ANOMALI

ANOMALI TARGETED THREAT MONITORING

OVERVIEW

Organizations face constant threats from sophisticated threat actors targeting their brand to inflict damage, making it harder for security teams to keep up and defend their brand from these attacks.

Unfortunately, many of the current tools take a reactive approach in identifying threats, leaving organizations to rely too much on their perimeter defenses to detect or stop attacks.

Anomali Targeted Threat Monitoring helps identify and defend against targeted attacks by continuously monitoring the threat landscape to alert on relevant threats and enable you to act quickly.

Anomali Targeted Threat Monitoring enables security teams to:

- Detect attacker infrastructure before it is operationalized
- Disrupt an attacker's ability to create an outbound channel
- Prevent harvesting and exfiltration of data
- Take action to minimize risk and potential damage

KEY BENEFITS

- Defend your brand against targeted attacks and brand abuse to maintain loyalty and trust with your customers
- Continuously monitor domains for cybersquatters and domain hijacking to prevent phishing and malware attacks
- Increase visibility into external threats to prevent sensitive data leaks and help mitigate risk before damage can occur.
- Receive clear and detailed alerts on suspected threats with recommendations on how to remediate the threat quickly and effectively.

KEY FEATURES

Anomali Targeted Threat Monitoring gives analysts the automated threat intelligence they need to respond to attacks quickly and effectively. Identified domains and compromised credentials are imported into ThreatStream, providing security teams with visibility and enriched intelligence to fully protect their assets, as well as increased efficiencies by operationalizing this targeted intelligence within ThreatStream.

ATTM

- Similar Domain Registration (phishing/brand abuse)
- Potential phishing URLs
- Suspicious SSL certificate registration
- Compromised credentials
- Domain Hijacking
- Leaked Credentials Monitoring

ATTM+

- Exposed Subdomain
- Domain expiration
- Email Vulnerability
- Leaked sensitive documents on hybrid analysis & joe sandbox
- Leaked code on github/gitlab
- Rogue Apps
- Pastebin brand mentions
- Employee doxing incidents
- Trademark application filing

KEY USE CASES

PHISHING DETECTION
Track key phishing indicators like registered domains, MX record changes, and DNS reputation, cybersecurity teams to proactively identify and cut off phishing attacks at their source.

BRAND PROTECTION
Scan external sources for fraudulent attacker activity targeting your brand, as well as monitor domains, IP addresses, mobile apps, and social media pages to identify imposters.

FRAUD PROTECTION
Identify fraud schemes using phishing sites, leaked credentials, and Social Security numbers, among others, to stop fraud before it happens.

ROGUE APP IDENTIFICATION
Discover rogue, malicious apps impersonating your brand that security teams typically do not search or monitor.

LEAKED CREDENTIALS MONITORING
Monitor for stolen credentials, passwords, and any other sensitive data that could give cybercriminals access to corporate systems.

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