SOC-as-a-Service - organization security as a service

Dawid Jankowski

Security Operations Center

Every company, regardless of its size, should prioritize the security of data and systems. Clients always rely on the confidentiality of sensitive data, contracts, and any other information that could be harmful if disclosed. A data breach can have catastrophic consequences both in terms of reputation and finances. It can lead to loss of credibility, contracts, production disruptions, and potential bankruptcy.

Since the outbreak of the COVID-19 pandemic, when most companies transitioned to remote work, cyberattacks have significantly intensified. According to purplesec.us, this increase is estimated at 600%, with annual losses from cyberattacks reaching 6 trillion USD. Moreover, this trend continues to accelerate, and is expected to double by 2025. Ransomware attacks (encrypting computer systems and demanding ransom for data recovery) alone are approximately 57 times more damaging than in 2015. Small and medium-sized enterprises are the most frequent targets due to the lack or insufficient security measures.

Effective defense against attacks requires the establishment of a Security Operations Center (SOC). It consists of cybersecurity experts who continuously monitor the organization's IT environment, update attack signatures and defense systems, and stay aware of new attack possibilities and trends.

What exactly SOC-a-a-Service is?

Creating your own SOC team is not only time-consuming but also costly. The constant competition for top IT specialists and ongoing training require significant investments. Thanks to modern cloud-based solutions, an excellent remedy to this problem has emerged in the market. SOC-as-a-Service is a service that acts as support in detecting and responding to threats targeted at the enterprise. The client's systems are secured by experts who continuously update their knowledge in the field of cybersecurity.

Why choose SOC-as-a-Service instead of building your own SOC team?

SOC-as-a-Service is a natural evolution in the realm of company cybersecurity. It is a response to the increasing risks associated with attacks on small and medium-sized enterprises.

There are four main areas of benefits associated with SOCaaS solutions:

1. **Significantly reduced risk of attack:** We have cybersecurity experts in our corner who continuously monitor security systems, greatly minimizing the risk of data breaches or production disruptions.

2. **Faster detection and preventive actions:** Time plays a crucial role during an attack. For instance, when a machine is infected, it needs to be immediately isolated from the rest, and when a user account is compromised, the password needs to be reset promptly. Professional SOC teams have proven predefined automations for rapid and precise response to cyber threats. Production can be restored so quickly that users won't even notice any interruption in service.

3. **Scalability:** As your company grows, SOCaaS grows with it. Experienced SOCaaS partners and providers can easily double SOC resources without any issues. These companies have a vast number of experts ready to work 24/7.

4. **Cost-effectiveness:** SOCaaS eliminates the need for maintaining an in-house unit, including staff, continuous training, office space, equipment, and licenses. For example, to ensure 24/7 monitoring, a small team is required, but the actual workload may be much less. SOCaaS providers have specialists who work more efficiently by dividing their time between different projects. It is estimated that SOCaaS can cost up to 90% less than a traditional in-house SOC unit.

Therefore, it is crucial to ask ourselves whether our defense systems are keeping pace with the increasing number of attacks each year, or even surpassing them.

Critical tools for the SOC team

The market for cybersecurity is progressing at an unprecedented pace. The expanding spectrum of threats, the shift to hybrid work environments, and increased reliance on cloud services have broadened the possibilities of attacks on organizations, requiring constant protection and monitoring. It is essential to realize that in the field of cybersecurity, there is no one-size-fits-all solution to all threats. However, experienced service providers in this field can effectively seek the best solutions. The post-pandemic reality and ongoing warfare necessitate a shift towards more proactive and advanced strategies for threat detection and response. Effective future-proof protection requires action to be taken today.