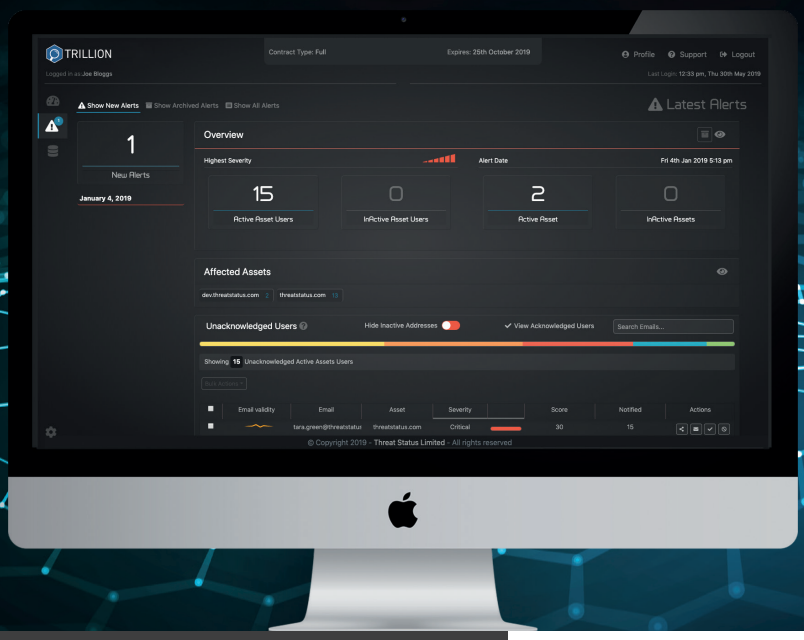
CROSSWORD CYBERSECURITY



ABOVE: TRILLION™

MANAGEMENT PORTAL

- Trillion™ constantly monitors the billions of account credentials passing through dark markets and criminal forums, looking for the few hidden accounts that might affect your organisation
- Intelligent risk engines identify which leaked usernames and passwords have the greatest potential to result in corporate damage
- Data filters and automatic live account detection makes data discovered by Trillion™ easy to navigate and validate, even for the largest organisations
- Trillion™ leverages the power of crowds by letting employees play an active role in verifying discovered data and securing your organisations
- End user interaction enables better engagement and educational awareness of security issues
- The management of business threats are perfectly balanced with the protection of user privacy. Built-in safe-guards secure the enterprise and your users simultaneously

Active Corporate Data Breach Credential Monitoring Platform

OVERVIEW

Usernames and passwords are frequently an organisation's primary line of defence when it comes to protecting systems and data. Occasionally additional layers of protection might be added such as 2FA (Two Factor Authentication), but this is rarely deployed across every high value application used by a business.

Attackers are aware of this too. They know that there will be systems in your organisation that don't have 2FA protection, either because it's too complex to deploy or its not even supported. The result is that most systems usually only require two pieces of information before allowing access to your data. One of those is a username (usually this will be a company email address – a public piece of information) and the second is a corresponding password. That's all the information needed to access your company secrets. Secrets like financial records, perhaps remote control of IT systems like a DNS server, or the ability to read company files.

Registered company number: 08927013

When this is taken into consideration along with how many passwords are used across a single organisation, and how the discovery of a single password by an attacker could bypass IT security controls, the potential impact is obvious.

The question then becomes – "how likely is it that someone could find a password for one of my employees?" and the answer is just as simple:

- Have you ever used the same password for more than one system on the internet?
- Could one of your employees have ever have used the same password for more than one system on the internet?
- Could one of those systems that you or your employees have ever used been compromised?

Commonly "yes" is the answer to all of these questions, and with billions of email addresses and passwords now in the hands of criminals and new ones being stolen every day the chances are that username and password combinations used by your staff are in circulation on criminal cyber markets right now.

DEFENCE AGAINST ACCOUNT TAKEOVER

Usernames and passwords leaked by 3rd party applications are a classic method used by criminals to gain access to business systems.

Whether it's through direct logins to cloud providers like Office365 or internet accessible RDP services, or accessing cloud based source code repository's to steel API keys, there are numerous ways attackers have found to use leaked usernames and passwords to cause massive damage to organisations over the last few years. Even when 2FA has been deployed, simply presenting valid credentials to legacy protocols and APIs frequently result in successful remote access or data theft.

Over 60% of data breaches are attributed to some kind of username and password compromise.

Trillion™ is designed to minimise these threats.

