Cyber Defence & Incident Response

Eliminate cyber risks with InfoGuard

InfoGuard
SWISS CYBER SECURITY

24/7 Cyber Defence Services from Switzerland

Managed Detection & Response
Hunting & Intelligence
Security Operations
Incident Response & Recovery
Forensics

Cyber Defence Services

Because cybercrime, skills shortages and reduced budgets are a reality

The highest threat evel has been reached. Current studies forecast losses of $10.5 trillion annually. Cyber attacks are among the greatest operational business risks and are comparable to an to the enormous force of nature that can strike with fatal force. Anytime and anywhere.

In the worst-case scenario, cyber attacks can affect companies unprepared – just like an avalanche that strikes suddenly and without warning. In such cases every second counts and every movement can set the avalanche in motion, a dedicated Security Operations Center (SOC) is the solution. The successful interaction of experienced experts, the latest technology and established processes within a SOC helps companies to protect themselves efficiently and effectively against attacks.

An enormous challenge! It is extremely difficult for companies of all sizes to find experienced security specialists. At the same time, the set up and 24/7 operation of a SOC represents a considerable investment. An endeavour that many companies don't want to afford.

You can't protect what you can't see

To make matters worse, most companies don't have complete insight into their security infrastructure and are confronted with a huge flood of warnings every day. This leads to an overload of security teams, critical alarms are overlooked and gaps in cyber security are emerging.

Cyber defence a must for your compliance

In light of the growing threat of cyber attacks, it's essential to strengthen your own cyber resilience. The NIST Cybersecurity Framework, Cyber Resilience Act, NIS2, DORA, ICT minimum standard and many other regulations explicitly require this. Non-compliance will result in massive sanctions. In addition, cyber incidents cause damage that threatens a company's existence and result in a massive loss of reputation.

How do you deal with this?

- Do you know the current cyber threat situation for your company?
- Do you have the necessary visibility to detect cyber attackers in your network?
- Can you prevent cyber attacks 24/7 before any business impact occurs?
- Are you able to react immediately to cyber attacks?
- Can you recover your ability to act quickly in an emergency?

The solution: Outsourcing this demanding task to an experienced Managed Detection & Response (MDR) service provider.

Cyber Defence & Incident Response

Detect and respond to cyber attacks and remain capable of acting

The top priority of InfoGuard Cyber Defence Services is round-the-clock monitoring – as SOC-as-a-Service or Co-Managed SOC – of your entire infrastructure so that cyber attacks can be detected immeditely and successfully defended against. To ensure that the Cyber Defence Service can be activated quickly, it is based on your existing infrastructure.

InfoGuard's in-house development team, ongoing investment in our Cyber Defence Center, the use of "Best of Breed" sensor technology and our platform developed and hosted in Switzerland ensure that we can react quickly to changing customer needs, new regulatory requirements and techno-logical trends.

When a security incident occurs, the focus is on protecting against a business impact and quickly restoring your ability to act through our own CSIRT. At the same time, we use forensic investigations to analyse the causes and attack vectors so that your cyber security can be sustainably optimised.

We accompany you on your entire security journey. Our service management team meets with you regularly to reflect on past incidents, discuss optimisation options and inform you about changes in the cyber threat landscape. Thanks to our experience and findings from many other customers, you benefit from customised security recommendations that continuously improve your cyber security.

We have successfully prevented business impacts from cyber attacks for all our customers with an MDR service.

InfoGuard CYBER DEFENCE CENTER

Benefit from our many years of experience:

24/7
Managed Detection & Response Services from our CDC in Switzerland

80+
Experts in dedicated SOC, CSIRT and Threat Intelligence Teams, a total of 250+ Experts

