Uptycs

Detection and Investigation for Modern Hybrid Environments

Detect Important Events and Speed Up Investigations

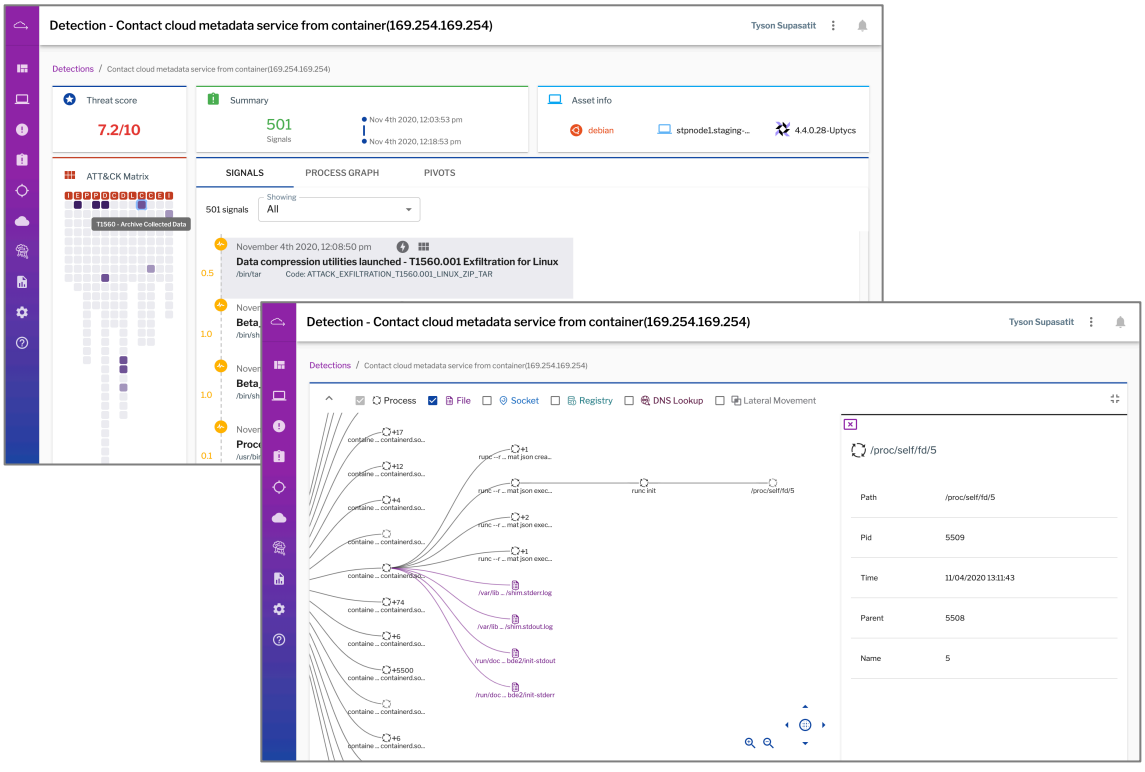
Uptycs collects a wealth of rich host data from Linux, macOS, Windows, and container environments in your datacenter and in the cloud so SOC teams have the broadest coverage possible for detection and investigation.

- **Connected insights:** Uptycs presents a unified view of hybrid environments so analysts can correlate activity across their on-premises and cloud deployments.
- **MITRE ATT&CK mapping:** Signals that comprise a detection are mapped to the MITRE ATT&CK framework so analysts can more easily understand the nature of an incident. Uptycs employs 500+ behavioral rules to cover the tactics and techniques described in MITRE ATT&CK.
- **Context-rich visualizations:** An intuitive process graph helps analysts see the parent-child relationships of processes involved in a detection, as well as artifacts such as files, sockets, DNS lookups, user logins, and registry entries.
- **Integrated threat intelligence:** A continuously updated threat intelligence database combines Uptycs' proprietary research, open-source data, and your own feeds.
- **Historical state:** The Uptycs Flight Recorder helps investigators reconstruct an exploit or attack on a system, even in ephemeral cloud workloads that are no longer running.
- **SIEM and SOAR integration:** The Uptycs API can send event information to your existing security systems for correlation and automated response.

MULTIPLE USE CASES: AUDIT & COMPLIANCE, FLEET VISIBILITY, THREAT DETECTION, AND MORE

FOR ENDPOINTS, SERVERS, CONTAINERS, & CLOUD

REAL-TIME, STREAMING & HISTORICAL QUERYING



SEE IT LIVE! www.uptycs.com/live-demo

aws partner network
Select Technology Partner

CIS SecureSuite® Membership

WWW.UPTYCS.COM