



Cyber Defence: A danger foreseen is a danger avoided

Swisscom has extended its range of Managed Security Services and is now offering comprehensive Threat Detection & Response solutions for corporate customers. This solution enables cyber threats to be identified early on, which means companies can protect themselves accordingly.

The threats to companies and public authorities from malware, hacking or phishing are now common occurrences.

As a network operator and experienced security specialist, Swisscom identifies and blocks millions of malware attacks and around 2,250 phishing attacks each month. While in the past the attacks were the work of bored teenagers, nowadays professional cyber criminals are behind them. Their attacks have achieved a new quality and also quantity.

There is often fire, even when there's no smoke

With the Internet of Things, increasing levels of artificial intelligence and cloud applications, a whole new world of opportunities are opening up for cyber criminals to damage companies. Hackers are able to take control of everyday networked objects, use them to build bot nets and then start DDoS attacks (Distributed Denial of Service) and the like. The attackers are also being more silent, and can remain unnoticed for months or even years, enabling them to cause a huge amount of damage. And the insidious thing is that you don't fight what you can't see or feel. This is why it's important to identify the work of cyber criminals as early as possible (detection) and intervene professionally (response).

Ready for the next generation of cyber attacks

The only thing that can help against these cyber threats is prevention, early detection and, in a worst case scenario, taking action with the help of professionals. Swisscom is now offering its customers comprehensive Threat Detection & Response solutions. Swisscom has been operating a 24x7 security operation centre for corporate customers in Zurich for around 7 years now, and has its own Computer Security Incident Response Team (CSIRT). The many years of expertise is now being utilised in the new Threat Detection & Response solution, which is available in four modular service versions:

1. Security Analytics as a Service

Companies receive an overview of potential security incidents from defined log files using the Security Dashboard. The customer thus receives the security analytics infrastructure as a service. The analysis and reaction to security incidents are handled by the companies themselves.



2. Security Operation Centre as a service

In addition to Security Analytics as a service, Swisscom also takes care of the security process services. Experienced security specialists analyse potential and confirmed security incidents on a 24x7 basis, interpret these and then provide the companies with specific recommendations for action.

3. Computer Security Incident Response Team as a Service

To be able to handle critical security incidents, support is obtained from experienced Swisscom security experts. These specialists use established tools and processes to trigger the Security Incident Management process and then handle this.

4. Threat Intelligence as a Service

Swisscom experts provide proactive information on the existence of sensitive business and personal information of a company in public and private networks (e.g. Darknet). As a result of this, customers receive unique information in a very timely manner, which may be a sign of leaks within the company.

Cyrill Peter, Head of Product Management Enterprise Network & Security at Swisscom Enterprise Customers, says: "We have noticed that the attackers are becoming increasingly professional and also working on a more industrial scale. And we are able to thwart these like no other: On the one hand, our network know-how enables us to see anomalies and potential attacks immediately and, on the other, the knowledge we gain from attacks flows automatically into our Threat Detection & Response services. Our customers benefit from our our unique swarm intelligence, which is unique in Switzerland".

Berne, 26 September 2017

More on Threat Detection & Response: <https://www.swisscom.ch/detection>