



# Incident Response

Respond to cyber incidents quickly and effectively with Eye Security

## So, you've just been attacked, what do you do?

### Deal with it yourself?

1

Isolation and containment are specialist cyber security skills. It can take time, which you don't have as the attack potential worsens.

### You might have an incident response plan?

2

Does this cover all types of threats and ramifications – you'll need the experience of all types of attack to be able to do so.

### Rely on your cyber security software?

3

Once an attack happens, there is only so much the software can do – it's already too late and you will not have the support you need.

### Engage external experts?

4

Liaising with external experts can be difficult without specialized knowledge, and time can be wasted doing so. Will it solve long-term vulnerabilities anyway?

Nobody wants to be a victim of a cyber-attack, but until you have, you do not realise the level of expertise it takes to immediately control it. Modern attacks carry a high level of sophistication and skilled attackers make it increasingly difficult for companies to protect themselves and to recover from a cyberattack; yet when it does happen, acting quickly and effectively is crucial to limit damage and high costs.

1/5

likelihood of a cyber attack

4 mins

avg. response time to an incident

## Your solution:

If you are attacked, you want to partner with the best – a team of experts, with years of experience gained areas from national intelligence and security agencies, amongst other specialist areas. These guys are on-hand 24/7, to ensure your operational processes are back up and running promptly. Some of the incidents we commonly face are:

- Encrypted files as a result of a ransomware attack
- Unexplained behaviour in operational systems
- Fraudulent e-mails sent by an attacker

We've seen all types of attack and with all of them, our remit is to fix the problem quickly and be there for you as an extended member of the team, calming things down and supporting.



## How Incident Response works

- **Triage**  
Swiftly identifying the incident type and assessing its impact on your data's availability, privacy, and integrity.
- **Kick-off**  
An immediate meeting to outline the Incident Response process, ensuring clear understanding and assigning responsibilities for all involved parties.
- **Containment**  
Analysing, containing, and minimizing the adverse consequences of the incident – meticulous actions to secure your digital assets.
- **Recovery**  
Removing the threat and restoring your systems with a methodical approach to bring your operational processes back online.
- **Evaluation**  
Actioning the valuable three lessons from the incident: fortifying network security, refining the Business Continuity Plan (BCP), and optimizing the response.

## The benefits of Incident Response

### Rapid response

The moment you reach out to our incident response hotline, we initiate analysis and take immediate steps to mitigate the threat.

### Limited damage

Deploying our expertise through Managed Detection & Response software swiftly, we secure your systems to prevent further damage.

### Back to business promptly

With such an experienced Incident Response Team, we ensure a swift return to normalcy, minimizing disruptions to your business.

# Meet the team

Why customers trust our team with their cyber security

Our team members bring a wealth of experience from the secret service and high-level security environments. With a track record of navigating complex threats, we combat cyber challenges intelligently and calmly, drawing on insights gained from real-world scenarios.

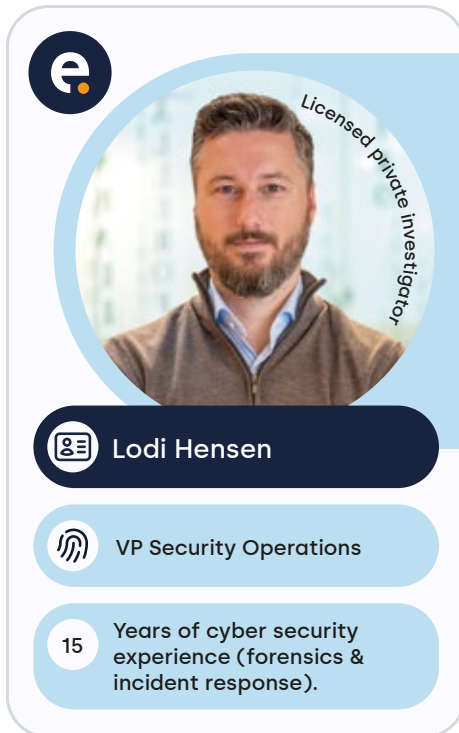


Profile card for Vaisha, Principal cyber security specialist, with 13+ years of IT security experience. The card features an orange background and a circular portrait of Vaisha.


 **Vaisha**


 Principal cyber security specialist


 13+ Years of IT security experience




Profile card for Lodi Hensen, VP Security Operations, with 15 years of cyber security experience (forensics & incident response). The card features a light blue background and a circular portrait of Lodi Hensen. A vertical text label 'Licensed private investigator' is overlaid on the right side of the portrait.


 **Lodi Hensen**

 VP Security Operations


 15 Years of cyber security experience (forensics & incident response).



Profile card for Michael de Klein, Senior cyber security specialist & Teamlead MDR, with 5+ years of experience (offensive and defensive). The card features a yellow background and a circular portrait of Michael de Klein.

 **Michael de Klein**

 Senior cyber security specialist & Teamlead MDR

 5+ Years of experience (offensive and defensive)



Profile card for Niels Teusink, Principal cyber security specialist, with 17 years of full-time IT security experience. The card features a yellow background and a circular portrait of Niels Teusink.

 **Niels Teusink**

 Principal cyber security specialist

 17 Years of full-time IT security experience



Profile card for Bas van den Berg, Principal cyber security specialist, with 8+ years of IT security experience. The card features a yellow background and a circular portrait of Bas van den Berg.

 **Bas van den Berg**

 Principal cyber security specialist

 8+ Years of IT security experience



Profile card for Davy, Senior cyber security specialist, with 6+ years of IT experience. The card features a yellow background and a circular portrait of Davy.

 **Davy**

 Senior cyber security specialist

 6+ Years of IT experience

## Our Incident Response Process:



## Your Incident Response checklist:

### 1 Identification

- ✓ Recognize and confirm the occurrence of a security incident promptly
- ✓ Define the scope and nature of the incident

### 2 Containment

- ✓ Isolate affected systems or networks to prevent further damage
- ✓ Implement temporary measures to minimize the impact

### 3 Eradication

- ✓ Identify and eliminate the root cause of the incident
- ✓ Remove malware, close vulnerabilities, and address weaknesses

### 4 Recovery

- ✓ Restore affected systems to normal operations
- ✓ Validate that the environment is secure and free from the incident's remnants

### 5 Communication and Documentation

- ✓ Notify relevant stakeholders, including management, IT teams, and, if necessary, law enforcement
- ✓ Document the incident, actions taken, and lessons learned for future improvements