Brandsek Continous Scan

BrandSek is dedicated to ensuring robust security through continuous scanning. This process is designed to proactively identify vulnerabilities and potential threats across all public-facing assets. Scans are performed continuously—at least once per day, with the flexibility to run multiple scans throughout the day—to provide real-time insights and rapid remediation of issues.

Asset Input & Discovery

The scanning process primarily starts with the root-level domain provided as input. From this input, our system automatically discovers the associated IP addresses and subdomains, ensuring comprehensive coverage of all public-facing assets. Additionally, the functionality allows for manual input—enabling users to add specific subdomains or IP addresses as needed. This dual approach guarantees that both primary and auxiliary assets are accurately identified and monitored.

Active Scanning :

Active scanning involves direct interaction with systems and assets to identify vulnerabilities. Active scans are strictly limited to publicly accessible assets only; no internal environment scanning is conducted, ensuring that sensitive internal systems remain undisturbed.

Components of Active Scanning

- **Vulnerability Assessment (VA) Scan:**
  Conducts detailed evaluations of public assets to identify potential security weaknesses.
- **SSL Scan:**
  Assesses the configuration and integrity of SSL/TLS certificates on public servers to ensure secure communications.
- **Email Security Scan:**
  Reviews email system configurations and security measures to detect misconfigurations or vulnerabilities.
- **Dangling Subdomain Detection:**
  Detects orphaned or misconfigured subdomains that could be exploited by attackers.

Frequency

- **Continuous Scanning:**
  Active scans are executed continuously—at least once per day, with the option to run multiple scans as needed to ensure timely detection and remediation of vulnerabilities.

Passive Scanning

Passive scanning involves monitoring external sources and publicly available data without directly interacting with the assets. This method offers insights into potential external threats and exposures that might affect BrandSek.

Components of Passive Scanning

- **Internet-Wide Vulnerability Assessment:**
  Utilizes large-scale external scanning services to identify vulnerabilities impacting BrandSek’s assets.
- **IP Discovery:**
  Continuously identifies and maps active IP addresses associated with BrandSek, helping to maintain an accurate digital footprint.
- **Dark Web Credential Monitoring:**
  Monitors dark web sources for any leaked or exposed credentials that could compromise security.
- **Chatter and Telegram Monitoring:**
  Tracks public discussions on platforms like Telegram to identify emerging threats or targeted attacks.
- **Surface Web Scanning:**
  - **Source Code Repositories:** Searches for exposed or misconfigured repositories.
  - **Postman and SwaggerHub:** Reviews public API documentation and testing platforms for vulnerabilities.
  - **Pastebin:** Monitors for the leakage or dumping of sensitive data.
  - **Open Cloud Buckets:** Checks for unsecured cloud storage that might expose critical data.
  - **Personal Information Checks:** Scans for unauthorized exposure of personal data associated with the brand.
- **Brand Security Checks:**
  - **Impersonation Detection:** Monitors for fraudulent use of the BrandSek identity.
  - **Look-Alike Domain Identification:** Identifies domains that mimic BrandSek to preempt phishing attempts.
  - **Social Media Impersonation:** Detects fake social media profiles replicating the brand.
  - **Mobile App Impersonation:** Identifies counterfeit mobile applications that could mislead users.
  - **Brand Mention Tracking:** Continuously monitors online mentions to detect any misuse or negative sentiment surrounding the brand.

Frequency

- **Continuous Scanning:**
  Passive scans are performed continuously—at least once per day—with the capability to run more frequently to ensure that any external threats or exposures are promptly identified and addressed.

Revision #1
Created 16 March 2025 08:44:28 by Admin
Updated 16 March 2025 08:45:38 by Admin