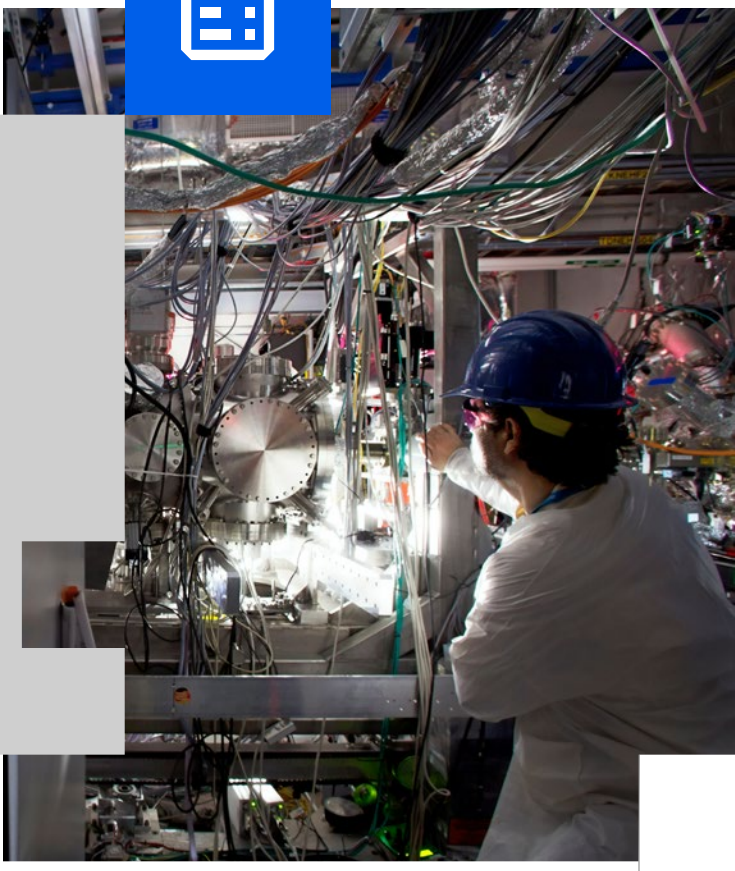
exabeam



Data Sheet

Exabeam Alert Triage

Enable analysts to quickly and confidently dismiss or escalate security alerts

The alert triage process requires analysts to sift through alerts, determine the priority of the alert, and then decide whether or not to escalate it for further review. Analysts must triage and respond to an overwhelming number of alerts spread across disparate tools. However, without performing a lengthy investigation, analysts have no way to efficiently determine whether an alert poses a risk to their organization or not. Without a standard triage process to follow, analysts struggle to rapidly triage alerts, leaving their organization vulnerable to a missed alert resulting in a breach.

Protecting your business from security threats on an ongoing basis requires more than merely presenting your analysts with an expansive list of alerts. Exabeam Alert Triage categorizes, aggregates and enriches security alerts with context like host, IP, severity of alerts and associated users and entities, so analysts can confidently and efficiently dismiss or escalate alerts from a single screen. Analysts get visibility into all of the alerts that security tools have triggered through a centralized view, reducing the likelihood of missing an alert.

