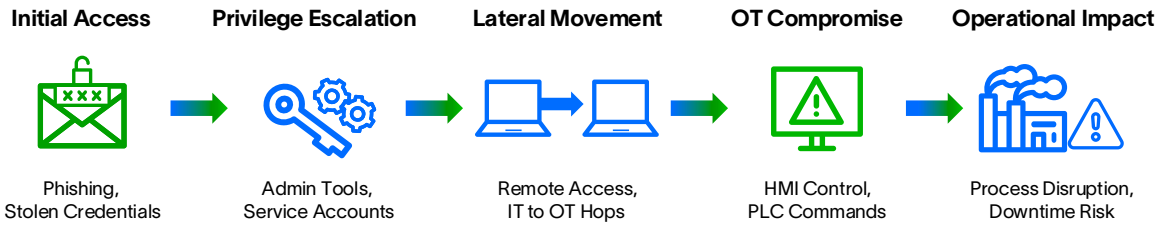

Figure 1.

A typical IT-to-OT intrusion path, from credential misuse to operational impact

The Exabeam Approach

Exabeam helps organizations unify security operations investigations across IT and OT environments while respecting segmentation and data locality constraints. New-Scale Fusion supports flexible deployment models, including cloud and self-hosted architectures, so organizations can analyze OT data that must remain within specific VLANs or on-premises environments.

Behavioral analytics, dynamic risk scoring, and automation are applied consistently across users, service accounts, devices, and OT systems. This approach allows security operations teams to detect threats that move from enterprise IT into segmented operational environments, prioritize real risk, and investigate efficiently without forcing architectural changes that OT teams can't accept.

Key Capabilities and Outcomes

Capability 1: How Does Exabeam Detect IT-to-OT Threat Movement?

Challenge

Attackers often pivot from IT into OT using legitimate credentials and trusted access paths. In segmented environments where OT systems operate on dedicated VLANs, this activity can appear routine when IT and OT monitoring remain disconnected, forcing analysts to rely on slow, manual correlation.

How Exabeam Works

New-Scale Fusion ingests telemetry from enterprise systems and OT sources into a shared investigation layer while allowing OT data to remain within required VLANs or on-premises environments. Analysts investigate user activity, system behavior, and OT signals together, identifying patterns that span IT and OT boundaries. Correlation connects credential misuse in IT with subsequent abnormal behavior involving OT devices or controllers. Threat Timelines assemble related events into a time-ordered view, reducing manual stitching across tools.

Outcome for the Customer

Security operations teams connect IT and OT activity into a single investigation path without breaking segmentation or data locality requirements.

Example

Critical Infrastructure Organization Streamlines Detection and Compliance

A critical infrastructure operator used Exabeam to unify investigations across enterprise and operational environments subject to regulatory oversight. Legacy OT systems generated limited telemetry, making traditional rule-based detection difficult to maintain.

Behavior-based analysis provided consistent visibility into user activity and system interactions across critical systems. Automated investigation timelines reduced manual correlation, helping the security operations team respond faster while simplifying audit and compliance reporting.

Outcome: Reduced analyst workload and improved consistency in monitoring and reporting across regulated systems.

Capability 2: How Does Behavioral Analytics Improve OT Detection Quality?

Challenge

Rule-based detection can miss low-and-slow misuse of trusted credentials, especially where historical baselines are limited and OT telemetry is sparse. Analysts can waste time reviewing routine activity that doesn't represent operational risk.

How Exabeam Works

Exabeam applies user and entity behavior analytics (UEBA) to users, service accounts, devices, and OT systems, and Agent Behavior Analytics (ABA) to AI agents operating in the environment. The platform establishes baselines for normal behavior, including access patterns, command activity, and communication timing. When behavior deviates, dynamic risk scoring elevates activity that deserves review. This approach aligns to OT realities, where attackers may rely on native tools rather than malware.

Outcome for the Customer

You focus analyst time on higher-risk behavior instead of routine noise.

Capability 3: How Does Exabeam Enable Response Without Disrupting Operations?

