POLYSWARM

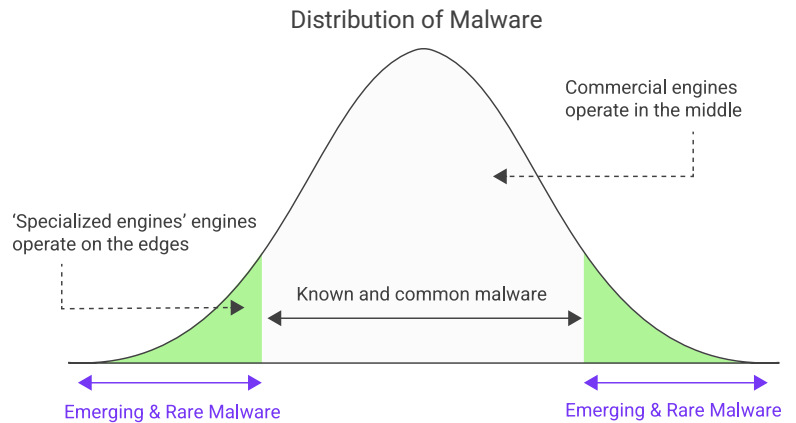## Early Detection for Unrivaled Protection:

Malware Intelligence Powered by the Hive

Staying ahead of emerging malware threats is the best way to protect your business. Yet the increasing magnitude and sophistication of malware attacks is an ongoing challenge. By tapping into PolySwarm's next-generation malware intelligence marketplace, you get better insight faster, so you can cut through extraneous, inaccurate data to detect, analyze, and respond to the most critical threats before they make an impact.

PolySwarm's first-of-its-kind market-place focuses on democratizing malware intelligence by using a blockchain backend to compensate both the researcher-based malware engines and ongoing sources of new malware samples. The result of this compensation model is that it enables you to prioritize, focus, and scale your cybersecurity efforts with unprecedented speed and accuracy.

- Early detection of threats
- Higher Accuracy
- SOC automation
- Unique samples

Catching the Threats That Others Miss

With a robust and growing network of threat detection engines, PolySwarm offers wide coverage against common threats. However, the real power comes from its specialized engines, with the ability to detect threats earlier and catch those emerging and rare threats that other engines miss entirely.

Distribution of Malware

Commercial engines operate in the middle

'Specialized engines' engines operate on the edges

Known and common malware

Emerging & Rare Malware

Emerging & Rare Malware

Rewarding Expert Insight to Improve Accuracy

PolySwarm is democratizing malware intelligence to elicit better intelligence by reducing the signal-to-noise ratio and eliminating false positives. Leveraging the power of the blockchain, we reward a global community of researchers for their early detection and expert insight via our native Nectar (NCT) token.

Contextual Threat Scoring to Enable SOC Automation

PolyScore is a threat scoring algorithm that provides the probability that a given file contains malware. It weights engines' determinations based on previous performance, resolving similar problems, confidence levels, and other indicators to produce a single, reliable score so you can:

- Make faster, more accurate decisions
- Reduce incident response escalations
- Save MDR time and money

PolyScore™   **0.88**

2/6 Engines reported malicious
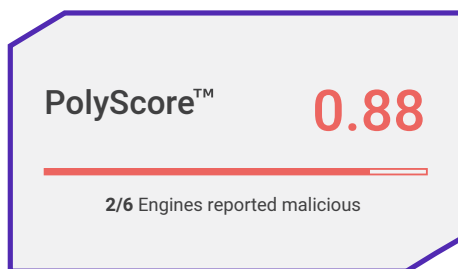
ADDITIONAL FEATURES

- Custom, geotargeted PolyFeeds
- Flexible metadata searches
- Unlimited YARA rules
- Private communities for enhanced security
- Relationship-first (support and service)

USE CASES

- Investigation & incident response
- Threat hunting & scoring
- Malware feeds
- Data enrichment
- SOC & security automation

INTEGRATIONS

PolySwarm provides seamless integration to a broad range of threat detections technologies

Technologies
- XDR
- SIEM
- SOAR
- TIP

Over 50 metadata tags per sample
- Malware family names
- Traditional hashes (SHA-1, MD5, etc.)
- Fuzzy hashes (TLSH, SSDEEP, etc.)
- Command & Control Infrastructure (IP, Domain, URL, etc.)

ANOMALI™   splunk> phantom   CYBER TRIAGE   CORTEX XSOAR BY PALO ALTO NETWORKS

CYWARE   ThreatConnect   Silobreaker   THREATQUOTIENT

LEARN MORE at PolySwarm.io

TRY OUR PRODUCT at PolySwarm.Network

@PolySwarm   Linkedin.com/company/polyswarm