Anomali Sandbox

Operationalize Detection and Respond to Evasive Threats Natively Inside Anomali ThreatStream

To do any security research or dive into malware analysis, you need an isolated testing environment that enables users to run programs or open files without affecting the application, system, or platform they run. Cybersecurity professionals use sandboxes to test potentially malicious software and analyze code without the risk of destroying a production environment.

Anomali Sandbox utilizes multiple threat analysis technologies to perform a deep analysis of evasive and unknown threats to detect unknown, zero-day, and evasive malware and enrich the results with threat intelligence.

This results in actionable compromise indicators (IOCs), enabling your security team to understand sophisticated malware attacks and strengthen defenses.

KEY HIGHLIGHTS:

- Automated phishing email detonation
- Import IOCs automatically from Sandbox into ThreatStream
- Scan IOCs for scoring and False Positive removal
- Automatically:
  - Initiate Investigations
  - Generate Threat Bulletins
  - Push IOCs to security controls and Anomali Match
- Optionally share detonation results with the Anomali community.

KEY CAPABILITIES

Anomali's detection capability combines:

- Deep analysis of suspected malware
- Deep analysis of URLs to detect phishing
- Cross-platform analysis — Microsoft Windows, Mac OS, Android, and Ubuntu
- Detailed detonation reports:
  - Screenshots
  - PCAP
  - Dropped files
  - Signatures
  - Network analysis
  - Behavior analysis

Key Differentiators

COLLECT

Automatically collect new internal threat intelligence from detonations of files and URLs targeting your organization.

- Harvest malicious IOCs discovered during detonation, curate them with Macula, and automatically feed these into your SIEM for threat hunting
- Ingest and analyze suspected malware files and generate detailed reports of the findings.
- Gather malicious IOCs discovered during detonation, curate them with Macula, and feed these into security controls for blocking/detection

ENRICH

Enrich your understanding by associating newly discovered IOCs with existing intel

- Understand relevant threats facing the organization so security teams can take action
- Gain context between generated IOCs, reports and sandbox submissions across multiple detonations is preserved for future analytical value
- Broad OS and file type support for detonations support different use cases
- Collaborate on and sharing reports help encourage more comprehensive communication and team alignment on relevant security threats

OPERATIONALIZE

Fully operationalize intelligence by automatically curating and disseminating IOCs from detonations.

- Automate workflows to improve analysis and response time
- Merge output artifacts into Anomali Investigations facilitate deeper analysis and understanding of threats
- Unify intelligence management to help security teams avoid disruptions and improve focus and efficiency

Key Use Cases

Malware Analysis

Adversaries are employing sophisticated techniques to avoid the detection of malicious files and email attachments, including ransomware, trojans, and worms. ThreatStream's integrated sandbox.

Threat Response

Sandbox malware analysis can expose behavior and IOCs that threat hunters can use to find similar activity, such as access to a particular network connection, port, or domain.

Automation

Sandbox results are merged with the security team's existing tagging taxonomy and existing Intelligence Initiatives/Intel Requirements, and they become part of the team's automated Rules to increase actionability, speed analysis, and improve response.

ANOMALI