Threats. Mastered. – New and highly modern Cyber Defense Center

All companies are faced with complex cyber security challenges:

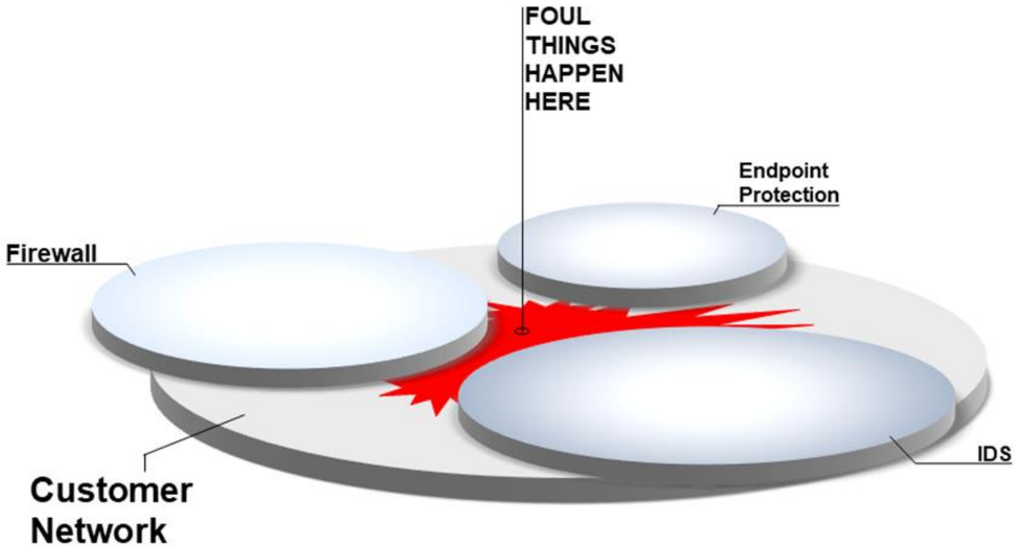
- **How can modern, targeted attack scenarios be identified?**
- **How is a correlation generated by events or chain of events?**
- **How can the risk potential be assessed?**
- **How to obtain applicable guidance on the treatment of risks?**
- **How can be checked whether improvements have been successful?**
- **How is an efficient flow of information organized for all stakeholders?**
- **How is risk transparency ensured from IT to business risk?**
- **How can IT security costs be saved?**

The Digital change and progress is the driving force behind the fact that more and more critical processes are being made electronically and via the Internet. The targets for cyber attackers become every day more lucrative and the possibilities are more varied and sophisticated.

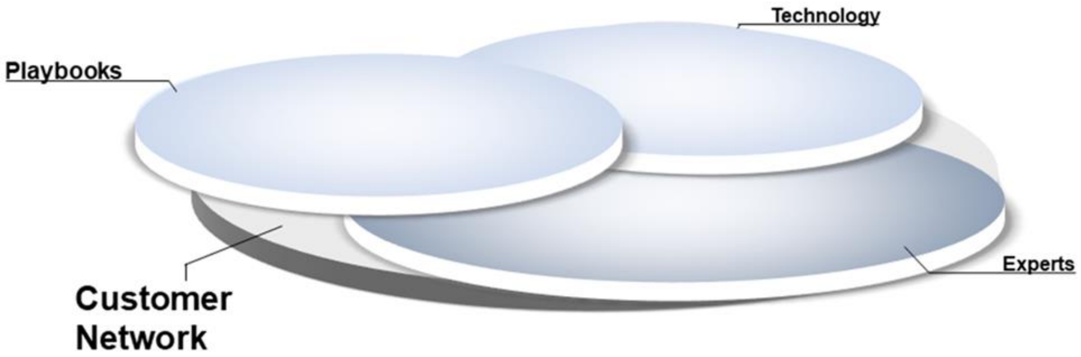
Due to the increasing complexity of IT, the growing threats and the lack of experts, it is nowadays hardly possible to protect itself against all attacks. Cyber attacks are quiet, complex and more and more often tailor-made. Prevention alone does not help anymore. To exist in the uncertain digital world requires the permanent search and the active identification of dangers.

It is of increasing importance to recognize when an attack on the company is successful. For this, experts are needed, who search for traces, based on modern analytical tools, in a methodical and structured way, clarify suspicious moments and act actively in the case of dangers.

What the past shows is that technology alone is not enough. Because the attackers adapt their attacks and move between the technologies undetected.



In addition to the use of state-of-the-art technology, a perfectly coordinated machinery of technologies, security experts and efficient processes is needed to secure these blind spots. The sustainability of existing technologies is thereby preserved and supported.



ISPIN AG with its Cyber Defense Service has put together a complete package that confronts these challenges.

- **Technologies:** State-of-the-art multi-stage detection modules include Advanced Correlation and Risk Detection.
- **Experts:** A well-established international expert team is available to our customers.
- **Playbooks:** Experienced and lived procedures, with know-how feedback loop back into the service.

We now offer to our customers a first-class, **Next Generation Managed Cyber Defense Service**, which is based in Switzerland. All the qualities are combined to provide you with comprehensive detection, analysis and response to cyber attacks. **The solution is designed for targeted and modern attack scenarios**.

The use of **state-of-the-art technology** allows for an **all-around visibility** of your digital infrastructure. The resulting insight maximizes the correlatability of the existing data and our team can use it to create far-reaching **chain of events**. Through **automation**, we ensure that a human must only intervene if a critical or decisive decision must be taken. Our used **fabric** integrates existing platforms. Thereby supports and ensures the sustainability of the existing technology.

When a threat is detected, an alert will be sent to **your experts**. Our Cyber Threat experts will then support and provide you with know-how and procedures to clean up the threat when necessary.

It has long been clear that it is only about when and how violently a cyber attack will take place. To always be prepared for all eventualities, it must be ensured that all data are consistently stored. In addition, we achieve **perfection in the depth of the analysis** and **a complete cover in the event range**.

The Cyber Defense Service can either be integrated into existing ITIL organizations as a **stand-alone service** or as a **fully integrated solution**, together with the ISPIN Cyber Care, Cyber Guard. We call this the **"fusion"** concept.

Your company benefits from this **synergy** and can obtain this service at a price and in a quality, which is on the market.

All use cases can be assigned to your business risk, giving you a **measurable risk transparency**.

Swiss Class and the sensitive data remain with the customer

A consistently developed architecture ensures that the sensitive data of the customer never leaves his company. Thus, compliance with many Swiss and international regulations is guaranteed (for example: **FINMA**, **PCI-DSS**, **GDPR**).