Uptycs

Live & Historical Incident Investigation

FOR DOCKER, MACOS, LINUX, WINDOWS

LIVE & HISTORICAL QUERYING

FLEET VISIBILITY

INTRUSION DETECTION & INCIDENT RESPONSE

VULNERABILITY MONITORING

AUDIT & COMPLIANCE

UNIVERSAL, OPEN-SOURCE OSQUERY AGENT

Overview: Uptycs Security Analytics Platform

With Uptycs, gain a consolidated view for monitoring and securing your cloud, on-premises, or hybrid infrastructure by moving from several point solutions to a single, unified view of your security analytics. By pairing the single universal agent, osquery, with a scalable security analytics platform, Uptycs enables a unified view for:

Fleet Visibility

Intrusion Detection

Vulnerability Monitoring

Audit & Compliance

Uptycs collects, aggregates and analyzes your endpoint (workstation, workload, container, virtual machine, or server) telemetry, making it available for live and historical query using SQL.

The Power of Osquery for Incident Investigation

Incident investigators and forensics analysts prefer osquery because it is:

- **Open source** – you'll know exactly what your endpoint agent is doing
- **Cross platform** – can be used in heterogeneous environments including macOS, Linux, containers, and Windows
- **Comprehensive** – osquery exposes 200+ system tables including kernels loaded, processes running, open sockets, user logins, ports, network connections, etc.
- **Lightweight** – a read only agent, optimized for performance
- **Highly extendable** - osquery can be easily modified to add features/functionality

Uptycs: Osquery for Incident Investigation @Scale

Uptycs leverages the power of osquery and makes it fast and manageable to deploy at scale. In addition to the rich data set osquery offers, Uptycs for Incident Investigation includes:

- **Live Query:** ask questions across hundreds or thousands of endpoints in real-time
- **Historical Query:** go back in time and completely recreate the state of any compromised asset to identify what happened and how. Easily collect and share artifacts for further investigation and remediation.
- **Integrated Threat Intelligence**: be alerted when a known threat is active in your environment. Uptycs integrates over 40 threat intelligence feeds across 8 categories including Malware, not recommended website, phishing, dga, attack, coinminer, anonymizer, nrd.
- **Open API:** easily integrate with your existing security ecosystem like Splunk, Demisto, Slack, PagerDuty, etc.

WWW.UPTYCS.COM

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