

CSIRT

Your life line in case of a cyber attack!

The spotit Cyber Security Incident Response Service service provides you cybersecurity expertise and support for responding adequately to security incidents such as hacks, breaches, malware infections, and other cybersecurity threats. CSIRT experts will guide you through an incident to get your organization up and running again as soon as possible, with minimal impact.

Incident Response Service

Spotit's CSIRT service provides you a **24/7 hotline** that is designed to activate an experienced CSIRT incident response team to address any cybersecurity incident. When onboarding to this service a **breach readiness assessment** is executed. This is to define the current state of technology, people, and processes. You get a clear view on the organization's ability to identify, investigate, and respond to different types of cybersecurity incidents. Part of this service is the installation of a **honeypot** warning system to detect anomalies early allowing to respond to threats promptly. This service also makes sure all **relevant data is maintained up to date** for all experts involved.

End-to-end Incident Handling

CSIRTs maintain detailed records of incidents, responses, and outcomes. A lessons learned meeting will be organized in order to agree upon an improvement action plan.

During the preparation phase, spotit will perform several actions to make sure that your organization and our response teams are fully aligned in terms of roles and responsibilities, forensic capabilities, and response capabilities.

Once the attacker's control has been removed, it is time to restore those parts of the infrastructure that were impacted by the incident to a fully operational state.

With a well-designed eradication plan, we progress to remove all attacker-controlled components from your infrastructure and shore up defences so the attackers cannot regain control.

As soon as an incident is reported for which urgent response is required, our CSIRT Incident responder team will perform a first analysis and evaluation whether it concerns a materialized or identified security incident and the criticality of it. Once an incident is identified, our CSIRT coordinates the response, which includes containing the threat, eradicating the cause, and coordinate the recovery of any affected systems.



We want to contribute to your ability to detect incidents immediately. If a cyberattack is identified, our teams are immediately activated and start the necessary activities in line with the response plan.

What are the benefits for you?

Guaranteed response times

This service ensures rapid response to incidents, minimizing the time between detection and containment.

Access to expertise

This service provides direct access to specialists with extensive experience in cybersecurity incident response, which might not be available in-house.

Operational continuity

By prioritizing rapid containment and recovery, this service helps to ensure business operations can continue with minimal disruption.

Preparedness and planning

This service helps you prepare for and mitigate the impact of cyber threats through proactive planning and readiness assessments.

Tailored incident response

No 'one size fits all', but this service includes customized response strategies based on your specific needs, industry, and regulatory environment.

Continual improvement

This service includes post-incident analysis and recommendations for improvements, leading to better security posture over time.

Cost efficient

This retainer services is more cost-effective than in-house capabilities or ad-hoc consulting, especially considering the potential costs of cyber incidents.

Scalability

This service allows you to scale your incident response capabilities as needed, without the need to invest in and maintain a large in-house team.

Compliance and risk management

This service supports compliance with legal and regulatory requirements by ensuring that incidents are handled adequately and in line with best practices in cybersecurity response.

Why should you choose for spotit's CSIRT?

- ✓ We prioritize a **customized approach**, understanding your specific challenges and requirements, and delivering personalized services to address cybersecurity concerns effectively.
- ✓ Our **proximity** plays a crucial role. We are near you in case of an incident to assess situations closely and collaborate efficiently. We fight the battle with you.
- ✓ We go for **eradication focused CSIRT**: this approach prioritizes immediate action to isolate and neutralize threats, preventing them from spreading and causing further damage. By concentrating on containment, the service enables you to quickly resume normal operations, reducing downtime and associated costs.
- ✓ **Our CSIRT experts** possess contextual understanding and domain knowledge that enables accurate assessment of security incidents.
- ✓ With more than **10 years of experience**, spotit is seen as a leader in the market with a unique offering of both cybersecurity & connectivity services

For more info and pricing, reach out to info@spotit.be