Why threat hunting should matter to every board

**Monitoring alone cannot detect every threat. Proactive threat hunting can expose gaps in defences and help organisations learn from others facing common threats. **

Boards should have confidence that their organisation can detect and investigate emerging cyber threats, including activity that existing security alerts may miss.

Organisations use a range of cyber security controls. They use security products, receive threat intelligence and monitor alerts from trusted providers. Many have well-developed processes for responding to known threats. But these measures can't tell you everything about your ability to detect an attack.

When a new attacker technique is identified, ask: **could we detect this technique if it was used against us?**

If your organisation can't answer that question, it may have gaps in its visibility or detection capability.

As attackers use AI to operate at greater speed and scale, identifying and addressing these gaps becomes increasingly important. Organisations need to be able to identify signs of malicious activity early, rather than relying solely on detecting an attack once its effects become apparent.

Threat hunting can help organisations test their ability to detect relevant attacker activity and expose gaps in their defences.

This blog is for boards of organisations that monitor their systems for cyber threats, either themselves or through a third-party provider. It explains why threat hunting matters as threats evolve, and how boards can support their organisation to learn from what it finds and turn those insights into stronger cyber defences.

Monitoring cannot detect every threat

Security monitoring is fundamental to effective cyber defence. It helps organisations identify potentially malicious activity using established detections and alerts. But not every threat will trigger an existing alert. This is where threat hunting can help.

Threat hunting is the proactive search for signs of cyber threats or intrusion that existing security rules and alerts may have missed. A hunt starts with a question or hypothesis, based on factors such as attacker behaviour or threat intelligence, and uses available security data to look for evidence. Threat hunting complements security monitoring; it doesn't replace it.

Focus on attacker behaviour

Cyber defenders have traditionally made extensive use of indicators of compromise (IoCs), such as malicious IP addresses, domains, file hashes, or malware signatures. These are useful but they can change quickly.

Attacker behaviours can be more enduring. Security professionals describe these behaviours as **tactics, techniques and procedures (TTPs)**. Put simply, TTPs describe *how* an attacker operates, rather than *what* specific tools or infrastructure they use.

> An IP address may change overnight. A technique for moving through a network may remain relevant for much longer. Focusing on attacker behaviour can therefore provide a more durable basis for detection.

Threat hunting allows defenders to use knowledge of these behaviours to ask whether they can see evidence of them in their own environment.

For more detail on how threat hunting works in practice, including the use of attacker TTPs, read our blog on observability and threat hunting.

You can't hunt what you can't see

Threat hunting depends on **observability**: having a clear and detailed view of what is happening across your organisation's networks, systems and services.

To investigate whether a particular attacker technique could be present, defenders need the right security data. Systems need to record relevant activity, and defenders need access to that data. Without it, they may be unable to see evidence that a technique has been used.

This means a threat hunt can reveal more than malicious activity. **It can also identify gaps in an organisation's visibility and detection capability.** For example, a hunt may show that defenders don't have the data they need to determine whether a particular attacker technique has been used.

For boards, that is valuable information. Even when a hunt finds no evidence of malicious activity, it can reveal where the organisation needs better visibility or stronger detection capabilities.

Those findings should feed back into the organisation's defences, for example by *improving the security data available to defenders*, *strengthening detections*, or *addressing other weaknesses identified by the* hunt.

What should boards be asking?

Responsibility for cyber defence is often spread across different teams, including security operations, infrastructure, technology, risk and governance functions. Boards need assurance that those teams can turn information about emerging threats into action, and that gaps in visibility or detection are identified, owned and addressed.

Boards don't need to understand the technical details of threat hunting or conduct hunts themselves. They should ask questions that test whether the organisation has an effective capability:

- Which attacker techniques are most relevant to our organisation?
- Can our defenders detect or investigate those techniques in our environment?
- Do our defenders have the security data and visibility they need to investigate them?
- When they identify gaps in visibility or detection, who is responsible for addressing them?
- How do we know whether those gaps are being addressed and our ability to detect threats is improving?
- Are our defenders learning from and collaborating with other organisations facing similar threats?

Boards should look for evidence, rather than relying on reassurance alone. This could include:

- examples of relevant attacker techniques the organisation has tested its visibility and detection capability against
- gaps those investigations have identified
- who owns them
- what has been done to address them

Over time, boards should be able to see whether those gaps are being closed and the organisation's ability to detect relevant threats is improving.

Build on the capability you already have

Effective threat hunting doesn't necessarily require a new threat-hunting team. Organisations may already have people, data and security functions that can provide much of the capability they need.

A useful starting point is to understand what already exists and where the gaps are. For example:

- do defenders have the security data they need?
- can they use that data to investigate attacker techniques across the organisation's systems?
- is there a clear process for acting on gaps that hunts identify?

Organisations should also consider how they use the threat intelligence they receive. Threat intelligence is most valuable when defenders can act on it, for example by turning knowledge of relevant attacker behaviour into questions they can test against their own systems.

Where skills or capability are limited, organisations should consider how existing security providers and trusted practitioner communities can support them, rather than assuming they need to build a new team.

Learn from other defenders

Organisations often face common adversaries, vulnerabilities and technologies. It therefore makes little sense for every organisation to solve every detection problem independently.

Sharing knowledge of attacker behaviour, relevant threat intelligence and approaches to threat hunting can help defenders build a broader picture of common threats, learn from each other and tackle security problems they have in common.

The NCSC encourages organisations to engage with defender communities, where they can exchange insights, discuss emerging threats and learn from real-world incidents.

What one organisation learns from investigating an attacker technique may also help others facing the same threat. Sharing these insights can improve the ability of individual organisations and the wider community to detect and respond to malicious activity.

Organisations can also learn from other defenders through sector-based Information Sharing and Analysis Centres (ISACs) and industry forums. Commercial threat intelligence providers can be another source of information about relevant threats.

Focus on capability, not the solution

For boards, the question is not whether to commission a particular threat-hunting product or create a new team. It is whether the organisation can investigate relevant attacker behaviour, identify gaps in its ability to detect threats, and act on what it learns.

Ask your defenders how they know they could detect the attacker techniques most relevant to your organisation, what gaps they have found, and what they are doing about them.

Patrick B, NCSC Communities Business Lead

WRITTEN BY

Patrick B
NCSC Communities Business Lead

PUBLISHED

17 November 2026

WRITTEN FOR

Cyber security professionals

PART OF BLOG

NCSC publications