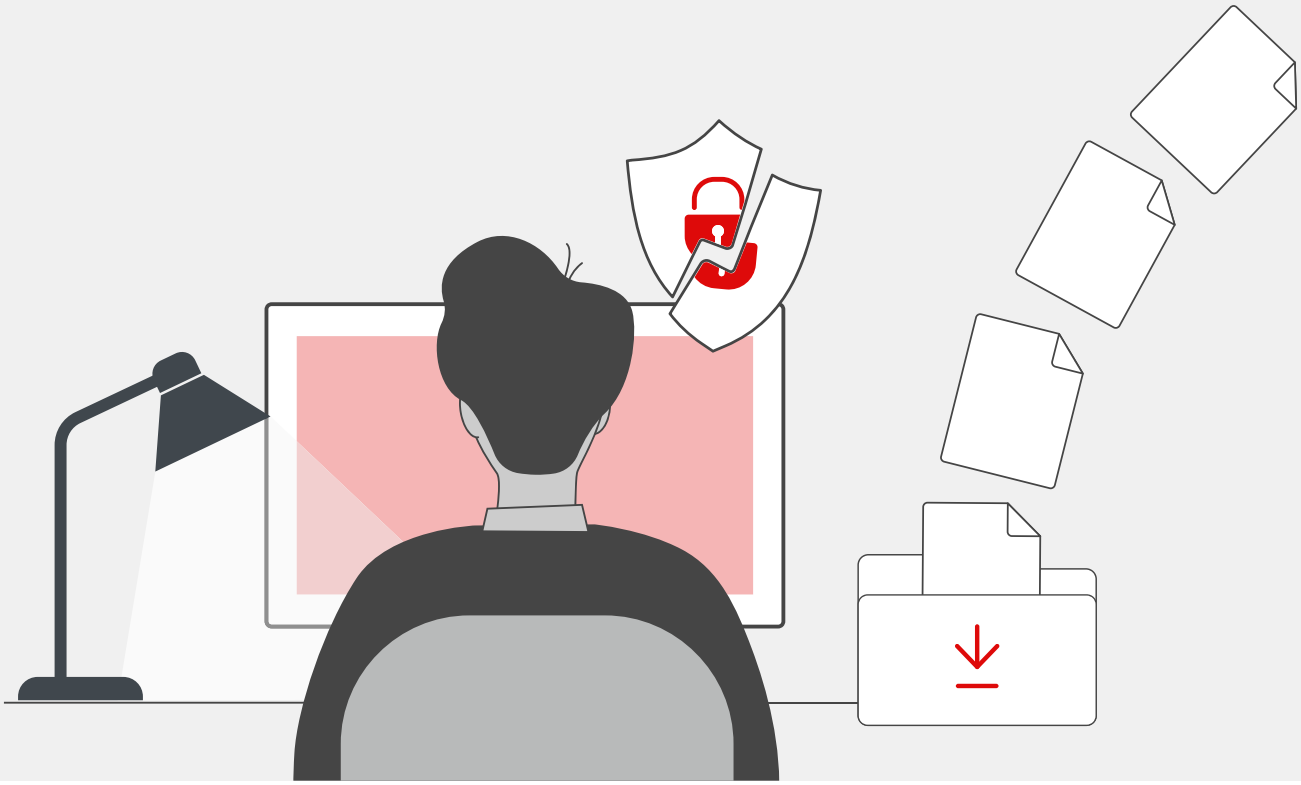
HoneyTrace

Trace. Detect. Respond.



USE CASE

Detecting Insider Threats

Are you actively defending your data from insiders?

Insider threats pose a significant risk as they involve individuals with authorised access to your organisation's systems that either accidentally or intentionally steal sensitive information. Detecting insiders is challenging since they have legitimate access, familiarity with security measures, and the ability to blend in with regular operations. Furthermore, malicious external actors can masquerade as legitimate users, making it difficult to distinguish their behaviour from regular activity in the period leading up to an attack.

