RAPID7 + MISP Threat Sharing

INTEGRATION BRIEF

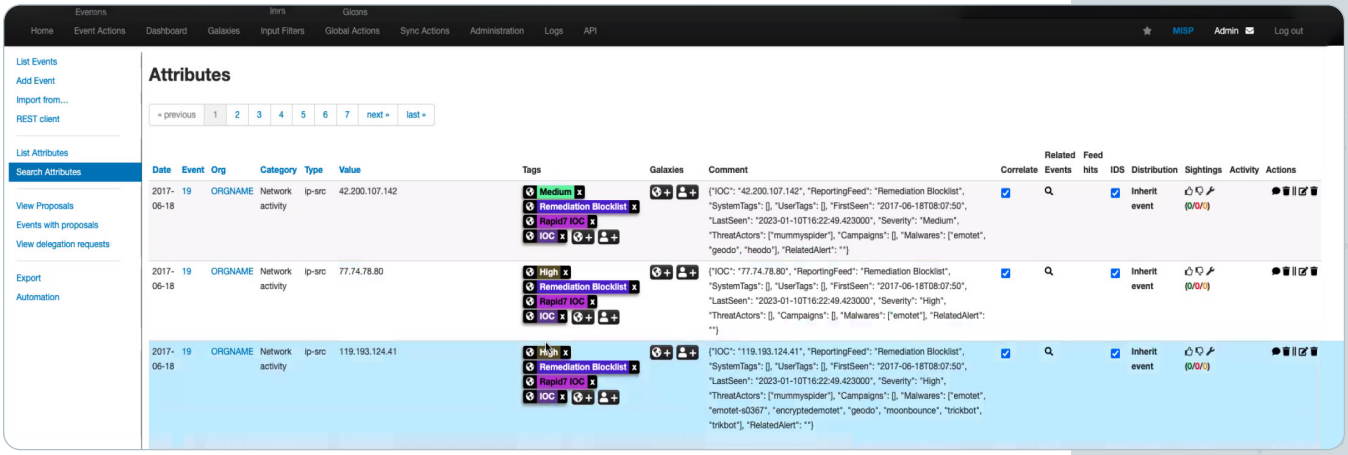
Prioritize and Automate Threat Response

Configure a MISP cloud device to pull IOCs from Rapid7 Threat Command

The Rapid7 and MISP integration allows customers to configure a cloud device to quickly pull Indicators of Compromise (IOCs) from the Threat Command Threat Intelligence Platform (TIP). The TIP levels up the user's ability to add context to IOCs so they can prioritize and automate response. MISP, an open source TI platform, adds an additional layer by automatically correlating relationships between attributes and IOCs from malware, attack campaigns, and more. With this integration, a user can stop threats earlier by better connecting the dots between IOCs and getting the full picture of a potential threat.

Integration overview

The integration creates events on MISP based on IOC group name and current date. IOCs are pulled from the Threat Command TIP with enrichment data including: first seen, last seen, source name, source confidence, severity, alert ID, user tags, system tags, threat actors, campaigns, and associated malware families. Once the IOCs have been added to MISP, integration users will be able to see all the relevant context and relationship data.



Benefits and Capabilities

- **Minimize** digital risk by taking down malicious campaigns as quickly as possible.
- **View** your entire digital footprint in a single-pane-of-glass dashboard.
- **Examine** updated relations with new data as it's added to MISP.
- **Transform** IOCs into actionable threat intelligence.
- **Detect** and prevent attacks, fraud, and threats.

Using Rapid7's MISP integration, we are able to check thousands of malicious indicators through our threat hunting tools. Grouping IOCs in separate MISP feeds enables more accurate and efficient threat hunting. While in MISP, Threat Command's tagging system allows our analysts to quickly understand the severity of the indicator and decide on further actions.

Security Engineer, Cyber Defense Operations, Large EMEA-Based Global Insurance Company

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.

MISP

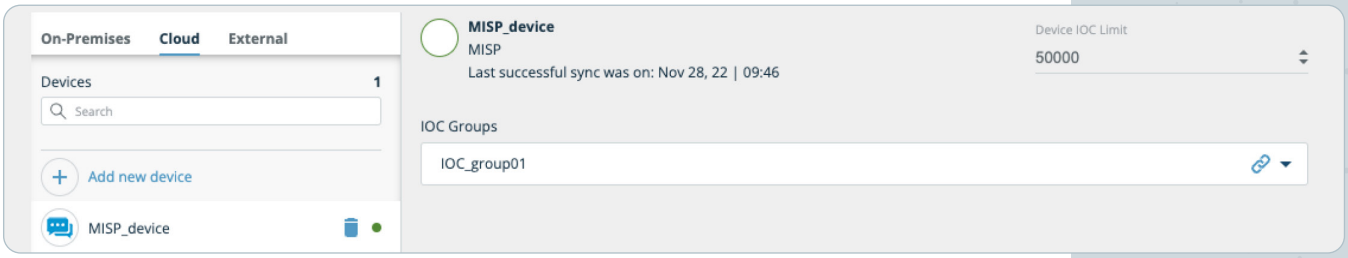
An open-source threat intelligence and sharing platform, the MISP project is designed for incident analysts and security professionals to support their day-to-day operations. It develops utilities and documentation for more effective threat intelligence by enabling users to share, store, and correlate IOCs in a structured manner. Leveraging the context that comes from this process, users can better spot and prepare for targeted attacks, financial fraud, vulnerabilities, and even counter-terrorism data.

Get started today

Add a cloud device to the TIP

Users must first add a MISP cloud device to the Threat Command TIP before then configuring the device to pull IOCs from Rapid7.

- Log in to Threat Command.
- From the main menu, select **Automation > Integrations.**
- From the Integrations page, click **Cloud.**
- Click **Add new device.**
- In the **Add New Cloud Device** dialog, type a **user-defined name** for the device (max 50 letters, spaces, numbers, and underscores).
- Select the **Device type** (The default device IOCs limit is displayed).
- Click **Add.**
- To verify that the new device is added, refresh the **Automation > Integrations page.**



About MISP

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.

For additional information

- Refer to the Threat Command User Guide
- Contact Customer Support: intsights-support@rapid7.com

RAPID7

PRODUCTS

Cloud Security
XDR & SIEM
Threat Intelligence
Vulnerability Risk Management
Application Security
Orchestration & Automation
Managed Services

CUSTOMER SUPPORT

Call +1.866.380.8113

To learn more or start a free trial, visit: https://www.rapid7.com/try/insight/