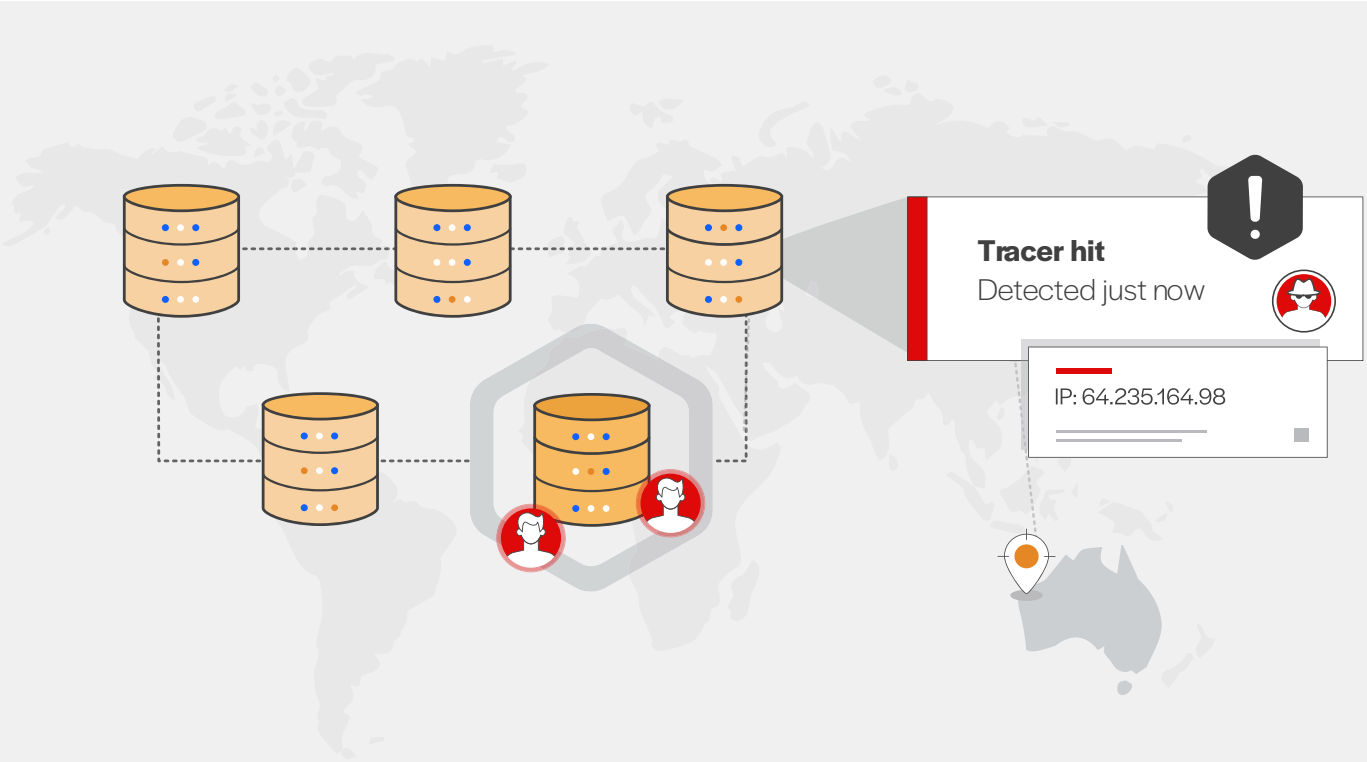
HoneyTrace

Trace. Detect. Respond.



USE CASE

External Data Breach Detection

Do you trust that your sensitive data remains safe?

Our reliance on digital systems and the growth of online data storage has contributed to the rising frequency of data breaches. These breaches involve unauthorised access to sensitive information and can have a significant impact on all organisations, our customers and partners.

Personal Identifiable Information (PII), including customer and employee data, is frequently a target for theft. Unfortunately, we only become aware of these breaches and the removal of this data after the damage has already occurred.

HoneyTrace can help you discover and provide a targeted response to the accidential or deliberate loss of personal and corporate data.

Detecting Data Breaches with HoneyTables & HoneyRecords

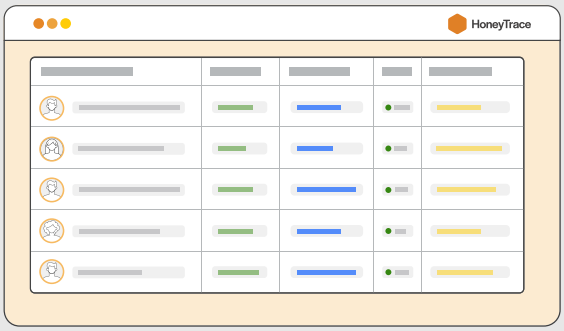
Sarah is concerned about the risk of her customer data being stolen. This data is organised in column and row entries, and is stored in several locations, including production databases and backups.

Sarah has anticipated the risk of a data breach by an external threat and wants to be notified of any potential network intrusion and unauthorised access to this data. This threat to her organisation will be reduced, if her team can detect and respond to a data breach in a timely manner.

To receive the earliest possible warning of a network intrusion, Sarah's team employs HoneyTrace to generate HoneyTables and HoneyRecords.

What are HoneyTables & HoneyRecords?

HoneyTables are structured data tables comprised of AI generated data stored in rows and columns.

