06 Steps to Effective Threat Hunting

Threat hunting is a tactic where IT experts proactively search for hidden malicious threats or activity within an organisation's network. When paired with standard cybersecurity measures, threat hunting offers small and medium-sized businesses full protection against cyber threats.

1 Make sure you have the right data and the right context

If you don't have any data, there is no way to search for threats. No data = no threat hunting. Make sure you collect data that gives a wide frame view of activity and behaviors across multiple operating systems

Hackers attack as often as every

39 seconds

2 Understand what "Normal" looks like

It's essential to create a picture of what 'normal' looks like for your environment. This provides an idea of what normal network behavior, data, and user activity looks like for your organisation. This is key to identifying threats that don't look normal to your environment.

43% of attacks are aimed at small and medium-sized businesses (SMBs)

3 Develop a hypothesis

Hypothesis are used in threat hunting as a foundation for investigations. Developing effective hypotheses are based on Open-source intelligence tools, frameworks, social intelligence, threat intelligence, and past experiences. As the threat environment is continually changing, intelligence-driven, hypothesis-based threat hunting will continue to expose risks.

35% of hunters create hypotheses to drive their threat hunting efforts

4 Investigate and analyse potential threats

After the hypothesis, investigating threat patterns in the data can give a better understanding of the attacker's tactics, techniques, and procedures (TTPs). If the hypothesis is correct and evidence of malicious activity is found, you must validate the full scope and impact of the threat.

42% of advanced, emerging threats are missed by traditional security tools

5 Plan a rapid and automated response to remediate threats

Once you uncover new tactics, techniques, and procedures (TTP), you must quickly and effectively respond to and correct the threat(s). Understanding the cause of the threat is key to improving future security and prevention measures. The main goal? Immediately stop the ongoing attack and prevent any damage from a potential threat.

The average time spent identifying and containing a security incident is

277 days

6 Make improvements and automate for the future

The final step is to update your system and data based on the knowledge gained during the threat hunting process. This allows your business to automate future prevention mechanisms. With improvements, an organisation's global security is improved due to the discoveries made during the threat hunting investigation.

4.35M average cost of a data incident

Contact us today!

Security@trustsystems.co.uk