Centralize Security Alerts

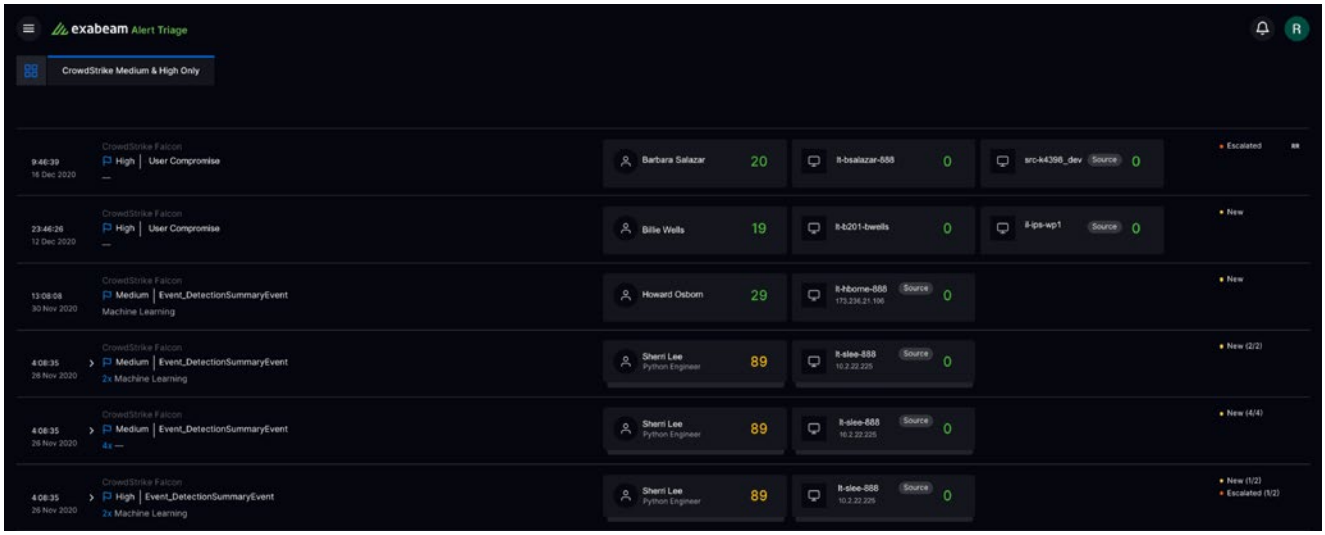
Alert Triage centralizes the alert triage process and organizes an analyst's triage efforts, so they can review alerts faster. Since analysts receive an overwhelming number of security alerts each day spread across various tools, they can easily miss a critical alert. A centralized view of 3rd party and Exabeam Data Lake triggered security alerts provides visibility into all of the alerts that security tools have triggered in an organization, minimizing the likelihood that an alert is missed or overlooked. Which in turn minimizes the likelihood that a missed alert results in a breach.

Categorize Alerts with Channels

With Alert Triage, managers can automatically categorize security alerts into channels to create a targeted list of alerts to prioritize and focus an analyst's time and build subject matter expertise within a team. Channels group alerts by shared traits such as vendor, alert name, alert type, severity and more. For better distribution of work, managers can assign channels to specific analysts or teams. Organizing alerts into channels helps focus an analyst's attention on a specific type of alert, and allows them to develop subject matter expertise. The more an analyst reviews a single type of alert, the quicker they will be able to distinguish a true threat from noise.

Aggregate Similar Alerts with Alert Aggregation

Alert Triage automatically aggregates high frequency alerts that share the same name, type, vendor and severity, so analysts can triage alerts efficiently. Alert aggregation enables analysts to understand how alerts relate to each other, to quickly determine whether an alert is significant. If an analyst determines the alerts do not pose a threat to their organization, the analyst can dismiss the group of alerts. Triaging alerts in batches boosts analyst productivity. Greater productivity means analysts are able to review a higher percentage of the incoming alerts, and reduces the possibility that an alert will go unreviewed and lead to a breach.



