OSINT ASSESSMENT

Contextual Security Solution's **Open Source Intelligence (OSINT) Assessment** is designed to uncover publicly available data related to the organization that could impact the security of their systems, applications or data. The OSINT Assessment includes three (3) key tasks; a Domain Review, a Third Party Breach Review and an Exposed Credentials Review.

With respect to the **Domain Review**, Contextual Security Solutions will conduct an audit of your existing domains to determine if any typos or variations have been registered (and/or are active) that could be used to perform typo-squatting, phishing, corporate espionage or URL hijacking. Examples of the variations to be assessed include, but are not limited to character omissions, character repeats, adjacent character swaps, adjacent character replacements, vowel swapping and bit flipping.

For the **Third Party Breach Review**, Contextual Security Solutions will attempt to harvest the organization's email accounts using a variety of OSINT tools to determine if any had been compromised or flagged as part of a third-party data breach in the last ninety (90) days and within the last year (365 Days).

As for the **Exposed Credentials Review,** Contextual Security Solutions will attempt to identify any accounts that have had their credentials disclosed publicly, or pasted, on known hacker sites.

BENEFITS

52% of Users

Employ the Same Password for Different Services

OSINT Assessments can assist organizations in identifying the registration and use of domains similar to their own. These domains are a primary vector in **phishing attacks**, which per the Verizon DBIR 2020 report (which includes a study of 2,907 breaches), resulted in **22% of the breaches observed**. Through the routine execution of OSINT Assessments, organizations can quickly identify and block access to malicious domains.

Also, per a 2018* study of roughly 28 million users and their 61 million passwords, a team of researchers found that roughly 52% utilized the same passwords (or very similar ones) for different services. This risk in this practice is obvious. If a user employs the same or a similar password with a third party service provider that has been breached, attackers with this information could target the organization. This threat is further compounded if that user has privileged access. It is also important to note that in 2020, roughly **20% of the breaches** studied in the Verizon DBIR were tied to **the use of stolen credentials**. Routine OSINT Assessments can help organizations monitor the status of their user accounts, especially when used outside of the organization.

OSINT ASSESSMENT COMPONENTS

Domain Review

Key activities of a **Domain Review** include, but are not limited to:

- Identification of recently registered domains that could be used in a **phishing** attack
- Identification of recently registered domains that could be used to perform **squatting**, **espionage** or **URL hijacking**.

Credentials Exposure Review

Key activities of a **Exposed Credentials Review** include, but are not limited to:

- Identification of harvested email accounts that have had their password **pasted** on any third party hacker sites.
- **Testing of disclosed username/ password combinations** against any remote access solutions in place

Third Party Breach Review

Key activities of a **Third Party Breach Review** include, but are not limited to:

- **Harvesting email accounts** from publicly available resources
- Identification of the harvested accounts that have been disclosed in a **third party breach**

Additional OSINT Activities

Additional activities performed as part of the **OSINT Assessment** include, but are not limited to the following:

- **Review the organizations public footprint** through publicly accessible databases (e.g. Shodan)
- Capture and review of the organizations public facing web pages to identify **misconfigurations / sensitive data disclosures**

* Panda Security July 22, 2018 "52% of users refuse their password" [https://www.pandasecurity.com/en/mediacenter/security/password-reuse/]