ANOMALI® DOMAINTOOLS

IDENTIFY, PRIORITIZE, AND RESPOND TO THREATS

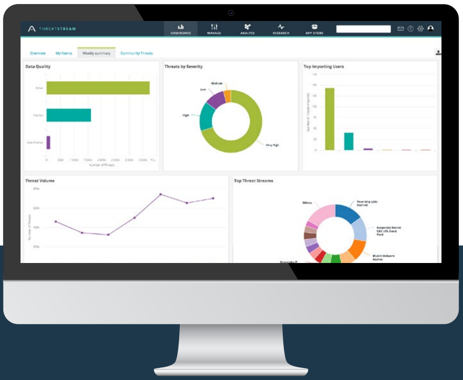
Context-based enrichment for domain names, IP addresses, hostnames, and SSL certificate hashes

DOMAINTOOLS AND ANOMALI JOINT SOLUTION FEATURES:

- The DomainTools Iris APP for the Anomali Threat Platform delivers the ability to contextualize, prioritize and mitigate threats.
- Conversion of threat data into actionable cyber threat intelligence that can be used for threat hunting, forensics, incident response, phishing detection, and brand and fraud protection.
- Ability to proactively identify and understand threats, prioritize them, and determine effective countermeasures.
- Automated threat identification, correlation and response.

IMMEDIATE TIME-TO-VALUE

- Ability to instantly access DomainTools' comprehensive data on domain name, DNS and related data.
- Further automation of proactive cyber threat operations.
- Inform risk assessments, help profile attackers, guide online fraud investigations, and map cyber activity to attacker infrastructure.



TURN DATA INTO INTELLIGENCE THAT STOPS THREATS

There is no way to avoid coming into contact with the various types of threats operating in the wild but there are ways to identify and block them before they have a chance to infiltrate your networks. DomainTools Cyber Threat Intelligence solutions enable organizations to assess the threat risk of domains and IP addresses, investigate the organization behind a domain, and map the online networks of criminal organizations in order to stop future attacks. Anomali delivers the most advanced and comprehensive platform for threat detection, investigation and response. Joint customers are able to increase their visibility over malicious actors while further speeding and simplifying their ability to mitigate the most serious threats.

CRITICAL INTELLIGENCE

Help analysts turn threat data into threat intelligence

FLEXIBLE DEPLOYMENTS

Fast, scalable implementation on-premises and in the cloud

IMMEDIATE RESULTS

Immediately start identifying malicious domains and IP addresses

REDUCING MTTR

CHALLENGE:

With countless threat indicators available through hundreds of different sources and feeds, identifying which are the most severe and prioritizing remediation is a challenging task.

SOLUTION:

By integrating DomainTools threat data into the Anomali Platform, joint customers can correlate the information with additional data sets and then automatically export it into existing security and ticketing systems.

CUSTOMER BENEFIT:

Automation capabilities allow security teams to decrease the amount of time needed to remediate the most serious threats.

CONTEXTUAL ALERTING

CHALLENGE:

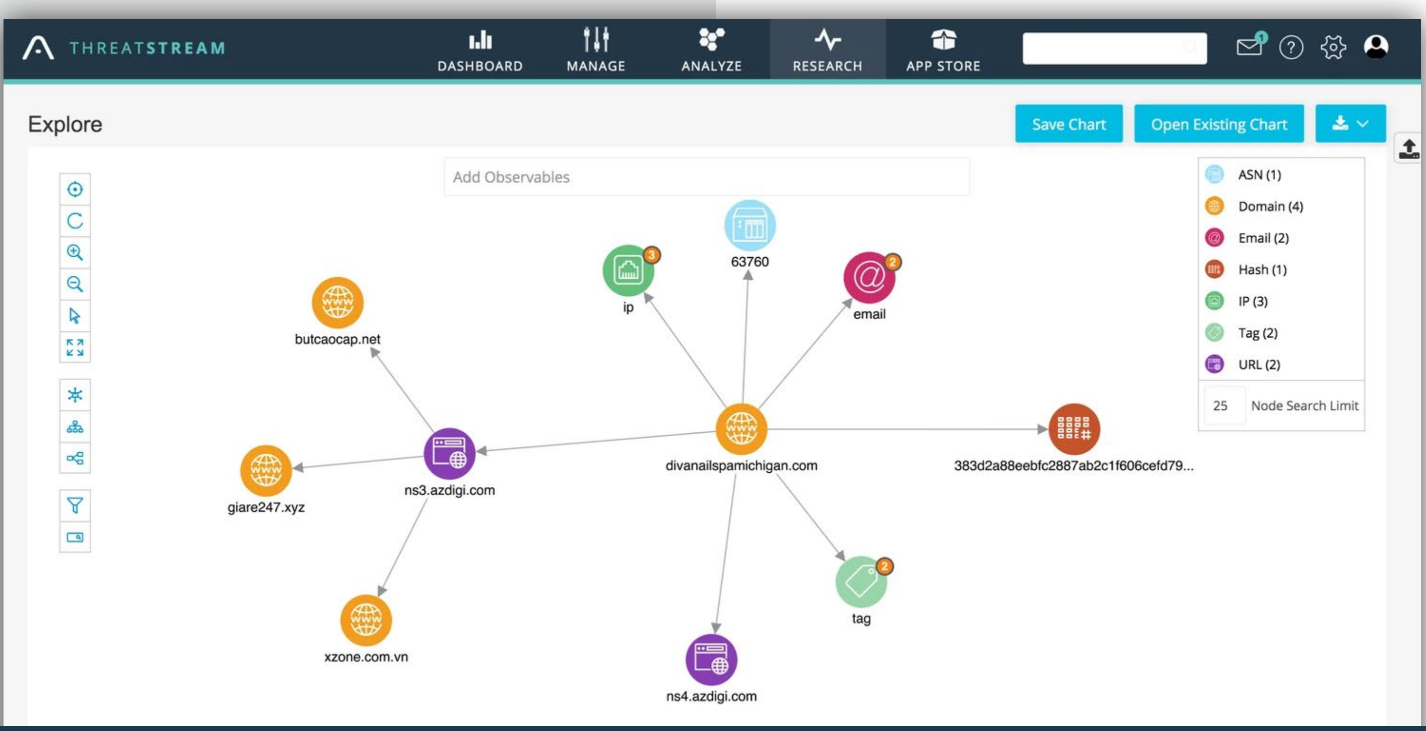
Determining the severity and validity of alerts within the SOC and CSIRT can be a cumbersome task that can evolve into an inefficient use of talented resources.

SOLUTION:

By integrating DomainTools threat data into the Anomali Threat Platform, joint customers can map connected infrastructure and proactively assess malicious infrastructure to give organizations the confidence in determining severity and validity of alerts.

CUSTOMER BENEFIT:

Providing the proper alert context allows the SOC and CSIRT to provide confidence, priority, and next steps based on adversarial TTPs.



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

ANOMALI®