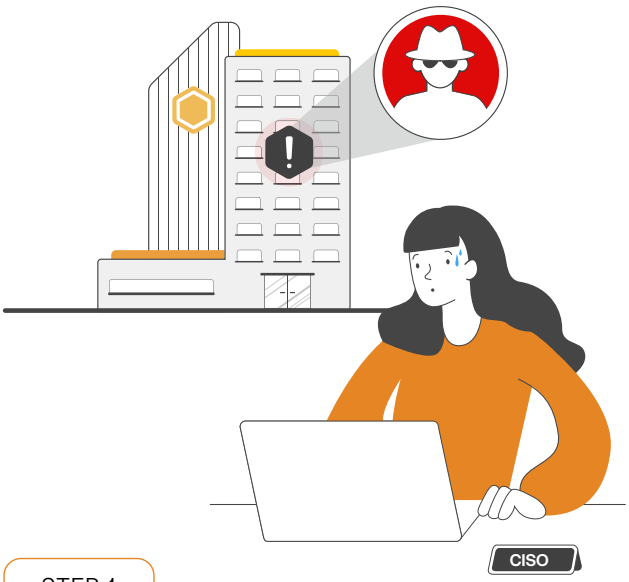
The trust placed in insiders often results in delayed detection, allowing threats to persist and escalate while causing financial, reputational, and operational damage to your organisation.

HoneyTrace can help you discover and provide a targeted response to insider threats.

Detecting Insider Threats with HoneyFiles

The risk of an insider threat is a significant concern for Sarah's organisation. Although there are no apparent signs of an insider threat, she's aware of the challenge in identifying such risks. Sarah is determined to remain vigilant and not overlook any misuse of access by her employees, contractors, or outsourced support.

To detect potential insider threats, Sarah's team uses HoneyTrace to create HoneyFiles.

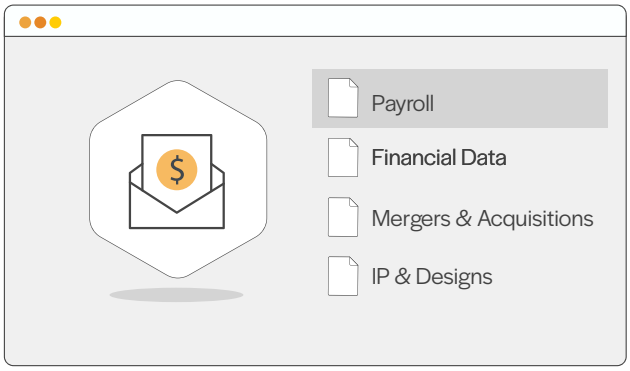


STEP 1

Conduct a planning workshop

Sarah's team conducts a planning workshop to create a strategy for a HoneyFile deployment. During this workshop, they define their deployment objective, pinpoint the types of data susceptible to insider theft, and determine the optimal HoneyFile deployment locations.

The team opts for a long-term insider strategy, attempting to identify employees engaging in unauthorised snooping activities. They consider the types of data likely to attract a snooping insider and identify topics such as payroll information and future organisational strategies.



For the HoneyFile deployment, they identify valid locations where administrators should not browse to by accident, as well as practical areas where this type of data could plausibly be stored.

STEP 2

Create a campaign

The team accesses HoneyTrace and creates an Insider Threat campaign, so they can track the HoneyFile activity in a central location.

What are HoneyFiles?

HoneyFiles are decoy files designed to detect unauthorised access to data. They appear to contain valuable or sensitive information; however, the content is entirely fake and generated by an AI engine.

As HoneyFiles are fabricated, there is no legitimate reason for them to be accessed. When they are strategically placed around a network, and a user interacts with the HoneyFiles, HoneyTrace will raise an alert for investigation.