Challenge

OT response requires control and restraint. Automated actions that work in IT can create safety or uptime risk in operational environments.

How Exabeam Works

When suspicious behavior appears, New-Scale Fusion assembles Threat Timelines that show how risk escalates over time and which accounts and assets are involved. Automation and response playbooks guide containment actions that respect operational constraints. Teams can isolate affected devices, disable compromised accounts, or notify security operations staff without triggering unsafe automated shutdowns. Exabeam Nova AI agents assist with triage and incident summarization to help teams act faster with consistent analysis.

Outcome for the Customer

You shorten response cycles while preserving operational stability.

Example

Global Manufacturer Narrows Focus at Scale

A global manufacturing organization in the life sciences sector used Exabeam to analyze large volumes of cross-environment data spanning IT and OT systems. The security operations team needed to identify genuine threats moving laterally across networks without overwhelming analysts.

Dynamic risk scoring prioritized high-risk behavior and reduced the volume of activity requiring manual review. AI-assisted investigation helped analysts qualify alerts faster and focus on cases that warranted action.

Outcome: Faster alert qualification and more effective prioritization in a high-volume, converged IT-OT environment.

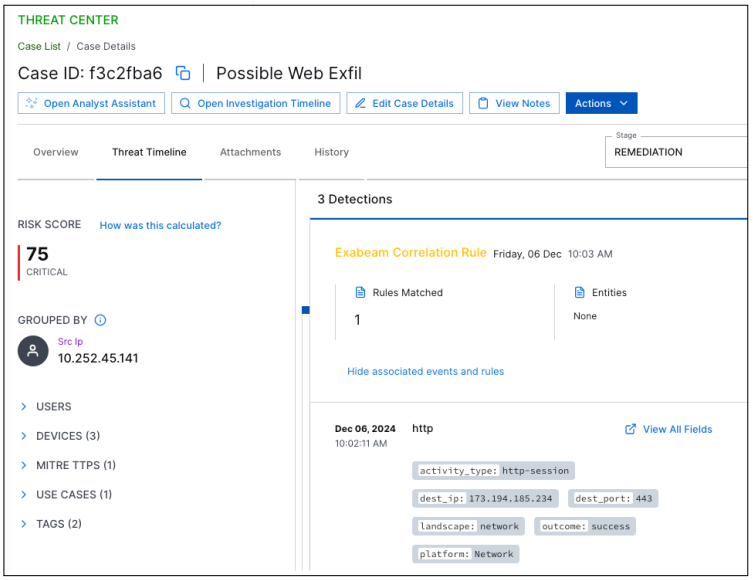

Figure 2.

Threat Timeline in Threat Center grouping related activity into a single investigation view

Exabeam Capabilities for OT Security Operations

Capability	Role in OT Security Operations
Unified Log Management and SIEM	Centralize data from OT devices, industrial systems, and enterprise sources so analysts can investigate activity in one place.
Behavioral Analytics	Establishes normal behavior for users, devices, and OT assets. Highlights anomalies tied to credential misuse and lateral movement.
Threat Timelines	**Connects related IT and OT activity into a clear sequence of events, reducing manual correlation.**
Automated Response Playbooks	**Guide containment actions such as account control, device isolation, and operational notification without disrupting services.**
Exabeam Nova AI Agents	**Summarize incidents, prioritize alerts, and surface relevant context to reduce analyst workload.**

Conclusion

Exabeam helps organizations unify security operations across IT and OT environments while respecting the realities of segmented networks, VLAN-based architectures, and strict data locality requirements. Behavioral analytics, including ABA, combined with automation and AI-assisted investigation, improve detection quality and shorten response cycles in operational settings.

About Exabeam

Exabeam is the leader in behavior intelligence for the agentic enterprise. As organizations deploy digital workers and confront machine-speed adversaries, Exabeam delivers flexible, industry-proven solutions for insider threat coverage of humans and agents and faster, more accurate threat detection, investigation, and response (TDIR). Learn more at www.exabeam.com.

exabeam™

Learn more at
www.exabeam.com →