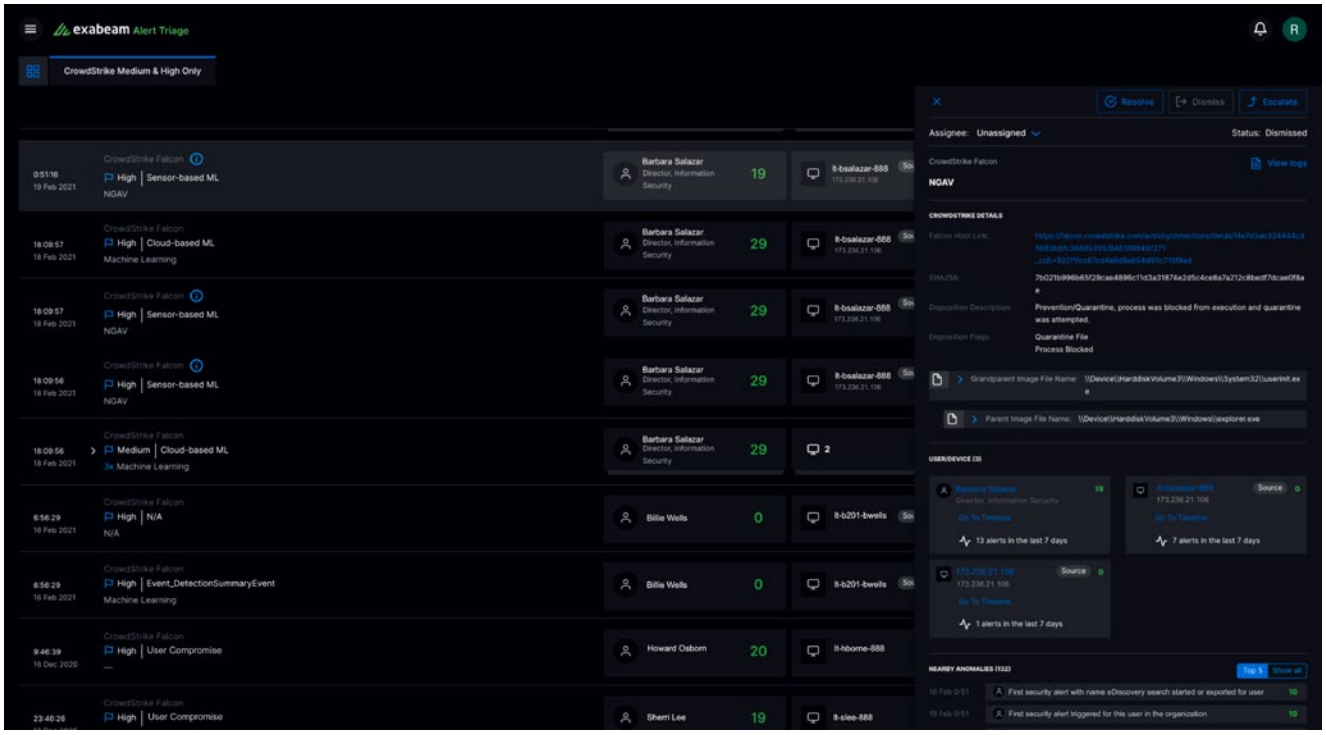
Security alerts are categorized into channels. Channels can be grouped by vendor, alert name, alert type, and severity. For example, here we see a channel for medium and high alerts from CrowdStrike.

