Atea XDR Service

Atea XDR service enables the customer to proactively and continuously develop their security posture and reduce the attack surface together with Atea's information security experts. The service ensures that XDR components and their integrations are optimally configured.

By implementing Atea XDR service, you can minimize the amount of information security incidents through continuous proactive development and take the full advantage of modern defense capabilities. It also helps you to maximize the return on investment (ROI) of the acquired technology.

This service offers you Atea's trusted cybersecurity experts who will proactively help you to develop your complex security environment.

Atea experts will proactively optimize Microsoft Security tooling capabilities and integrate new features as Microsoft Security Ecosystem evolves. Reducing the operational complexity will also lead to cost savings.

With increased visibility we can strengthen your Security Posture and Secure Score, hence offer you a better understanding of your security landscape.

Weekly communication ensures that you are aware what kind of actions has been made to prevent well-know and current threat campaigns and how your Security Posture is strengthened.

As a prerequisite you have Microsoft M365 E3+E5 Security, A5, or E5 licenses and Microsoft Sentinel in use.

This service is not a reactive SOC (Security Operations Center) service, and service is delivered on business days, 8:00-16:00.

Contact Atea sales to get a more detailed presentation about the service and its benefits to your organization.

Service delivery model

Agreement

Kick-off meeting

- Stakeholders
- Communication plan
- Service goals
- Access and credentials

Rollout and QA phase

- Tasks based on RACI -model
- Access verification
- Playbooks verification

Production phase

- Service delivery
- Weekly customer communication
- Monthly meeting and report
- Documentation and change management

Pricing

- Fixed monthly cost based on your end user count

Atea XDR service is based on Microsoft Security Ecosystem components.

ATEA