InfoGuard
SWISS CYBER SECURITY

SECURITY INFORMATION & EVENT MANAGEMENT (SIEM) SERVICE

Your security in the hands of Swiss Cyber Security Experts.

The SIEM (Security Information & Event Management) service forms the cornerstone of InfoGuard SOC services. Thanks to the real-time analyses of information stemming from your infrastructure threats and vulnerabilities in the ICT infrastructure are identified so that they can be selectively eliminated as quickly as possible. At the same time you obtain complete transparency regarding the security status of your ICT infrastructure thus enabling you to increase the security level over the long-term.

- Professional security information & event management provided by dedicated cyber threat analysts
- Monitors your infrastructure around the clock to identify external and internal threats promptly
- Alerts in the event of dangers or disruptions thanks to real-time analyses
- Relieves your IT from having to analyse huge and complex amounts of data
- Continuous refinement of attack scenarios by our pentesters and analysts
- Assists you in adhering to the regulations and compliance requirements
- Weekly reporting and provision of needs-based services at fixed costs

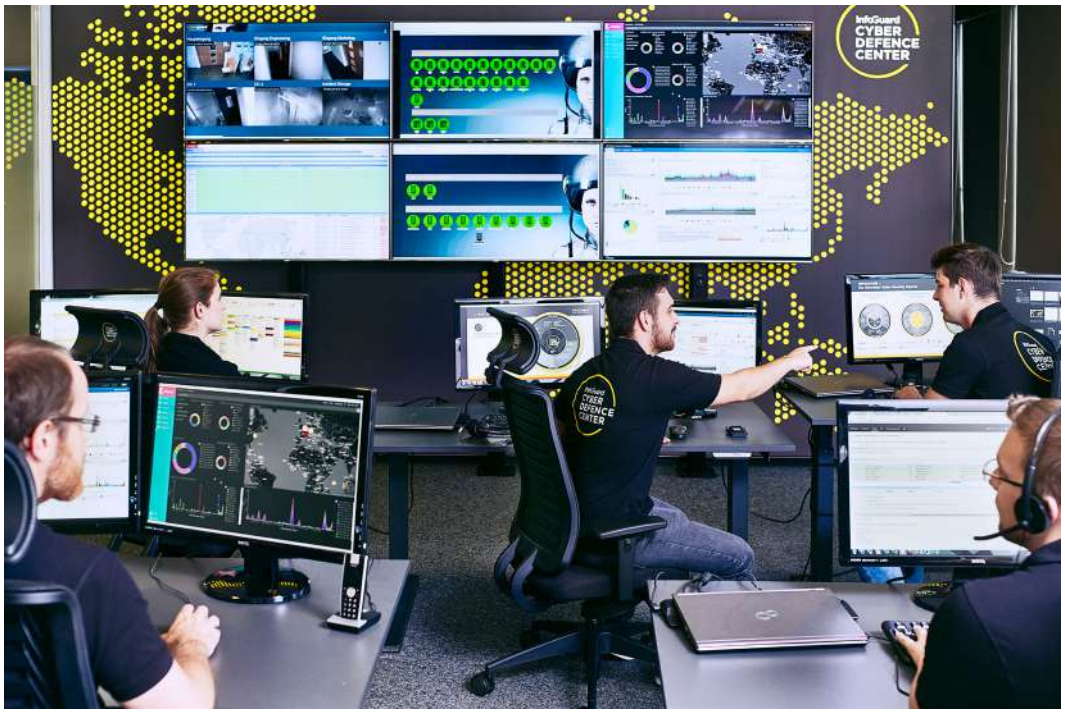
INFOGUARD SIEM SERVICE

Cyber Defence from Switzerland

As part of the SIEM Service InfoGuard's Cyber Defence Center takes over the consolidation and analyses of security-relevant log data for the client and, if requested, the elimination of vulnerabilities. At the same time, InfoGuard experts with their many years of experience in cyber security are at your disposal 24-hours a day. Thanks to in-depth knowledge of the industry, the interdisciplinary skills between offensive and defensive cyber security and extensive experience in penetration testing and ethical hacking we are able to estimate the security threats that apply to a specific company. The location in Zug, georedundancy, a multilevel security concept and the redundant configuration of electrical, network and system components guarantee maximum confidentiality and availability. Connectivity to the customer infrastructure is achieved over redundant site-to-site VPN connections.

Experience and expertise of cyber threat analysts

Our cyber threat analysts monitor the current risk situation daily and analyse information from the darknet, threat intelligence feeds and other sources. They identify and evaluate threats that confront your company, networks, systems, applications and services daily and propose specific measures and recommendations for action before damage is done. Based on current cyber threat intelligence our analysts are always one step ahead thus allowing you to benefit from the latest findings in the detection of cyber threats.



Thanks to standardised incident management processes (e.g. triage, research, documentation) you have the assurance that the quality of the services remains consistently high and that all steps are documented in a manner that can easily be understood. Clearly defined escalation paths from tier 1 analyst to tier 2 up to tier 3 team approach with pentesters make sure that at any point in time the proper resources with the appropriate expertise get involved. All services are organised consistently according to the ITIL processes and embrace preventive, reactive, operative and strategic components. All services are regulated by a „Service Level Agreement“ (SLA).

Our SIEM service includes:

Network and Asset Classification
An important element of the SIEM service is the weighting of assets and networks in terms of their significance for your company. This weighting is essential for the subsequent correlation and escalation of security incidents.

