ANOMALI SANDBOX

Operationalize Detection and Respond to Evasive Threats Natively Inside Anomali ThreatStream

DETECT UNKNOWN THREATS

Anomali Sandbox performs deep analysis of evasive and unknown threats, enriches the results with threat intelligence, and delivers actionable indicators of compromise (IOCs), enabling your security team to better understand sophisticated malware attacks and strengthen defenses. Multiple threat analysis technologies combine to detect unknown, zero-day and evasive malware.

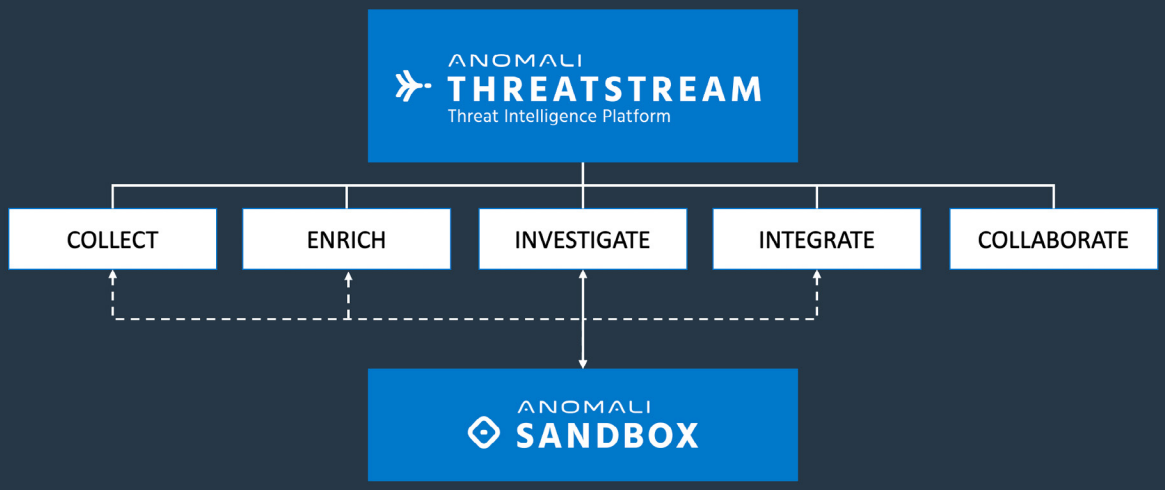
RESPOND FASTER

Save time and make all security teams more effective with easy-to-understand reports, actionable IOCs and seamless integration. With your Anomali Sandbox a natively integrated component of your ThreatStream threat intelligence platform, insights are automatically included where you need them and where everybody can access them, with no wasted effort or risk of compartmentalization of the data with a specific team, and included findings immediately accompany any established workflow.

GET COMPLETE THREAT VISIBILITY

Uncover the full attack lifecycle with in-depth insight into all file, network, memory and process activity, and inform all stages of the ThreatStream security lifecycle with sandboxing insights.

- Collect new internal threat intelligence from detonations of files and URLs targeting your organization
- Enrich your understanding by associating newly discovered IOCs with existing intel
- Augment your investigations by exploring the attack infrastructure of malicious files and URLs
- Fully operationalize the acquired intelligence by automatically curating and disseminating IOCs from detonations to your security controls



ANOMALI SANDBOX BENEFITS

TURBOCHARGE YOUR THREATSTREAM INSTANCE

The embedded sandboxing capability in ThreatStream significantly enhances detection and investigations along several dimensions, including:

- Automated phishing email detonation
- Import IOCs automatically from Sandbox into ThreatStream
- Macula scan IOCs for scoring and False Positive removal
- Automatically initiate Investigations
- Automatically generate Threat Bulletins
- Automatically push IOCs to security controls
- Automatically push IOCs to Anomali Match
- Optionally share detonation results with the Anomali community

SANDBOX CAPABILITIES

Anomali's detection capability combines

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

USE CASES

MALWARE ANALYSIS

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

- Allows you to automatically ingest and analyze suspected malware files and generate detailed reports of the findings.
- Can automatically harvest malicious IOCs discovered during detonation, curate them with Macula, and feed these into security controls for blocking/detection

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.

- ThreatStream can automatically harvest malicious IOCs discovered during detonation, curate them with Macula, and automatically feed these into your SIEM for threat hunting
- Match can automatically use sandbox detonation data to retrospectively search historic firewall and proxy logs or other SIEM data to find threats that have penetrated the network

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

ANOMALI®