ANOMALI®

FARSIGHT SECURITY

Farsight Security® DNS Intelligence

Delivers Unmatched Visibility to Improve Threat Detection and Proactively Defend Against Cyberattacks

ANOMALI AND FARSIGHT JOINT SOLUTION FEATURES:

- Farsight Security offers real-time Passive DNS data as part of the Anomali APP Store, a marketplace for premium threat intelligence.
- When Anomali users identify a potential malicious IP address or domain name, they can—with a click of a button—purchase access to Farsight's Passive DNS data to quickly investigate these digital artifacts to advance their investigations.
  - Access real-time and historical Passive DNS data from within the Anomali platform
  - Enhance, enrich, and contextualize threat intelligence data to concentrate investigations

IMMEDIATE TIME-TO-VALUE

- Discover associations among threat actors and track and block their activity.
- Perform fact-based risk assessment of domain names and IP addresses.
- Uncover all domains using the same name server infrastructure used by a "known bad" domain.
- Reveal the IPs an adversary is using to conceal malicious activity and avoid takedowns.

ACCELERATE INCIDENT RESEARCH AND POST BREACH ANALYSIS

Anomali and Farsight Security recognize the value that threat intelligence sharing and collaboration plays in increasing the speed and accuracy of threat investigations.

CRITICAL INTELLIGENCE

Contextualize, correlate and transform all of your threat and network data to increase the value of your security operations.

FLEXIBLE DEPLOYMENTS

Fast, scalable implementation on-premises and in the cloud.

IMMEDIATE RESULTS

Improve the speed, accuracy and global view of your digital investigations for faster risk mitigation and prevention.

CASE STUDY:
A NEW THREAT FROM AN OLD ENEMY

CHALLENGE:

Incident Response teams discover new threat intelligence only to find that the threat has been around for months. The team needs to 'turn back the clock' and see if anyone in their organization previously visited the identified and/or associated sites and potentially compromised their network.

SOLUTION:

By enriching Anomali data with Farsight Security's DNSDB, Incident Responders can use historical DNSDB records to gain context and learn the footprint of the attacker's DNS infrastructure. This will allow Responders to observe the attacker's use of DNS to conceal their identity and uncover how employees have engaged with those sites.

CUSTOMER BENEFIT:

Access to historical DNS enriches current threat data to quickly understand and respond to threats and security compromises.

CASE STUDY:
PROACTIVELY DETECT AND ISOLATE ADVANCED THREATS

CHALLENGE:

Threat Hunters map out the miscreant's infrastructure in preparation for take down or discovering advanced threats.

SOLUTION:

Historical DNS allows Hunters to map out the attacker's infrastructure. By enriching Anomali data with Farsight Security's DNSDB, Threat Hunters can learn the historical DNS mappings of the IP addresses, name servers, and mail servers associated with the attacker's organization.

CUSTOMER BENEFIT:

Tie related infrastructures to the attacker's organization and see other related infrastructures to proactively detect and isolate advanced threats.

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

ANOMALI®