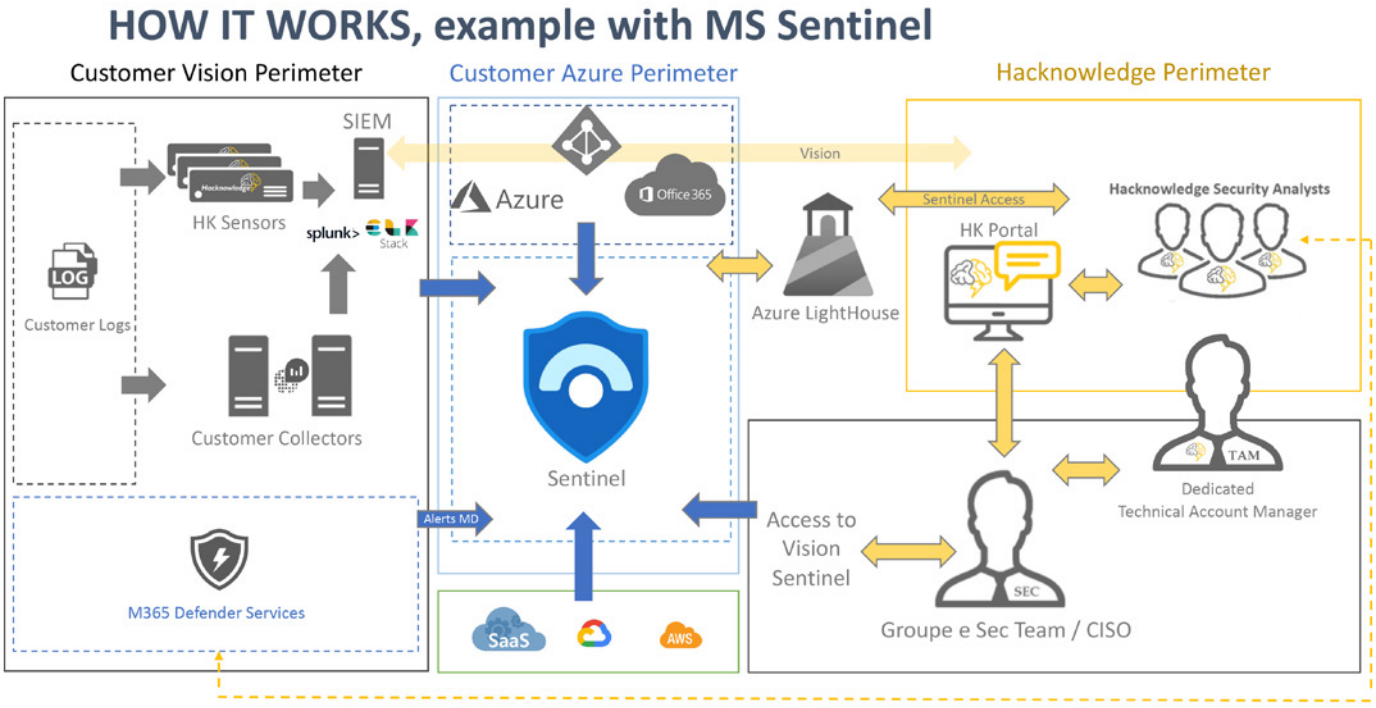
# Cybersecurity monitoring
## Reducing the time between a security breach and its detection

Cybercrime is not science fiction, but a real threat to companies. Affected companies are quickly confronted with ransom demands, production downtimes and expensive repair work. It takes around 100 days on average for an organization to discover a breach or be notified of it. This makes ongoing monitoring of the systems all the more important. The managed service from cybersecurity specialist Hacknowledge aims to reduce this time to the minimum and help customers to take action and prevent any hacking activities in their network.

### Security Operations Center (SOC)

Hacknowledge provides a managed SOC and a managed SIEM (Security Incident and Event Management) to collect the logs if not available. It's an all in one product but very adaptive to the customer's environment. The service is Swiss, simple and efficient. "Swiss" means that the data remains in Switzerland at all times. "Simple" stands for leveraging of the existing IT security environment, and "efficient" emphasizes the service's ability to adapt to the customer's context.



## Your advantages

– Monitoring your infrastructure 24/7: the expert security engineers detect and respond to threats using the cutting-edge VISION Cyber Management™ solutions.

– Reporting qualified security incidents and helping your security team to focus on actionable events: we take over the log handling for you, creating more time to work on the qualified incidents.

– Swiss-based solution: all data is stored in Switzerland, all the engineers work from Switzerland, no cross-border issues relating to confidential or personal data.

– Hacknowledge is ISO 27001-certified (without any exceptions) and GDPR-compliant.

– Vendor-neutral company: you are guaranteed to be supported by an independent service provider.

– The solution is transparent, and you have full access to your data (e.g. logs and security events) at all times.

– The side services cover the full spectrum of cybersecurity, from pentesting to forensics and employee awareness.

## Monitor. Detect. Respond.

1) The first step is to define the perimeter to be covered, both in terms of IT environment and use cases. It's better to start small and grow.

2) Hacknowledge can deploy an SIEM to consolidate and correlate the security logs; if an SIEM is already in place, Hacknowledge should be able to connect to it to deliver the SOC service.

3) Hacknowledge supports the customer in collecting the log and reporting it to the SIEM. Sensors may be helpful to enrich and parse the logs closer to the log source, avoiding noise in the network and optimizing the amount of data sent to the SIEM.

4) Hacknowledge deploys use cases one by one to ensure functional and effective monitoring. We will test the scenarios together and filter false positives.

5) On top of reporting security incidents as soon as necessary, Hacknowledge delivers regular security reports to ensure continuous improvement of the collaboration.

## Adaptive and flexible

Three SIEMs are natively supported by the SOC: SPLUNK, Microsoft Sentinel and Vision (Kibana and ELK stack). Hacknowledge is very adaptive and flexible, enabling the security monitoring to be deployed in your IT and OT environment smoothly and efficiently.

**Post CH Communication Ltd**
**E-Government**
**Wankdorfallee 4**
**3030 Bern**
**Switzerland**

**E-mail egovernment@swisspost.ch**
**swisspost.ch/e-government**