RAPID7 + elastic

INTEGRATION BRIEF

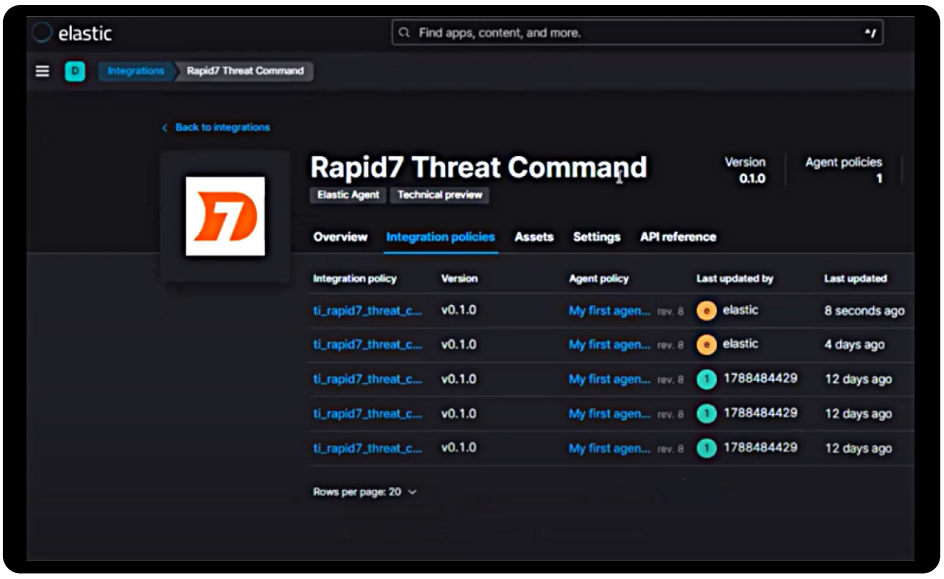
Rapidly Remediate External Threats

Protect your environment by integrating Threat Command and Elastic data

Joint customers can quickly gain valuable insights from the data correlation between Rapid7 Threat Command and their Elastic SIEM environments. Once users configure and activate the integration between the two platforms, they can leverage Threat Command to better assess their attack surfaces, detect suspicious behavior, and employ intelligent automation to remediate threats faster.

Integration overview

The Rapid7 Threat Intelligence and Elastic SIEM integration allows users to retrieve organization-specific alerts from Threat Command, Indicators of Compromise (IOCs) from the Threat Intelligence Platform (TIP), and Common Vulnerabilities and Exposures (CVEs) from Vulnerability Risk Analyzer. Once a user has configured the integration, data streams will begin to yield actionable information based on filters for severity, type, and status.



Capabilities and Benefits

- **View** and act on all data streams from a centralized dashboard.
- **Analyze** data via graphical representations like pie charts and geographical maps.
- **Investigate** specific IOCs via a direct link into the Rapid7 Threat Command TIP.
- **Retrieve** IOCs from up to six months ago.
- **Identify** threats faster across an expanding attack surface.

Rapid7 Threat Command

Find and mitigate external threats

Rapid7 Threat Command continuously discovers critical threats targeting your business by mapping external intelligence to your unique digital assets. Threat Command delivers tailored intelligence from across the clear, deep, and dark web in the form of actionable alerts categorized by severity, type, and source. Customers can fine-tune alert creation based on relevant characteristics of threats and implement unique rule sets to define exactly what constitutes an alert, based on specific criteria.

Threat Command is a leading platform for Digital Risk Protection featuring best-in-class remediation capabilities and seamless integration with existing security solutions to eliminate operational vulnerabilities, secure data, and protect resources.

Elastic

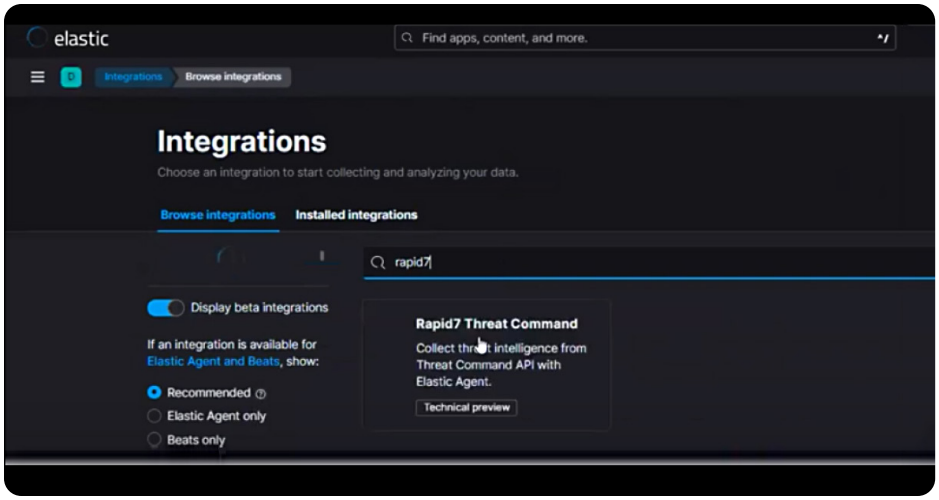
Elastic enables users to connect, scale, and explore data throughout cloud-native infrastructure and applications. Users can leverage a new approach to SIEM that offers fast and flexible search, investigation and hunting through years of archives, and the ability to block ransomware and malware with a single agent. Elastic provides visibility across a user's global environment to tackle threats at scale.

Get started today

Begin collecting intelligence from the Threat Command TIP

Please follow these initial steps to enable the integration:

- Install Elasticsearch (for storing and searching data) and Kibana (for visualizing and managing data).
- Add the Threat Command integration on the external tab of the Elastic platform Integrations page.
- Check prerequisites for Transforms and prerequisites for Actions and Connectors.



For Additional Information

- Refer to the Threat Command User Guide.
- Refer to the integration technical documentation.
- Contact Customer Support.

About Elastic

https://www.elastic.co/

About Rapid7

Rapid7 is creating a more secure digital future for all by helping organizations strengthen their security programs in the face of accelerating digital transformation. Our portfolio of best-in-class solutions empowers security professionals to manage risk and eliminate threats across the entire threat landscape from apps to the cloud to traditional infrastructure to the dark web. We foster open source communities and cutting-edge research–using these insights to optimize our products and arm the global security community with the latest in attacker methodology. Trusted by more than 10,000 customers worldwide, our industry-leading solutions and services help businesses stay ahead of attackers, ahead of the competition, and future-ready for what's next.