Recorded Future and TheHive

PRODUCT OVERVIEW

TheHive is a scalable, open source and free Security Incident Response Platform, tightly integrated with MISP (Malware Information Sharing Platform), designed to make life easier for SOCs, CSIRTs, CERTs and any information security practitioner dealing with security incidents that need to be investigated and acted upon swiftly. TheHive enables analysts to collaborate, elaborate, and act to gain precious insight, speed up your investigation, and contain threats.

JOINT INTEGRATION DESCRIPTION

Recorded Future for TheHive allows users to Enrich observables using Recorded Future's open, closed, technical and proprietary intelligence via Cortex Analyzers. Additionally, users can feed Recorded Future alerts into TheHive to automate case creation.

CHALLENGES OVERCOME THROUGH INTEGRATION

The integration between TheHive and Recorded Future provides the necessary context around incident observables to assist incident responders in making more informed decisions, quicker dismissal of false positives, prioritizing incidents to reduce risk, and overall saves analyst time. Automated case creation in TheHive from Recorded Future alerts related to company risk such as newly registered typosquatting domains, leaked credentials found on the dark web, and much more.

USE CASES

The integration between TheHive and Recorded Future allows security responders to:

- Detect and gain context on IP Addresses, Domains, URLs, and Hashes with real-time external intelligence to identify true incidents and dismiss false positives. Context from Recorded Future includes risk scores, risk rules, and evidence details as well as related Threat Actor, Attack Vector, Malware, and other related IOCs.
- Bring Recorded Future alerts into TheHive to automate case tracking while improving time to response.
- Reduce time for threat detection, remediation, and response

About Recorded Future

Recorded Future arms security teams with the only complete threat intelligence solution powered by patented machine learning to lower risk. Our technology automatically collects and analyzes information from an unrivaled breadth of sources and provides invaluable context in real time and packaged for human analysis or integration with security technologies.

About TheHive

A scalable, open source and free Security Incident Response Platform, tightly integrated with MISP (Malware Information Sharing Platform), designed to make life easier for SOCs, CSIRTs, CERTs and any information security practitioner dealing with security incidents that need to be investigated and acted upon swiftly.

DATA SHEET