CYBERSECURITY 101 · eBuilder Security

Threat Hunting

The most capable attackers get in without setting off a single alarm, and some stay hidden for years. Threat hunting is how you find them. Here is what it is, and the one habit that shortens their head start.

WHAT IT IS

Threat hunting is the proactive search for attackers who are already inside your network but have not set off an alarm. The tools most teams rely on, from antivirus to a SIEM, only catch known signatures and written rules. The most capable intruders make sure they match neither, so someone has to go looking. Threat hunting is that active search, done by people using data rather than waiting for a warning.

WHY IT MATTERS

5+ years

How long a state-linked group kept undetected access inside some victim networks.

CISA advisory, 2024

Up to 18,000

Organisations that installed the trojanised SolarWinds update before it was caught.

SolarWinds SEC filing, 2020

24 and 72 hours

The NIS2 deadlines to warn and then fully report a serious incident. Fast detection is what makes them survivable.

NIS2 / Cybersäkerhetslagen

WHAT HAPPENED

In February 2024 CISA, the NSA and the FBI warned that a Chinese state-sponsored group called Volt Typhoon had hidden inside US critical infrastructure networks for as long as five years. It used legitimate built-in tools and stolen but valid accounts, so there was no malware to detect. The agencies told organisations to actively hunt for the activity, because signature-based tools could not see it. (CISA, 2024)

RED FLAGS TO WATCH FOR

You will not get an alert for the quietest intrusions, so hunt for the behaviour instead.

- Legitimate admin tools like PowerShell used at odd hours or on machines that never normally run them.
- Valid accounts logging in from new locations or acting outside their usual pattern.
- Unexpected outbound connections from trusted servers or trusted software.
- Long stretches where nothing is flagged, on systems no one is actively reviewing.

THE ONE RULE THAT STOPS IT

Assume a breach has already happened and go looking for it on a schedule, rather than waiting for a tool to raise the alarm.

THEN BUILD THE HABIT AROUND IT

- Centralise your endpoint, network and identity logs so a hunter can query them in one place.
- Run regular hypothesis-driven hunts on your most valuable systems and accounts.
- Adopt MITRE ATT&CK as a shared language for the techniques you hunt for.
- Turn every confirmed finding into a new automated detection rule.

MYTHS AND FACTS

MYTH

Our firewall and EDR already stop attacks, so hunting is unnecessary.

FACT

Those tools catch known signatures and rules. The strongest intruders use legitimate tools and valid accounts to avoid both, which is why CISA urges organisations to hunt.

MYTH

Threat hunting is the same as incident response.

FACT

Hunting is proactive and starts before any alert. Incident response is reactive and starts once a threat is confirmed. Hunting often feeds it.

MYTH

No alert means no breach.

FACT

The most dangerous intruders generate no alert at all. Their absence from your dashboards is exactly what hunting is designed to test.

THE LEGAL DUTY

Continuous monitoring is now a legal duty under NIS2, in force in Sweden as Cybersäkerhetslagen (SFS 2025:1506) since 15 January 2026, with boards personally accountable under Article 20.

GET HELP

eBuilder Security, based in Stockholm, provides managed detection and response with proactive threat hunting, so someone is actively looking for what your tools miss. Read the full guide at the link below.

Read the Full Article →