Go from reactive to proactive:

5 criteria to select the right MDR partner for your business

Dubex:

Dubex:

The current threat landscape places almost impossible demands on IT security managers, and the way you organise security in your business:

- you need to balance a growing number of devices, each representing a new addition to your company's attack surface,
- while taking into account human resource scarcity,
- and avoiding hostile attack methods.

This leaves even the smartest IT security manager breathless.

That's why many companies choose to work with a cybersecurity partner for a Managed Detection & Response (MDR) solution.

But how do you select the best MDR solution and service partner for your business?

Here are 5 criteria to navigate the MDR jungle.

With an MDR service agreement, log management is outsourced to a third party service partner that analyses and handles critical incidents, attack patterns, and alerts for you around-the-clock. This extension of your security team means you can concentrate on scaling your business, and not take the operational hassle in-house.

Cyber Security Specialists Who Are Always Watching

Investigation

Certified analysts classify the threat incidents based on ML, threat intelligence, and their own expertise

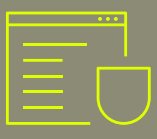
Mitigation

Analysts mitigate and resolve threat incidents, and escalate them to you proactively as needed.

1 2 3 4

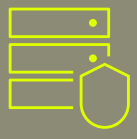
Detection

Threat incidents are identified in real-time by ML-based detection engines.



Analysis

They interpret and document all relevant console incidents and provide you with recommendations for mitigation and resolutions.



1. Get management on board

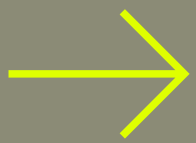
Cyber security is not only the IT department's responsibility - it's a shared responsibility that affects everyone in the entire organisation. An MDR solution is a financial and resource benefit to the business and should be high on the agenda of the executive team and board of directors.

But how do you actually get management on board the MDR journey?

Start by finding a service partner who is used to handling executive and board-level communication, if you don't have the skillset inhouse yourself. A trusted advisor can help you put MDR, and cyber security in general, at the top of management's agenda.

Next, make sure your MDR solution offers management reporting.

This includes reporting on the current and global threat landscape, which the service partner should have years of expertise in. Management is also presented with a detailed alert overview, so they get actual proof that incidents are indeed happening, and that they are being mitigated quickly.



2.
Go local

It may sound like a no-brainer, but finding a local MDR partner can be an advantage for your business when navigating the jungle.

With a local partner, you have clarity of where your logs are located and certainty of your data will not leave the country.

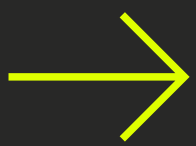
What's more, advice from the 24/7 monitored Cyber Defense Center can be communicated in your language, so you don't have to use extra capacity to keep up with a fast-talking security specialist in a foreign language when you're in a tight spot.

3.
Visibility and insight is golden

It's a great advantage to find an MDR partner that offers full insight into your own log data on the SIEM platform.

Some MDR service partners offer access to a dashboard where you can follow the log monitoring in real-time, which mirrors the MDR partner's log monitoring centre.

Consider whether it's valuable for you to be able to monitor logs from your own office desk. **It can provide greater visibility internally in the company (also for management), so you always have access to what's happening, real-time.**



4. Think technology-processes-people

We know you're good at your job, so this can be said without any offence: very few companies have the necessary capacity and experience to handle an incident from start to finish. And to be able to do it quickly.

Therefore you and your organisation need to take a hard look at your cyber crisis plans, your compliance skills to evidence for business insurance, and retention time on log data.

Can your internal skill set match a service partner's expertise in technology-processes-people?

It is often here, the great MDR partner shows its worth to your business.

5. Expand your experience, resources and expertise

The threat landscape is changing by the minute, so ask yourself: do we have the internal resources to continuously generate new, and updated, use cases based on the current threat landscape?

Having access to the latest threat intelligence on the current threat landscape can minimise massive operational losses to your business.

Therefore you should call for a broad and long-standing experience in IT security and attack vectors for your new MDR service provider.

Be at the forefront of MDR

Contact

Danni Bach Pedersen

Head of Cyber Defence Center

dbp@dubex.dk

+45 2018 1551