THREATQUOTIENT™ POLYSWARM

THREATQ™ AND POLYSWARM

Technology Segment: Malware Enrichment & Analysis

The PolySwarm integration empowers users to seamlessly access context on a file hash, domain or IP address and gain insights into the malware behind it. Users may pivot on enrichments to research and discover related IOCs for a given malware campaign. This integration allows users to subscribe for a feed of emerging malware seen by PolySwarm where proactive detection and blocking is supported.

THREATQ BY THREATQUOTIENT™

ThreatQuotient's solutions make security operations more efficient and effective. The ThreatQ data-driven security operations platform is both open and extensible, supporting the integration of disparate security technologies into a single security infrastructure, automating actions and workflows so that tools and people can work in unison. Empowered with continuous prioritization based on their organization's unique risk profile, security teams can focus resources on the most relevant threats, and collaboratively investigate and respond with the aim of taking the right actions faster.

MALWARE INTELLIGENCE BY POLYSWARM

PolySwarm's unique multi-engine platform uses cutting-edge research engines by independent and corporate research teams who compete to give the most accurate analysis based on a cryptocurrency-driven marketplace, collated using machine-learning algorithms into a simple, single PolyScore. PolySwarm's platform provides SOC teams with easily-actionable malware feeds and enrichments, while providing intelligence teams with powerful and detailed malware analysis.

The Integration supports a variety of use cases such as:

- A complete malware research and analysis capability with actionable confidence scoring (PolyScore)
- Identify related actor infrastructure by pivoting on enrichments for attribution assessments

INTEGRATION HIGHLIGHTS

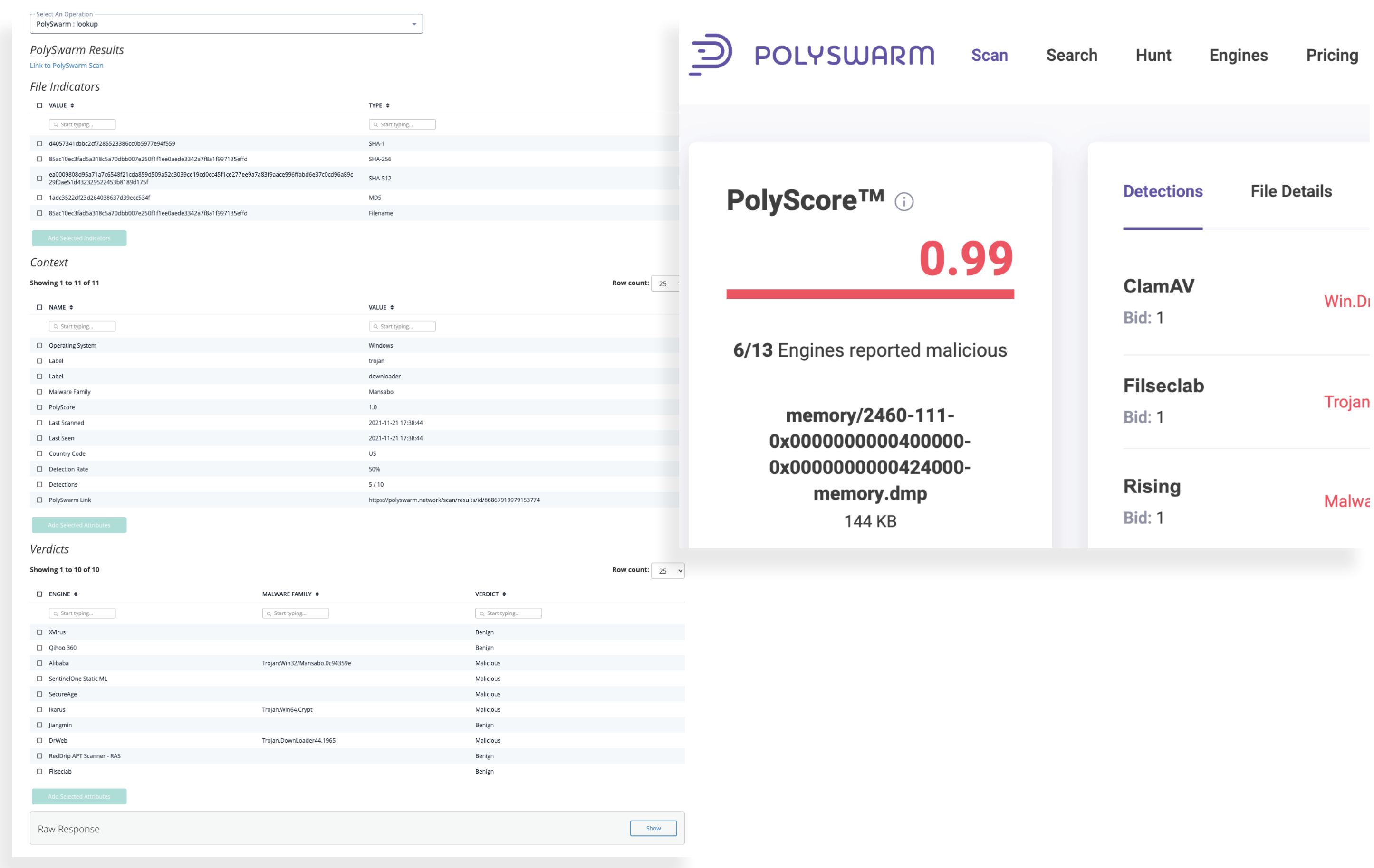
Simple right-click insights into any malware file hash or malware infrastructure

