SECURITY SERVICES

MDR for Microsoft Sentinel

THE DIGITAL WORLD HAS CHANGED.

Cybercrime getting more sophisticated

The rise in the sophistication of cyber threats require organizations to take additional steps. Not only has the volume and extent of these attacks increased, also the speed at which attacks unfold has gone up significantly. From initial access to lateral movement to exfiltration, attacks can happen in a very short length of time, leaving a relatively little window of opportunity for defenders to step in and take remediating actions.

Leverage existing investments

Numerous organizations face limitations in terms of budget, resources, expertise, or the desire to establish and operate an in-house Security Operations Centre (SOC). Despite these challenges, their senior leaders recognize the ongoing necessity of round-the-clock protection against persistent threats. As a result, they must seek alternative methods for identifying and responding to cyber incidents that could jeopardize both their own operations and the safety of their customers, regardless of the time of day or night.

Our solution

Cegeka provides a Managed Detection and Response (MDR) service with Microsoft Sentinel, covering all enterprise environments including hybrid and multi-cloud.

We leverage your existing Microsoft Sentinel to provide our SOC analysts visibility of the complete environment to detect the threats of tomorrow. We do this by correlating and analyzing a wide range of data sources in real-time, including network activity, user behavior, endpoint data, and various IT and security logs. By aggregating diverse data streams and leveraging up-to-date threat intelligence, we swiftly detect and respond to security incidents.

Key benefits

Broad 24x7 Detection

Gain a broad visibility of your hybrid and multi-cloud environments by levereging Microsoft Sentinel. Our experienced SOC analysts will continously monitor 24x7 looking for any threats.

Respond & recover as far as needed

Because every second counts, we take action to contain the threat with automated threat response according to what is desired.

Resillience & transparacy

Our Cyber Security Advisors provide guidance on improving your Security Posture. Combined with Horizon this will give a continuous view on how everything is evolving

DETECTION

Advanced Threat Intel
Using Industry-leading threat intel to detect real-time threats in your Microsoft Sentinel environment

Threat hunting
Intel-based Threat Hunting to detect attacks which bypassed existing defenses

24x7 Security Monitoring
Our SOC analysts will 24x7 continuously monitoring the Microsoft Sentinel and perform investigations to uncover Security Incidents

RESPONSE

Threat response
Off the shelve response actions which we will take upon approval or fully automated

CSIRT Services
Provide assistance for digital forencics, compromise assess or red teaming assements.

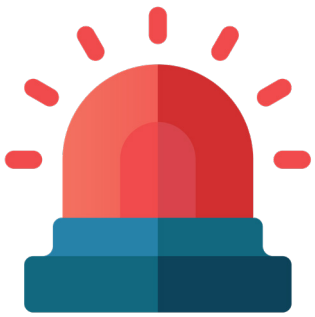
RESILIENCE & RECOVERY

Service management
Monthly security service meetings to see what has happened and what the evolution is.

Cyber Security Advisory
Our Cyber Security Advisor will provide actionable resilience improvement to strengthen the security posture.

Why use Microsoft Sentinel?

- Powered by Cloud-native technology
- Integrations with Microsoft 365 Defender and various other technologies.
- Visbility across all enterprise environments
- Industry recognitions: Forrester Wave & Gartner Magic Quadrants



Why combine Cegeka & Microsoft Sentinel

We help you with:

- **Set up and configure** Microsoft Sentinel
- **Privacy** as you own your data
- **24x7 Managed Detection & Response** service
- **Threat Response** to contain Security Incidents
- Working with **Certified Microsoft experts**
- **Monthly Security meetings** to improve resilience
- **End-to-end Security response services**, fully integrated with other infrastructure solutions.

Microsoft cegeka

READ MORE ABOUT OUR SOLUTIONS