12+
Years of SOC Experience & Competence

300+
Cyber Defence & CSIRT Clients

4
Weeks for the structured SOC Onboarding

Hundreds of Incident Response Cases per year

BSI-qualified APT Response Provider, FIRST Member

Swiss SOC Platform

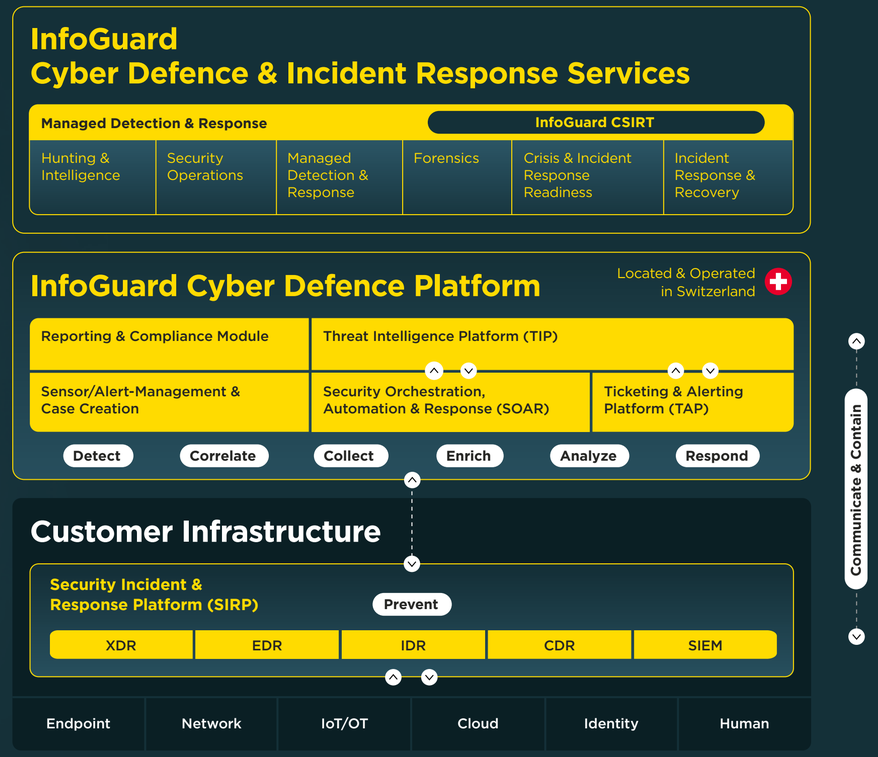
InfoGuard Cyber Defence Platform - At the heart of effective and efficient cyber defence

The InfoGuard Cyber Defence Platform – developed in-house, highly scalable and operated on-prem in Switzerland – forms the core of our Cyber Defence Services and is based on an open XDR architecture.

This also allows you to use our services as a co-managed SOC. To ensure that we see threats from all angles, the platform collects data from endpoints, networks, IoT/OT infrastructures, cloud environments and identities. Automation allows individual customer requirements to be realised efficiently.

By using different detection methods – including machine and deep learning – the platform can quickly detect anomalies and suspicious behaviour and enrich them with insights from actual security incidents, simulated cyber attacks and threat intelligence feeds. Thanks to the swarm intelligence among hundreds of customers, thousands of security incidents and hundreds of IR cases every day, the best possible protection and the fastest possible response are guaranteed. Threat alarms in distributed IT infrastructures can be forwarded specifically to the relevant departments.

The platform offers comprehensive transparency and works seamlessly with your existing technology stack. This shortens the onboarding time and eliminates vendor dependency. It also ensures that sensitive customer data is protected at all times and stored exclusively in our data center in Switzerland.



Cyber Defence & Incident Response Services from the Swiss Experts

Comprehensive protection against cyber attacks

Govern, Identify & Protect

Hunting & Intelligence

Our threat intelligence team actively searches for attack indicators in your infrastructure and cyber threats on the darknet. Benefit from our experience from recent cybercrime incidents, hundreds of incident response cases and insights from our Red Team.

- Compromise Assessment
- Threat Hunting
- Cyber Threat Intelligence (CTI)
- Cyber Deception
- Security Consulting
- Cyber Security Assessments
- Penetration Testing & Red Teaming

Protect

24/7 Security Operations

Thanks to the use of our Managed XDR and SIEM services, cyber attacks are detected and defended against in a targeted manner. Coping with the constantly changing threat landscape also involves permanently checking vulnerabilities and monitoring potential attack risks. Our cybersecurity specialists uncover changes to your vulnerabilities and misconfigurations at an early stage.