Access to a global multi-engine database for context on malware file hashes

Leverage a feed of first-seen malware variants for automated detection and blocking

High-speed sandboxing analysis of new suspicious files through niche detection engines

- Implement and enhance cross-functional security workflows with SOC automation and orchestration
- Conduct XDR Hunting using emerging ransomware TTP's and malicious code from the underground



Select An Operation: PolySwarm : lookup

PolySwarm Results

Link to PolySwarm Scan

File Indicators

☐	VALUE	TYPE
☐	d4057341cbbc2cf7285523386cc0b5977e94f559	SHA-1
☐	85ac10ec3fad5a318c5a70dbb007e250f1f1ee0aede3342a7f8a1f997135effd	SHA-256
☐	ea0009808d95a71a7c6548f21cda859d509a52c3039ce19cd0cc45f1ce277ee9a7a83f9aace996ffabd6e37c0cd96a89c29f0ae51d432329522453b8189d175f	SHA-512
☐	1adc3522df23d264038637d39ecc534f	MD5
☐	85ac10ec3fad5a318c5a70dbb007e250f1f1ee0aede3342a7f8a1f997135effd	Filename

Context

Showing 1 to 11 of 11 Row count: 25

☐	NAME	VALUE
☐	Operating System	Windows
☐	Label	trojan
☐	Label	downloader
☐	Malware Family	Mansabo
☐	PolyScore	1.0
☐	Last Scanned	2021-11-21 17:38:44
☐	Last Seen	2021-11-21 17:38:44
☐	Country Code	US
☐	Detection Rate	50%
☐	Detections	5 / 10
☐	PolySwarm Link	https://polyswarm.network/scan/results/id/86867919979153774

Verdicts

Showing 1 to 10 of 10 Row count: 25

☐	ENGINE	MALWARE FAMILY	VERDICT
☐	XVirus		Benign
☐	Qihoo 360		Benign
☐	Alibaba	Trojan:Win32/Mansabo.0c94359e	Malicious
☐	SentinelOne Static ML		Malicious
☐	SecureAge		Malicious
☐	Ikarus	Trojan.Win64.Crypt	Malicious
☐	Jiangmin		Benign
☐	DrWeb	Trojan.DownLoader44.1965	Malicious
☐	RedDrip APT Scanner - RAS		Benign
☐	Filseclab		Benign

PolySwarm™ PolyScore™ 0.99

6/13 Engines reported malicious

memory/2460-111-0x0000000000400000-0x0000000000424000-memory.dmp
144 KB

ClamAV Bid: 1	Win.Di
Filseclab Bid: 1	Trojan
Rising Bid: 1	Malwa

ABOUT THREATQUOTIENT™

ThreatQuotient improves security operations by fusing together disparate data sources, tools and teams to accelerate threat detection and response. ThreatQuotient's data-driven security operations platform helps teams prioritize, automate and collaborate on security incidents; enables more focused decision making; and maximizes limited resources by integrating

existing processes and technologies into a unified workspace. The result is reduced noise, clear priority threats, and the ability to automate processes with high fidelity data. ThreatQuotient's industry leading data management, orchestration and automation capabilities support multiple use cases including incident response, threat hunting, spear phishing, alert triage, vulnerability prioritization and threat intelligence management. ThreatQuotient is headquartered in Northern Virginia with international operations based out of Europe and APAC. For more information, visit www.threatquotient.com.

For more information, visit: www.threatquotient.com.

ABOUT POLYSWARM

PolySwarm is a launchpad for new technologies and innovative threat detection methods that compete to protect you against malware in real-time. We bring them together to help you better detect and respond to emerging threats, the ones that are more likely to go undetected by existing solutions. We are powered by a network that combines the wide coverage from commercial and specialized detection engines into a marketplace. PolySwarm detects threats earlier as these specialized engines are niche, research driven and often authored by independent, well known researchers and security teams, developing cutting-edge threat detection methods. We're driven to improve the threat intelligence landscape for ourselves, our clients and the industry at large. By providing robust incentives that align participants' interest with continued innovation, PolySwarm will break the mold of today's iterative threat intelligence offerings.

*For more information, please visit https://polyswarm.io/ or try PolySwarm free at https://polyswarm.network/