ANOMALI® POLYSWARM

THREATS COME FROM ALL ANGLES, YOUR PROTECTION SHOULD TOO

A launchpad for new technologies and innovative threat detection methods

ANOMALI AND POLYSWARM JOINT SOLUTION FEATURES:

- Data Enrichment: File and URL enrichment provided by a crowdsourced network of cutting edge, anti-malware solutions.
- Performance-based compensation to the researcher community.
- Early detection of threats: driven by highly specialized, research-driven engines, focused on emerging malware and 0-day threats.
- Threat scoring: A single, authoritative score that provides the probability a file contains malware.

IMMEDIATE TIME-TO-VALUE

- Actionable Automation: Enables SOC and CTI teams to make decisions quickly at scale with unprecedented accuracy.
- 25% of PolySwarm samples are not yet in VirusTotal.
- Expanded coverage against emerging threats, the ones more likely to be missed by existing solutions.
- Simple, easy-to-use integration.

CROWDSOURCED, RESEARCHER-DRIVEN MALWARE INTELLIGENCE

As the volume and complexity of cyber threats increase, CTI & SOC teams have to deal with an ever-growing queue of alerts, requiring them to contextualize and prioritize incidents at scale. The PolySwarm-Anomali integration allows users to obtain file and URL reputation services with a single click, in real-time, from a network of independent malware detection engines. PolySwarm summarizes crowdsourced verdicts into a single, authoritative number called PolyScore™, providing the probability a given file contains malware.

SPECIALIZED SOLUTIONS

Access to focused researcher-driven engines to detect critical threats

UNIQUE ENGINES & SAMPLES

Solutions and samples that can't be found in other multiscanners

CONTEXTUAL THREAT SCORING

PolyScore™ filters the noise and amplifies the signal by weighting engine's opinions based on performance

SOC AUTOMATION:

CHALLENGE:

A large, fast-growing MSSP is experiencing an unprecedented increase in the number of alerts they are managing on their clients infrastructure due to COVID-19. They need a scalable way to determine whether incoming files are malicious or benign to compliment their existing solutions. Their existing multiscanners solution has a hard time concluding on file maliciousness, since engine's verdicts are often conflicting, requiring additional intuition-based work from analysts and SOC team members, thereby impacting the profitability and productivity of the organization.

SOLUTION:

SOC integration via Anomali ThreatStream, along with PolySwarm's malware intelligence. Using a single, authoritative number computed from recent crowdsourced verdicts, engine strengths, confidence levels, and other relevant threat indicators, all sourced from millions of daily assertions in the PolySwarm network.

CUSTOMER BENEFIT:

PolyScore enables SOC automation and allows analysts and CTI teams to make quick defensive decisions at scale, with unprecedented accuracy.

DATA ENRICHMENT/ THREAT HUNTING

CHALLENGE:

An Anomali customer has uncovered a suspicious SHA256 hash from an internal EDR protected endpoint and wants to know more about this threat. The customer's EDR vendor and existing malware enrichment solutions does not have any additional information on the suspicious hash. They want a second opinion of the hash and if malicious they want such details as the malware name, C2 information and the ability to pivot to other similar hashes. These details will enable their SOC and IR teams to proactively block or locate other potential infections.

SOLUTION:

Anomali ThreatStream, through PolySwarm's integration, provides in-depth enrichment capabilities such as listing most of the major hashes including MD5, SHA1 and the fuzzy hashes of TLSH and SSDEEP. Scan search results over time allow SOC teams to understand how detections have changed overtime for additional context on the threat. Via the graph pivoting functionality, PolySwarm's integration allows for the enrichment of the sample with domain and IP information found in the malware by static analysis and other malware that contain the same domain information.

CUSTOMER BENEFIT:

The ability to quickly get a second opinion from cutting edge researcher driven engines and use this metadata within the Anomali platform to identify additional important details and information. This process dramatically increases both the speed and productivity of the respective SOC, CTI and IR teams and enables the organization to effectively safeguard the enterprise.

info@anomali.com | www.anomali.com
808 Winslow St, Redwood City, CA 94063 USA
1-844-4-THREATS

ANOMALI®