- Managed XDR, SIEM/Vulnerability
- Vulnerability Management
- Digital Risk Exposure Service
- Cloud Security
- Managed Security & Network

Detect & Respond

24/7 Managed Detection & Response (MDR)

Monitoring of your endpoints, identities, networks and cloud environments by our Cyber Defence Center in Switzerland, our own Cyber Defence Platform, experienced experts and established processes as well as the use of leading, AI-based detection & response technology so that you can detect and respond to modern cyber attacks and ensure your ability to act.

- Extended Detection & Response (XDR)
- Endpoint Detection & Response (EDR)
- Identity Detection & Response (IDR)
- Network Detection & Response (NDR)
- Cloud Detection & Response (CDR)
- Security Information & Event Management (SIEM)

Respond & Recover

Incident Response & Recovery

Successful cyber attacks can never be completely ruled out. Quick and professional intervention by recognised experts is crucial. Our own CSIRT (Computer Security Incident Response Team) is at your side around the clock and guarantees you a rapid restoration of your ability to act. InfoGuard is a BSI-qualified APT responder, and a member of FIRST (Forum of Incident Response and Security Teams). It also acts as an incident response partner and claims handler for leading insurance companies and brokers. The Incident Response & Recovery process is seamlessly integrated into every SOC process.

- Incident Response & Recovery
- Incident Response Retainer
- Crisis & Recovery Management
- Negotiation & Legal Support
- Payment Support

Recover

Forensics

If cyber attacks results in a data breach or cyber incident, you need an experienced partner at your side. Our analysts and forensic experts help you to clarify security incidents with forensic analyses while ensuring that you can optimise your cyber security in the long term. We actively take care of securing, analysing and evaluating digital traces and evidence in your entire infrastructure. The analyses and evidence can be used in court.

- Large Scale Forensics
- Network, Computer & Memory Forensics
- OT & IoT Forensics
- Cloud, Mobile & Email Forensics
- Malware Reverse Engineering
- Expert & 2nd Opinion for IR Cases

Prevent & Recover

Crisis & Incident Response Readiness

It's crucial for companies to prepare professionally for a possible security incident. In a joint workshop, we develop emergency operations, crisis management, infrastructure management and recovery as well as a continuous improvement process based on our specially developed and proven templates and our experience from hundreds of cyber incidents.

- IR Readiness Assessment
- IR & Recovery Plan
- IR Table Top Simulation

Securing
Your Digital
World

InfoGuard
SWISS CYBER SECURITY

Your Cyber Security
Our Passion & Expertise

Cyber Defence & Incident Response are crucial, but only two aspects of comprehensive and successful cyber security. Our 360° cyber security approach also includes Cloud Security, Managed Security & Network Solutions for IT, OT and cloud infrastructures, Penetration Testing & Red Teaming as well as Security Consulting Services. We provide our services from the ISO 27001-certified and ISAE 3000 Type 2 audited Cyber Defence Center in Switzerland.

2001
Over 20 Years of Experience and Expertise

100%
Independent

250+
Security Experts

4
Locations in Switzerland, Germany and Austria

24/7
Real-time Monitoring and Emergency Intervention

ISO 27001
ISO 14001
ISAE 3000 Type 2

Swiss Cyber Defence Center CDC

CSIRT
Computer Security Incident Response Team
BSI-qualified APT Response Provider and FIRST Member

Do you have a security incident? We provide you with fast, competent and experienced support at all times.

+41 41 749 19 99

DE +49 896 142 9677

AT +43 1 442 0177

investigations@infoguard.ch

Baar (Head Office)
InfoGuard AG
Lindenstrasse 10
6340 Baar
Switzerland
+41 41 749 19 00
info@infoguard.ch
infoguard.ch

Bern
InfoGuard AG
Stauffacherstrasse 141
3014 Bern
Switzerland
+41 31 556 19 00
info@infoguard.ch
infoguard.ch

Munich
InfoGuard Deutschland GmbH
Landsberger Straße 302
80687 Munich
Germany
+49 896 142 9660
info@infoguard.de
infoguard.de

Vienna
InfoGuard GmbH
Graben 19
1010 Vienna
Austria
+43 1 442 0170
info@infoguard.at
infoguard.at