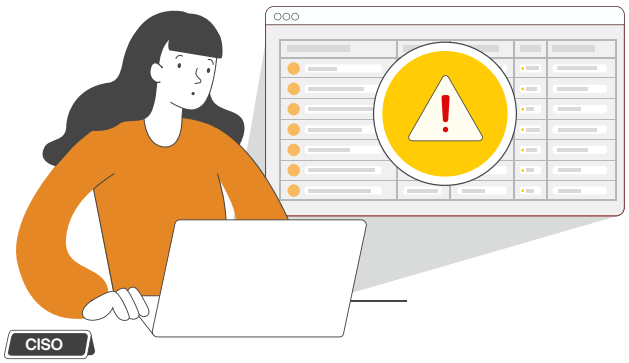


HoneyTables can be deployed as a document on your file system. Alternatively, the HoneyTable can be converted and deployed as a database. As HoneyTables contain entirely fake data, any interactions with the data are rare, obvious and suspicious.

HoneyRecords are singular rows of AI generated PII.

These records can be inserted into your real databases. They are globally unique and only exist in this single instance, so any appearance of this record outside of the database is very rare and highly suspicious.

If you receive an alert from the HoneyRecord, this can indicate your real data has been accessed and potentially stolen.



STEP 1

Conduct a planning workshop

Sarah's team begins by conducting a planning workshop to create a strategy for a HoneyTable & HoneyRecord deployment. Due to the speed of generation and ease of deployment, Sarah directs her team to undertake early action and iteratively deliver improvements to the plan.

STEP 2

Create a campaign

The team accesses HoneyTrace and creates an External Data Breach campaign, so they can track the HoneyTable & HoneyRecord activity in a central location.

STEP 3

Generate and configure tracers

Based on their strategy, the team generates a HoneyTable and a HoneyRecord containing fake customer records. During the generation process, the email tripwire, beacons, search, data breach & 3rd party detection tracers are configured.

STEP 4

Deploy a HoneyTable

Sarah's team deploys the HoneyTable using two methods.

For the initial deployment, the team places the HoneyTable as a document in their file system. They craft an enticing filename to attract malicious actors who are searching for this type of data.

For the second deployment, the team converts the HoneyTable into a MySQL database, to mimic their existing customer database. To make the HoneyTable database more attractive, they deploy the database configuration file, which includes administrator credentials, onto their system administrator's workstation.

Both versions of the HoneyTable are placed in an enticing but realistic location, that is unlikely to be accessed by legitimate users. Instead, it lures the attention of malicious actors.

What are tracers?

Tracers are the detection mechanisms, that detect interactions with HoneyTable and HoneyRecord data. All tracers have their strengths and weaknesses. We recommend configuring more than one tracer, to increase your likelihood of detecting unauthorised access.

Beacons are Thinkst Canarytokens and office macros. Beacons are triggered when a file (docx, pptx and xlsx) is accessed, while there is a live internet connection. HoneyTables can be deployed as an xlsx file on your file system. If a beacon is embedded, you will be notified when someone opens the file.

Email tripwires are fake email addresses that are triggered when the email account receives an email. If you receive an alert from an email tripwire, this gives you an indication that someone has accessed the HoneyTable or HoneyRecord and may be attempting to use that email for further reconnaissance activities.

Data leak tracers are triggered when uniquely crafted content is discovered on one or more data leak sites. For HoneyTables & HoneyRecords, HoneyTrace will be looking for instances of email tripwires appearing on these sites.

Basic search tracers look for matching file information on the open internet. For HoneyTables & HoneyRecords, the search tracer will look for email tripwires that have been exposed. Alerts from basic search and data leak tracers indicate that your HoneyTable or HoneyRecord data has been compromised and leaked on the internet.

3rd party detection tracers produce an MD5 & SHA256 hash for the HoneyTable or HoneyRecord. These can be ingested into your existing cybersecurity systems such as Endpoint Detection & Response (EDR) and further track when these files have been accessed or moved.

STEP 5

Deploy a HoneyRecord

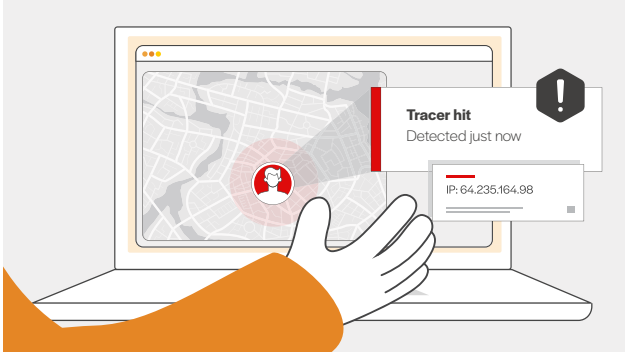
The team deploy a HoneyRecord within their real customer database as a secondary measure to ensure they are notified if their real data is accessed.

Sarah creates a routine process to generate new HoneyRecords and rotate them through the legitimate data periodically. This enables the team to understand the timing and likely source of the data breach.

STEP 6

Enable monitoring with EDR & SIEM

For an additional layer of monitoring, the team uses their existing Security Information and Event Management (SIEM) and Endpoint Detection & Response (EDR) systems to set up rules and alerts around HoneyTable access. ie. log correlation.



STEP 7

Identify suspicious behaviour

As HoneyTable & HoneyRecord data is fake, there is no need for any legitimate users to interact with them. Therefore, alerts can indicate suspicious behaviour and should be investigated.

Sarah is alerted to any suspicious activity, enabling her to respond quickly, secure her legitimate data and reduce the impact of the data breach.

Start tracing today

Contact us: info@penten.com

Amiosec penten