banyax

M/ETI

Managed External Threat Intelligence

Powered by Cyberint

SECURE YOUR ORGANIZATION BEYOND YOUR CYBER DEFENSE PERIMETER.

Focuses on uncovering hidden risks or external factors like third-party breaches, data dumps, domain abuse, and executive impersonations across the Deep and Dark Web, enabling prompt actions to protect your sensitive data.

ATTACK SURFACE MONITORING

Identifying and assessing all potential entry points in an organization's systems that could be exploited by attackers, aiming to reduce vulnerabilities and improve security.

THREAT INTELLIGENCE

Gathering and analyzing information about potential and active security threats to help organizations anticipate, prevent, and respond to cyberattacks.

EXTERNAL THREAT DETECTION

Identifying and monitoring security threats from outside an organization to prevent or mitigate potential damage.

banyax Quest

Banyax Quest™ Service Delivery Platform

Transparency and communication are critical factors to respond quickly to external cyber threats. Banyax Quest™ is a collaborative platform where your team can see exactly what our analysts see and interact with them in real time to contain threats. Banyax Quest™ provides answers to what, who, why, and where for every threat. Enabling you to threats and how to contain them.

Visibility is the name of the game in Cybersecurity

- Threat Intelligence Platform.

24×7×365 Real-Time Cyber Defense Services
Monterrey, México | CDMX, México | Dallas, Texas
info@banyax.com
www.banyax.com

banyax

OFFERINGS

banyax

Proactive Brand and Image Protection
Searching, monitoring and early detection of brand and image presence on the internet, in order to detect unauthorized use, fake websites or misleading profiles that may impersonate your brand or image for fraudulent purposes.

Brand Protection scanning in Covert Forums and Platforms to Detect Conversations and Brand Abuse
Searching a wide variety of online forums, social networks and other websites, identifying conversations, comments, posts and reviews where the brand is mentioned, or the organization's image is alluded to. Analyzing these conversations to identify potential brand abuse, misrepresentation, defamation or impersonation that may mislead employees or our customers/consumers.

Key Executive Identity Theft Protection
Searching social networks, forums, websites and the Deep web for any mention of the executive's name, position and brand, to identify fictional profiles with the intent to impersonate, defraud or damage the reputation of the executive or the organization by spreading false or defamatory information.

Detection and Protection Against Domain Abuse and Spoofing Attempts (fake websites)
Evaluation and monitoring of the web in search of new domains containing the brand name, its variations or keywords that facilitate its association, with the intent to impersonate and defraud (theft of personal or financial information, unfair sale or damage to the reputation of the brand).

Notifications & Dashboards
Centralized dashboard and real-time email notifications via Banyax Quest, allowing for quick access to alerts and incident analysis, ensuring no threat goes unnoticed.

Takedown of Malicious Content
We manage the entire process to protect against digital threats by removing malicious content such as phishing sites, fake social media accounts and fraudulent applications with advanced tools and a team of cybersecurity experts.

Exposed Credential Notification and Monitoring on the Dark Web
Searching social networks, forums, websites and the Deep Web for any mentions where stolen data is traded, to find stolen credentials (email and password combinations) of employees or customers related to the organization or brand.

Identifying Exposed Application Source Code through a Unique Identifier
Monitoring unique code identifiers and APIs for detection of exposed source code on the web to prevent spoofing with the intent to defraud or deceive employees or consumers.

Identification of Infected Computers through the Search for Infostealer Logs and Other Types of Malwares
Monitoring and specialized search for suspicious activity in various threat intelligence feeds and proactive scanning of events generated by Infostealers and other types of malwares, indicators of compromise (IoCs) to identify Botnet activities, providing early defense against potential network threats and cyber-attacks.

Identification of Reconnaissance Tools, Vulnerability Scanners and/or Ransomware Seeking to Attack the Organization
Monitoring of your organization's exposed attack surface to identify the tools of attackers and/or third parties attempting to cause an effect to your systems through vulnerability scans, technology reconnaissance and malware infections.

OFFERINGS

banyax

Intelligence and Recommendations

Monthly cyber intelligence reports detailing identified vulnerabilities, threat actors and prevalent tactics, techniques and procedures (TTPs) on the dark web. This information allows us to anticipate threats and take proactive measures to protect your organization.

Identification of Erroneous Configurations of Domains that Could Lead to Incidents

Proactive monitoring of the external attack surface related to you organization's public scope, to detect deviations in configurations by comparing them with known CVE databases and recommending remediation actions to strengthen the cybersecurity posture.

Email Server Blacklist Identification

Periodic queries of blacklisted mail server databases for matches between the IP addresses or domains of your organization's mail servers to uncover potential system compromises, such as spamming from compromised servers.

Identification of Security Concerns Related to Web Interfaces for Employees and/or Exposed Customers

Monitoring the web for access interfaces that match the domain, IP or brand of your organization within scope, which have vulnerable access forms and/or exposed to cybersecurity issues.

External Cloud Storage Monitoring

Proactive searching for data exfiltration related to cloud storage external to the organization's primary domain.

Identification of Vulnerabilities in Ports and Services of the Monitored Domain

Proactive searching for existing vulnerabilities across ports and services of monitored domains, comparing them with known vulnerabilities commonly exploited by threat actors. Identification and analyzing of exposed technologies, their severity level according to the risk they pose to your systems, sharing recommendations to strengthen your cybersecurity posture.