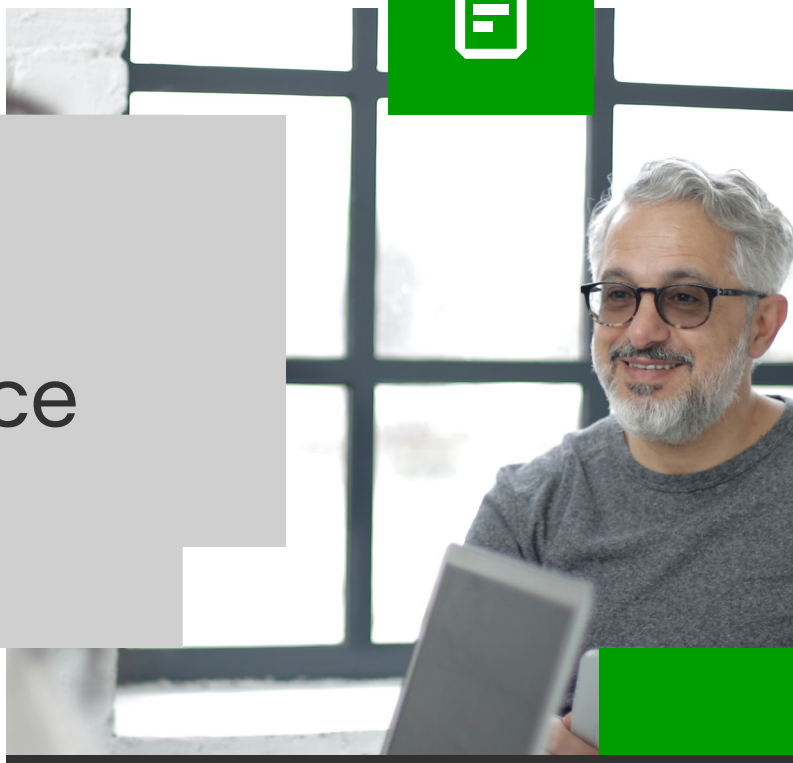
exabeam

Data Sheet

Exabeam Threat Intelligence Service

Integrated Threat Intelligence enables smarter workflows



Understanding your adversaries is a priority for any security organization. But how can you fight these adversaries without knowing the bad actors or locations? Exabeam Threat Intelligence Service provides critical visibility and knowledge about security threats, threat actors, and indicators of compromise (IoCs), which can give your security team more accurate risk scores evaluating attackers — improving your understanding of the danger they pose to your environment.

Exabeam Threat Intelligence Service integrates curated feeds from ZeroFox and OSINT across the Exabeam SOC Platform and workflows. With Threat Intelligence Service, analysts can leverage known malicious IP addresses, domain reputation, and other IoCs without needing to install apps, write scripts, or alter workflows. Threat Intelligence Service infuses detection and response efforts with IoCs. The result is higher accuracy correlation rules and behavioral analysis models, and more detailed forensic and threat data in automated response playbooks and use cases.

Benefits

- **Native integration with SIEM, UEBA, and SOAR workflows within the SOC Platform to improve analyst productivity**
- **Machine learning-based curation uses raw threat intelligence data to find malicious IoCs**
- **Included free in all Fusion SIEM and Fusion XDR products**

Interested in learning more?
Sign-up for a demo today.

Avoid disjointed workflows and add-on fees

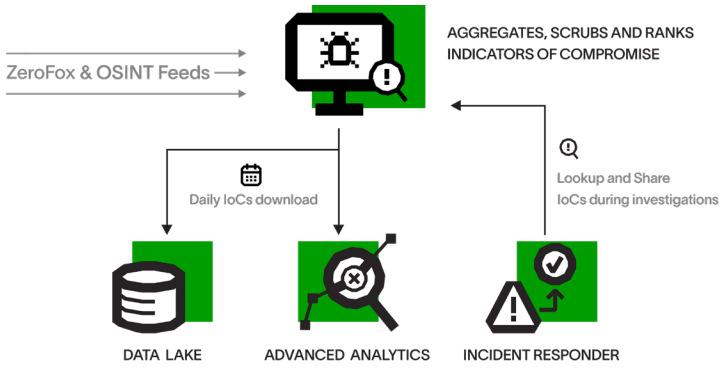
Threat Intelligence Service is a free add-on that ships out-of-the-box as part of the Exabeam SOC Platform for both Fusion SIEM and Fusion XDR. Threat Intelligence Service uses known malicious IP addresses, domain reputation, TOR network sources, destinations, and other IoCs to create smarter risk scores without needing to install apps, write scripts, or alter workflows. The result is highly accurate correlation rules and behavioral analysis models, as well as more detailed forensic data in automated response playbooks.

How it works

Threat Intelligence Service ingests ZeroFox and OSINT threat intelligence feeds, which it aggregates, scrubs, and ranks using proprietary machine learning algorithms to produce a highly accurate, up-to-date stream of IoCs. This feed is published to all products in the SOC Platform and is refreshed every 24 hours.

The Threat Intelligence Service integration powers many of the pre-packaged use cases by providing global telemetry and pairing it with the internal intel derived via behavioral analytics. This allows:

- Analysts to easily search for IoCs within log data
- Use of threat intelligence data as an input for analytics and elevating risk to user or entity sessions based on anomalous activity
- Forensic analysis and investigation via one of Incident Responder's automated response playbooks



Categories of IoCs threat feeds available via Threat Intelligence Service include:

- IP addresses associated with ransomware or malware attacks
- Domain names and URLs associated with sites that often contain malware, drive-by compromises, and more
- Domain names associated with phishing or ransomware
- Known TOR endpoints

Exabeam SOC Platform

About Exabeam

Exabeam is a global cybersecurity leader with the mission to add actionable intelligence to every IT and security stack. The leader in Next-gen SIEM and XDR, Exabeam is reinventing the way security teams use analytics and automation to solve threat detection and incident response (TDIR). Exabeam offers a comprehensive cloud-delivered solution that uses machine learning and automation focused on a prescriptive, outcomes-based approach. We design and build products to help security teams detect external threats, compromised users, and malicious adversaries while minimizing false positives to protect their organizations.

For more information, visit exabeam.com.