exabeam

EXABEAM THREAT INTELLIGENCE SERVICE DATASHEET

Natively Integrated Threat Intelligence Enables Smarter Workflows

Understanding your adversaries should be a top priority for any security organization. Threat intelligence services aid this effort by providing critical knowledge about security threats, threat actors, and indicators of compromise (IoCs), which can give your security team an edge against attackers—thus making your team better equipped to defend your organization.

Exabeam Threat Intelligence Service fully integrates a natively curated threat intelligence feed across the Exabeam Security Management 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 data in automated response playbooks.

AVOID DISJOINTED WORKFLOWS AND ADD-ON FEES

Threat Intelligence Service—one of the Exabeam Cloud Security Services—ships out of the box as part of the Security Management Platform and does so at no additional cost. Threat intelligence Service is embedded directly into Exabeam's security information and event management (SIEM), user and entity behavior analytics (UEBA), and security orchestration and automation (SOAR) workflows to help analysts identify and mitigate new and emerging attacks using fresh indicators of compromise without the swivel chair incident response user experience that plagues other threat intelligence platforms. Eliminating the need to toggle back and forth between a SIEM, 3rd party threat intelligence platform, and point security products—in order to operationalize threat intelligence data—allows security analysts to take action on IoCs without suffering productivity loss.

KEY FEATURES:

- Native integration with SIEM, UEBA, and SOAR workflows within the Security Management Platform to improve analyst productivity
- Machine learning-based curation transform raw threat intelligence data into a highly accurate feed of malicious IoCs for use in threat detection

HOW IT WORKS

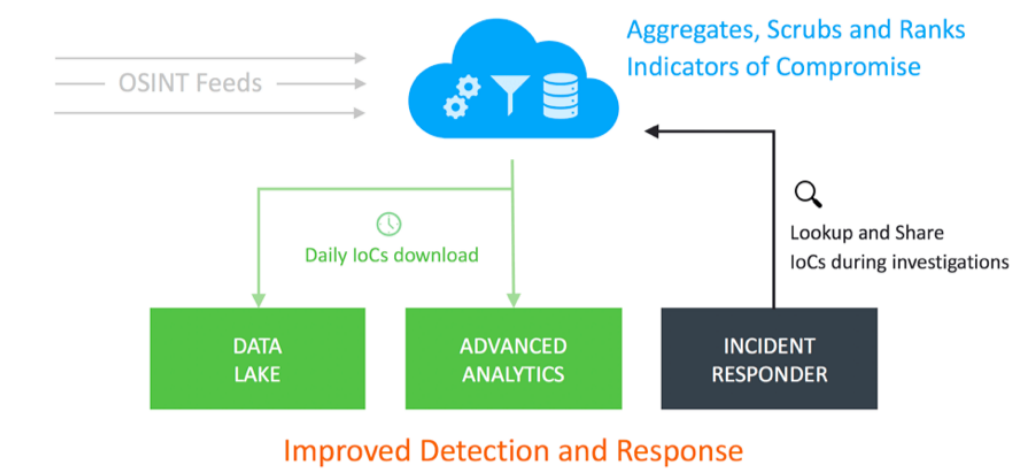
Threat Intelligence Service ingests several open-source threat intelligence feeds, which it then aggregates, scrubs, and ranks using proprietary machine learning algorithms to produce a highly accurate, up-to-date stream of IoCs. This feed is published to all products in the Security Management Platform in a once a day update.

Threat Intelligence Service is consumed via daily updates by all Exabeam products, example use cases include:

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

Categories of IoCs made available via Threat Intelligence Service include:

- IP addresses associated with ransomware or malware attacks
- IP addresses associated with the TOR network
- Domain names associated with ransomware, phishing or malware attacks

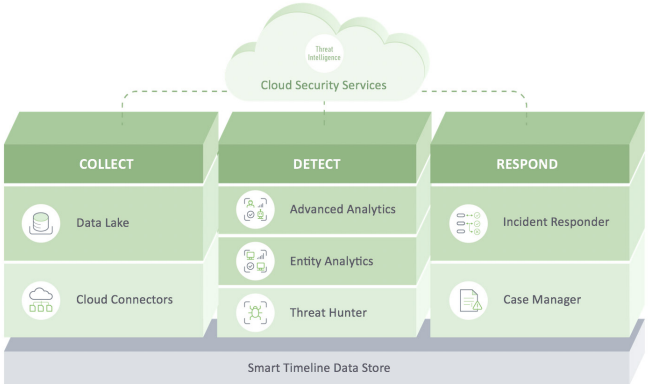


EXABEAM SECURITY MANAGEMENT PLATFORM

Threat Intelligence Service is key component of the Exabeam Security Management Platform.

The platform includes:

- Exabeam Data Lake
- Exabeam Cloud Connectors • Exabeam Advanced Analytics • Exabeam Entity Analytics
- Exabeam Threat Hunter
- Exabeam Case Manager
- Exabeam Incident Responder



FOR MORE INFORMATION, PLEASE CONTACT EXABEAM AT INFO@EXABEAM.COM