Automate Triage with Context Enrichment

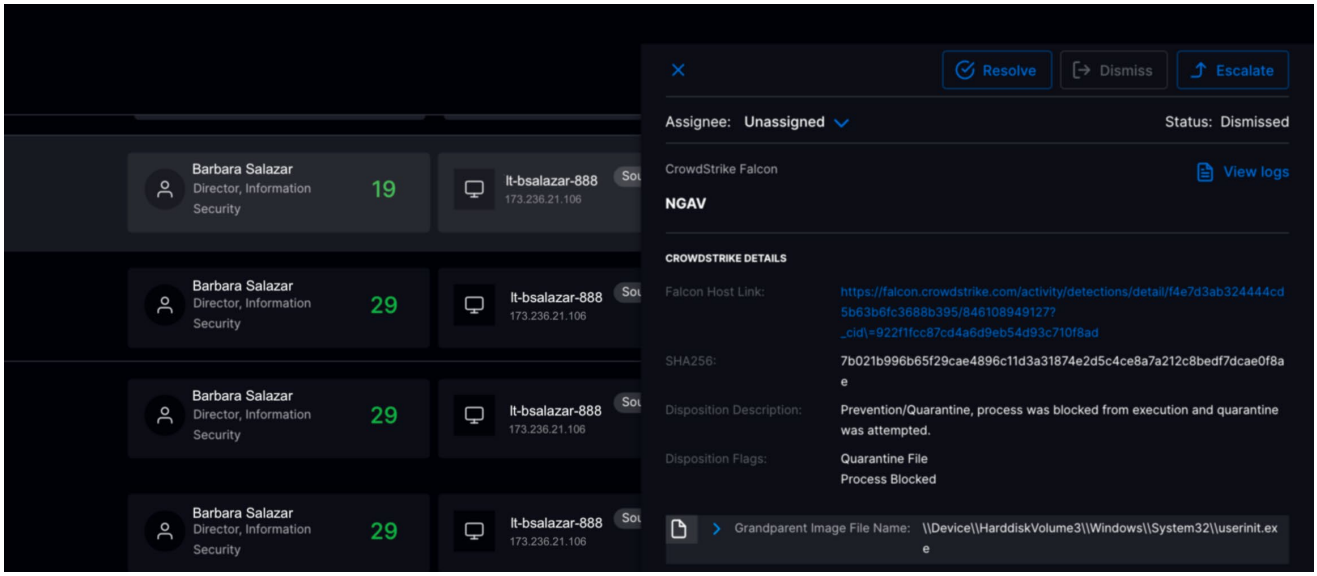
Alert Triage enriches security alerts with the context needed to rapidly review and triage alerts from a single screen. The context provides answers to questions like: What is the nature of the alert? Who is the user/asset associated with the alert? Is this an actual attack? Was the attack successful? Without the need to pivot and query in a SIEM, analysts have the context they need to rapidly escalate or dismiss an alert. Automating the triage process with context enrichment improves analyst productivity, thus enabling them to close more alerts faster with minimal technical expertise and without repeatedly querying multiple systems.

Streamline Incident Creation

Alert Triage integrates with Exabeam Case Manager to automatically create incidents from escalated alerts. When an alert is escalated, an incident is automatically created, handing off the alert to the incident response team. The case includes alert-specific information like alert name, type, and severity, so an incident responder can quickly continue the investigation. Integration with incident response automates the final step of the triage process and forwards notes and research to the incident responder, expediting an analyst's ability to triage alerts.



Security alerts are enriched with context including host, IP, severity of alerts and associated users and entities.



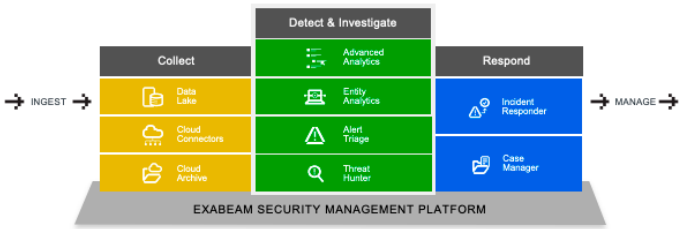
When an analyst reviews an alert, the alert provides an option for the analyst to quickly dismiss or escalate the alert.

Exabeam Security Management Platform

Exabeam helps security teams outsmart the odds by adding intelligence to their existing security tools – including SIEMs, XDRs, cloud data lakes, and hundreds of other business and security products. The Exabeam Security Management Platform helps you enhance your current security tools incrementally by adding improved threat detection, repeatable, threat-centric outcomes, and improved productivity.

The Exabeam Security Management Platform includes:

- Data Lake
- Cloud Connectors
- Cloud Archive
- Advanced Analytics
- Entity Analytics
- Alert Triage
- Threat Hunter
- Case Manager
- Incident Responder



To learn more about how Exabeam can help you visit exabeam.com today.