KnightLight by TruStack

Most users don't like to manage multiple passwords and tend to reuse the same passwords again and again. This means that there is a high percentage any compromised usernames and passwords could potentially be the same credentials for their corporate data, making this a natural starting point for any malicious attackers who have a desire to compromise a network.

What is KnightLight

TruStack provides a service which proactively monitors for stolen data that is available on the dark web and based on a company's email domain; for example; @trustack.co.uk.

This is a real-time monitoring service with daily and monthly summaries, so we can quickly advise customers of any new compromises found.

In addition to this monitoring, we can monitor up to 3 VIPs within each companies personal email addresses.

These can be C-level directors or key personnel who may be valuable targets for compromise. This will involve monitoring their personal email accounts (i.e. Gmail, Yahoo, Hotmail etc.) ensuring they know they are not compromised personally as well as commercially.

In the event of no new compromises being found in any month, the customer will receive a 'Cleanbill of health' email.

79% of CIO's are concerned that users might not follow security guidelines when working from home*

Flexible, Subscription Based Pricing

- Monthly subscription, per mail domain regardless of the number of users within a company.
- 3 VIP emails monitored with basic subscription - additional personal domains can be purchased

64% of IT Managers admit that the rapid transition to WFH may have caused security gaps*

Benefits of KnightLight

- Notification of compromised passwords so IT can ask users to change their passwords immediately.
- Identification of users using their corporate email address/passwords for public services such as betting sites, LinkedIn, Facebook etc. Companies should amend their security policies to demand users do not use corporate email addresses for these types of services.
- Most users don't use many different passwords so if LinkedIn is compromised, there is a good chance those credentials could provide network access to corporate systems.
- If a company's accounts are compromised a pen test won't show up any issues. A legitimate account with correct details is accessing services, this would look like authorised access.
- As cloud services extend ever wider, it is complex and costly to ensure end to end security, if you are compromised you need to know about it and remediate.

Amongsts mid-sized organisations, concern grew about credential theft from 53% to 80% during the pandemic*

What's Included?

- 24 x 7 scanning for compromises, daily notifications of any new compromises.
- 'Clean Bill of Health' email in months where no new compromised data is discovered.
- Indication of any Personally Identifiable Information (PII) also available on the dark web. This may include username, address, phone number, date of birth, full name, credit card number etc. We cannot show this information for privacy reasons, but we do highlight wherever it is found. Individuals can then take the matter up privately with their bank or credit rating agencies.
- Monitoring of personal email addresses for up to 3 key members of staff. These additional email addresses benefit from the same level of alerting as the company monitoring.

*2020 Cyber Threat Report - Netwrix