Log data analyses in real time
The SIEM platform is based on IBM QRadar‘s technology. It consolidates log source event data from thousands of endpoints and applications throughout the network and performs immediate normalisation and correlation activities on raw data to reliably identify real threats and minimise the number of false positives. You are provided with access to the SIEM platform via the web-based cyberguard portal and, where the need arises, analyse and evaluate log data in real time yourself.

Threat detection thanks to InfoGuard Use Case Engineering
Apart from the identification of generic anomalies and behaviour InfoGuard‘s Cyber Defence Center detection mechanisms build on self-created threat scenarios, the InfoGuard use cases. In addition to a precise description of the threat and distinguishing characteristics they also include response plans and the approaches to be taken when a situation becomes serious. This will enable a focused and standardised response to the threat to be set in motion. The SIEM service allows you to benefit from the constant development of the use cases by our pentesters and analysts.

Threat Intelligence
The all-embracing logging capabilities of the SIEM platform and the integrated correlation engine assist in the analysis and response to attacks that are not recorded or have been overlooked by other security solutions. Thanks to enrichment with up-to-the-minute threat intelligence data on security threats in the internet new dangers and already infected devices can be identified more quickly and prioritised so that attacks can be prevented or kept to a minimum.

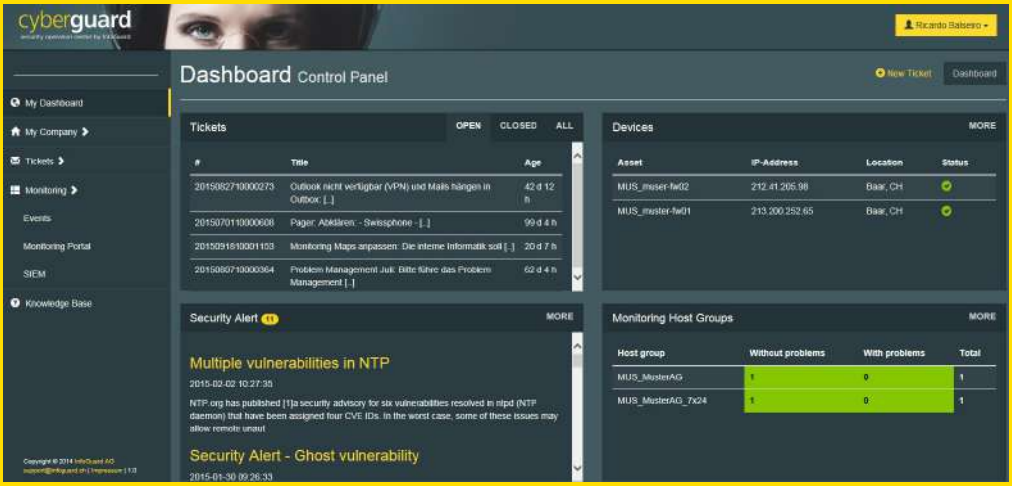
Upgrading the SIEM service:

Vulnerability Management
Vulnerability scans can be configured via the SIEM platform directly and run on your in-house system environment. The combination with our vulnerability management enriches the classified assets with valuable vulnerability information, which can be used to continuously tighten the security procedure and for prioritisation purposes. The identified vulnerabilities are analysed so that the most exposed systems can be protected first and the security policies tailored to provide maximum protection for these vulnerable systems. Moreover, the virtual patch service makes recommendations for the most popular IPS manufacturers. This enables externally accessible infrastructures to be protected at perimeter level until the weakness has been remedied.

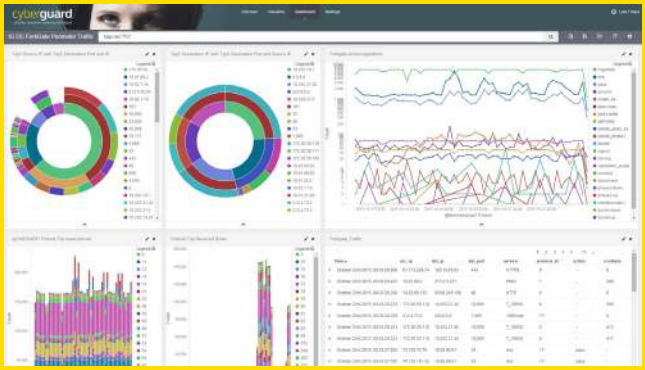
Security Incident Analysis & Response
With the integration of Tanium at the endpoints metadata from processes will be automatically stored for analysis if an attack is detected in the SIEM. Our cyber threat analysts can quickly and efficiently commence with the analysis of an attack and, if requested, perform actions authorised by clients to the endpoints to contain the attack.

MAXIMUM TRANSPARENCY 24 HOURS A DAY

The web-based cyberguard portal provides you with a rapid overview of the actual status of your infrastructure 24 hours a day, all open tickets and the current threat situation. In addition, the history informs you about what has happened over a specific time frame. At the same time you can generate comprehensive reports via the online portal and request adjustments to the service or infrastructure.



Apart from the SIEM Dashboard customer-specific dashboards can be created from log data if required.



InfoGuard's Security Information & Event Management Service guarantees maximum service quality at fixed costs.

Cyber Defence Services – 7x24 from the ISO 27001 certified Swiss SOC

In addition to the SIEM service our ISO 27001 certified InfoGuard Cyber Defence Center in Switzerland manages the entire service spectrum: Starting with support and continuing with outsourced cloud and managed security services up to and including the SOC service, where our cyber threat analysts and security experts look after your security around the clock.

InfoGuard AG
Lindenstrasse 10
6340 Baar / Switzerland
Phone +41 41 749 19 00

Office Bern
Stauffacherstrasse 141
3014 Bern / Switzerland
Phone +41 31 556 19 00

INFOGUARD.CH