INCIDENT RESPONSE RETAINER

In case of a security incident, we support you quickly, competently and proficiently

You could be the victim of a cyber attack at any time. Our Incident Response Retainer is the perfect solution when it comes to acting in a prepared, fast, efficient and effective manner.

- Support from our experienced Computer Security Incident Response Team (CSIRT)
- Fastest possible detection and isolation of the attacker
- Comprehensive damage analysis by security experts from our Swiss Cyber Defence Center
- Assistance in restoring normal business operations
- Compliance with the obligation to report a security incident within 72 hours according to GDPR

INFOGUARD IS THERE FOR YOU IN CASE OF A SECURITY INCIDENT

Today's threat landscape makes it inevitable that security breaches will also occur in your company. Therefore, you should be able to respond as quickly and professionally as possible.

That's exactly what we prepare for you in our joint onboarding workshop. And when the time comes, we can react, together with you: quickly, competently and with a lot of experience from other incidents. Day and night.

What you can expect from our service

- Onboarding workshop with **analysis** and **identification of your critical IT systems**. This makes it possible to react quickly and appropriatly in case of an incident.
- **Customer-specific**, **documented instructions** that clearly describe, based upon the event, what is done by whom, with which tools, and under which restrictions.
- You have access to proven cyber security experts at any time **7×24** – all InfoGuard **CSIRT** experts are SANS-certified or SANS instructors.
- By virtue of the existing contract, no time is lost and the **damage analysis** and the **necessary measures** can be implemented immediately.
- Your incident response process benefits from our **knowledge** of potential threats and **findings from other IR activities** and other InfoGuard cyber defence services.
- **Endpoint Detection & Response (EDR) Technology** can be rolled out when necessary to search for traces of an attack and to contain the attacker.

InfoGuard
CYBER DEFENCE CENTER

Incident Response Retainer – tailored to your exact needs

A security incident is not a good time to exchange business cards. That is why we establish a set of contractual terms and conditions so that you can call on our experts immediately in the event of an incident and get exactly the support you need.

Onboarding Workshop

In an onboarding workshop, our experts get an overview of the relevant processes and guidelines but also of your infrastructure and the corresponding specifications. The critical IT systems are also identified.

Our incident response onboarding workshop:

- documents the structure of your infrastructure and defines the relevant contacts.
- defines how InfoGuard should proceed in case of an emergency.
- defines the service features required from our CSIRT.

▼

DATA BREACH / INCIDENT

▼

Response

The InfoGuard CSIRT pinpoints the intruder, contains the impact, isolates the affected systems and makes recommendations regarding the implementation of measures. Depending on the situation, the response will be rolled out with an EDR technology by the CSIRT.

▼

Recovery

The CSIRT supports the customer to eliminate all traces of attack. Findings from the incident will improve the security system in the long term.

SECURITY EXPERTISE FROM SWITZERLAND

Highly qualified cybersecurity experts and analysts work in the InfoGuard Cyber Defence Center (CDC) in Switzerland. The CDC at our location in Zug is ISO 27001 certified. It has a multi-level, physical security concept and the security systems are monitored around the clock. InfoGuard also has experts in legal matters and professionals in crisis communication.

Do you believe that our Incident Response Retainer could be a good solution for your company? Get in touch with us. We would be pleased to explain our services to you personally. Benefit from our experts, who know your business and your environment, helping to reduce the time to contain an incident and minimise its impact.

ISO 27001
CERTIFIED

INFOGUARD.CH