SUPERIOR DATA COVERAGE

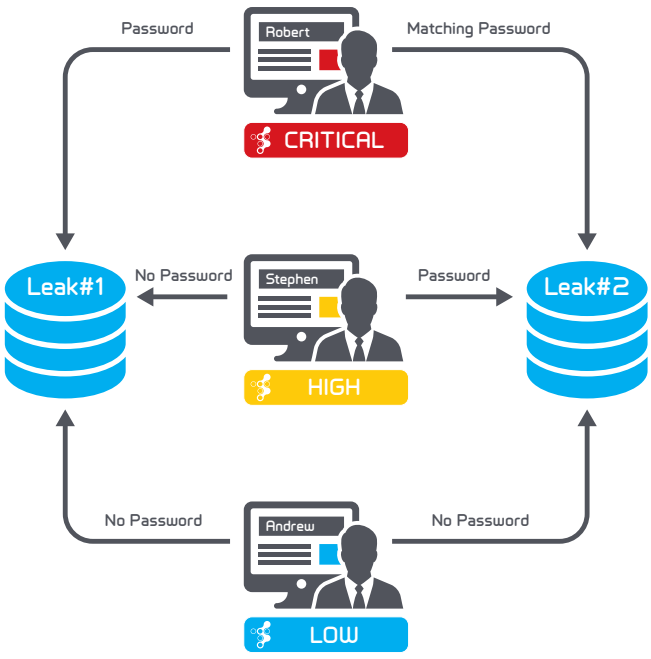
Trillion™ constantly monitors and inspects information originating from data breaches across the internet, looking for credentials that could belong to our customers. Tens of thousands of leaked username and password pairs are typically located every day - millions every month - which have been made available on dark markets and closed forums. Trillion™ has industry leading and award winning capabilities in the location and analysis of leaked data and is trusted by some of the world's biggest brands, and even some of the smallest.

RISK ANALYSIS

Not all data leaks are equal and it's important that you get an accurate understanding of the threat. The contents of data breaches can be varied and complex, and just because there might be a password for one user in a leak, there may not be a password for another. When a new leak is found by Trillion™, each individual entry will be analysed, looking for your data before having a risk scored applied.

This ensures you know specifically if accounts for your organisation could be at risk.

Trillion™ also uses dynamic big data mining to compare any new data with previously seen information, updating risk profiles for each user account as appropriate.



DATA FILTERING AND ENTITY MANAGEMENT

It's one thing to be alerted to potentially harmful user credentials, but it's another thing to manage that data effectively. Trillion™ provides the tools and intelligence needed to be able to effectively separate the noise from the real issues.

Trillion™ supports entity validation, meaning that it can actively try and determine whether the email addresses discovered on forums and dark markets are still relevant to your business. Using passive verification options including dynamic mail server requests or Active Directory queries Trillion™ can automatically flag the accounts that look like they belong to employees who still have live accounts in your infrastructure and therefore potentially matter the most.

Accounts that are less interesting or considered irrelevant can be supressed by an administrator ensuring they are removed from future alerts.

SECURE PASSWORD HANDLING

When it comes to dealing with leak data, the information that matters the most is usually passwords.

Without being able to visibly see the passwords data can't be trusted as authentic and remediation is difficult. Rarely will a user be able to remember all of the passwords they used on websites across the internet, and whether a password that was allegedly leaked might match one they use on company infrastructure today.

However, leaked passwords belong to the user and need to be protected from further distribution. This is important in order to protect the user from any further compromise of potentially private applications, and also to prevent the security teams from potential allegations of misuse.

Trillion™ addresses this balance of 'need-to-know' and 'need-to-protect' by providing features that enable secure sharing of discovered passwords through a unique user portal. Company security officers can securely request that Trillion™ transmit passwords to its owner, where it can be viewed and verified in a secure environment. Password strength hints are provided to security officers, based on password commonality and entropy, but the password cannot be accessed by anyone other than the original creator. This protects the organisation, the user and ensures data handling is in accordance with data protection legislation.

CROWD SOURCING FEEDBACK

Ultimately the reason to monitor for leak data is to know if the business needs to intervene in order to protect the data and systems of the organisation.

If the data being distributed turns out to be false, or inaccurate, then no action will be required. But if the information is correct, relevant and potentially harmful to the organisation then it may require a rapid response.

The most effective and accurate way of determining the correct response to a data discovery is to bring the affected user into the response and remediation process.

When a security officer decides to share data located from a breach with a user, the user is asked to respond with feedback on the material found and whether it looks accurate. This feedback benefits all organisations using Trillion™ by increasing the overall confidence in the breach data, and it helps security officers locally determine if they need to take a proactive response.

INCIDENTS

Trillion™ supports the concept of incidents. Optionally, incident features can be enabled that will specifically ask the user to confirm if the password shared with them is in active use on a corporate system.

A positive response to this request will instantly raise an incident in Trillion™ and alert the organisation's security team. An incident in Trillion™ indicates clearly that a users leaked password could provide access to a corporate system.

CROSSWORD CYBERSECURITY

+44 20 3953 8460 info@crosswordcybersecurity.com

Capital Tower, 10th Floor, 91 Waterloo Rd, South Bank, London SE1 8RT

Registered company number: 08927013