arco
IT SECURITY SERVICES

Detection and Response

Threats to IT environments often occur on weekends and public holidays, when attackers assume that systems are left unsupervised. Thus, the earlier security issues can be identified – through continuous logging, 24/7 monitoring, and a rapid response team – the quicker you can get back to business as usual.

At Arco IT, we want you to be able to sleep easy, knowing that your systems are being monitored 365 days a year and incidents are immediately addressed. To protect your business, your security monitoring needs to be high-performing and high-responding.

That's why we've partnered with an international expert to provide a powerful Security Operations Center (SOC) that seamlessly integrates into your on-premise and cloud-based systems to constantly monitor for potential threats and take action in case of security issues.

A 3-STEP PROCESS

Through our rigorous and thorough process, security threats will have no place to hide.

1. MONITOR

We integrate your systems (e.g. Endpoints, Servers, Active Directory, Firewalls, Networks, Microsoft Office 365, Cloud Resources, etc.) with a customizable and proven detection platform that monitors your system around the clock with AI-based detection logic.

2. ANALYZE

A team of dedicated security analysts contextualize the information and triage the events.

3. RESPOND

When an attack is detected, we ensure that the issue is resolved, no matter what. Guided by pre-agreed playbooks and years of practical experience, we work independently or hand- in- hand with your IT department and suppliers to contain the threat and recover your systems as soon as possible.

WHAT YOU CAN EXPECT

We'll make sure that monitoring your systems and responding to threats is hassle- and headache- free. In addition to a SOC, you'll have support from a trained international Incident Response Team, skilled at analyzing and responding to issues, alongside a strong local team in Switzerland. Take comfort in working with a partner you know and trust, while enjoying the confidence that comes with knowing your IT environment is in safe hands.

YOU BENEFIT FROM:

- ✔ Proactive, end-to-end protection against internal and external issues
- ✔ Live dashboards and regular reports about the status of your systems
- ✔ Platform customization for infrastructure or critical application monitoring requirements
- ✔ Affordable, pay-as-you-go solution for quick and flexible deployment
- ✔ Recommendations for continuous security setup improvements based on industry standards (e.g. MITRE ATT&CK framework), by analyzing incidents and current developments in the global threat landscape

arco Albulastrasse 34, 8048 Zürich 044 244 02 20 info@arco-it.ch www.arco-it.ch