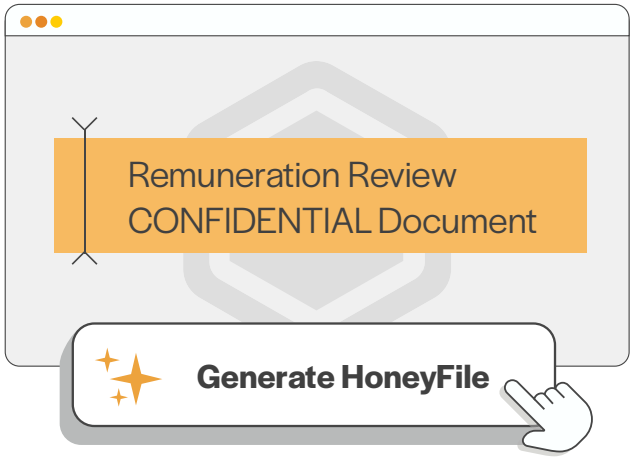
HoneyTrace has various HoneyFiles templates that can be customised to match the branding and identity of your organisation. You can also create HoneyFiles by uploading your own templates.

STEP 3

Generate HoneyFiles

Sarah & the team use AI processes and templates in HoneyTrace to create a series of HoneyFiles containing content that corresponds to the topics they've chosen.

They configure tracers for each document, so they can detect access to the HoneyFiles. A combination of tracers are used to increase their likelihood of detection.

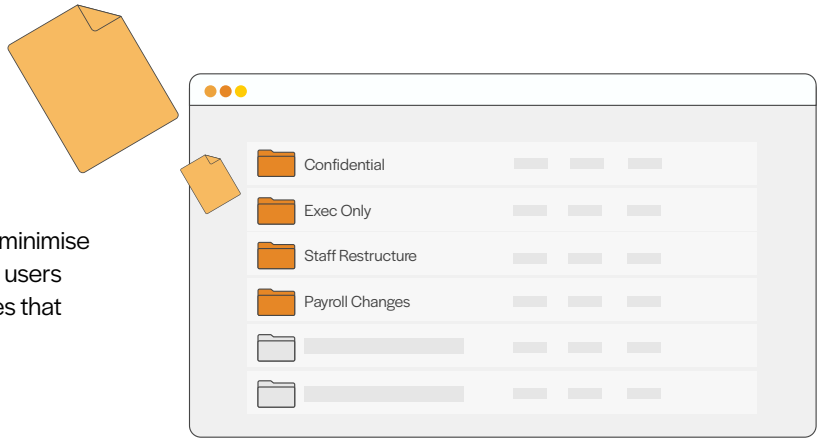


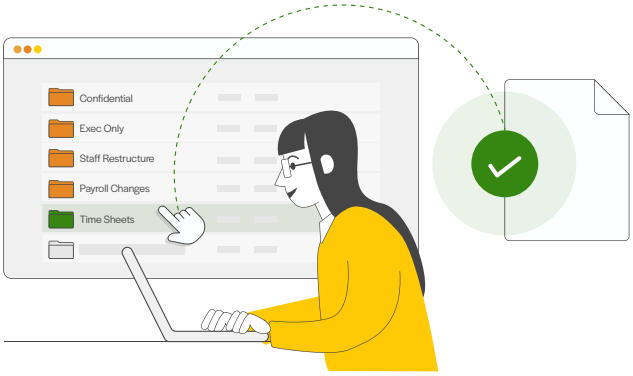
STEP 4

Deploy HoneyFiles

The team collaborates with selected members from various departments to create folders inside the finance, HR, and executive areas. They use enticing folder names to match the HoneyFile content.

They work with each department member to minimise access to the folders, ensuring that legitimate users don't inadvertently engage with the HoneyFiles that will be placed inside.





STEP 5

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 access to each of the HoneyFiles ie. log correlation.

STEP 6

Identify suspicious behaviour

As HoneyFiles are fake, there is no need for any legitimate users to interact with them. Therefore, alerts can indicate suspicious behaviour and should be investigated. Alerts produced by HoneyTrace and other cybersecurity systems enable Sarah's team to investigate a potential insider threat.