WHAT IS MANAGED THREAT HUNTING AND WHY SHOULD YOU INVEST IN IT?

Threating hunting - it's a relatively new offensive strategy being deployed by organisations and managed service providers (MSP), but it's one that gaining increasing traction.

And it's no surprise with its more proactive approach to searching for and detecting cyber security threats.

As cyber criminals continue to devise increasingly sophisticated forms of attack, the need for more rigorous security methods is becoming essential to keeping your confidential data secure.

That's where threat hunting comes in.

Put simply, threat hunting is:

The repeated process expert analysts carry out to proactively search networks to identify and isolate security threats that escape traditional detection methods.

Like many in-house cyber security solutions, threat hunting can be difficult and expensive for businesses to implement and manage. As such, many are turning to threat hunting as a service.

Partnering with an MSP has a host of benefits. Not least because it provides access to an already-established team of cyber security experts and the associated technology.

In our latest blog, we take a closer look at what managed threat hunting is and its many benefits...

What is threat hunting?

Threat hunting is the process of proactively searching for cyber threats that are hidden in your network.

It is the job of expert threat hunters to search your networks and endpoints to find malicious actors that have been missed by your existing security solutions like firewalls, intrusion detection systems (IDS), malware sandboxes and SIEMs.

Threat hunters use manual and machine-assisted methods to proactively search for indicators of compromise or gaps in your detection coverage.

Once inside, a hacker can remain in a network undetected for months. So, threat hunting not only improves your threat visibility, but it also enables threat hunters to alert incident response teams efficiently to respond to threats before they can escalate.

What makes threat hunting different?

There is also often some confusion over how threat hunting is different from other applications, such as penetration testing.

While pen testing performs a simulated cyber attack on your systems to identify weaknesses, threat hunting assumes that an organisation has been compromised.

The role of the threat hunter is to understand how an attacker would think and the techniques they would use to compromise the organisation. They can then create automated detection use cases to discover new attack patterns to identify unusual behaviour of users, methods and systems.

By doing this, the threat hunter is always one step ahead of traditional security systems (firewalls, IDS, SIEMS, etc.) that adopt a more reactive response to potential attacks or a security incident that has already occurred.

The keyword for threat hunting is, therefore, "proactive". It's all about proactively hunting for threats in real-time to improve the organisation's detection coverage.

What are the benefits of managed threat hunting?

With talent shortages and time-consuming processes, many organisations are turning to external threat hunting rather than managing it internally.

Benefits of outsourcing your threat hunting include:

1. Access to experts

Threat hunting requires skilled cyber security analysts. Recruiting and retaining these key members of staff can be tricky. By partnering with an MSP, you can leave the responsibility of recruiting new staff and providing specialist ongoing training in their hands and take advantage of their pool of highly-skilled experts.

2. Greater accuracy

With external threat hunters dedicated to focusing on searching your networks, you can be sure you'll receive a more accurate and faster service. MSPs also have access to their advanced tools and technology to provide more precise responses than a business typically could.

3. Increased efficiency

The huge number of alerts and the large amount of data analysts face is one of the biggest challenges of threat hunting. It's a laborious task. Leaving threat hunting to external professionals keeps your IT department free to continue with their day-to-day tasks and servicing the business.

4. Continuous threat hunting

The level of involvement threat hunting entails should never be underestimated. It's a constant activity that runs on a 24/7 basis. By leaving this task in the capable hands of external threat hunters ensure your networks are properly and continuously monitored.

Our complete range of managed cyber security services keep your business protected 24/7. With years of experience, best in class processes and a team of security experts, we can devise a solution that's tailored to your exact requirements and potential cyber threats.

Contact us today for more information and to discuss your business' needs.