cipher
a PROSEGUR company

MDR

(Managed Detection and Response)

MDR (Managed Detection and Response)

Cipher presents an MDR solution, remotely addressing the cybersecurity needs of organizations. Composed endpoint protection solutions, mail protection (antivirus, antimalware, phishing), protection of IoT/OT and SIEM/SOAR environments.
It proposes the implementation of a cybersecurity platform designed to help companies prevent, detect, investigate, and respond to advanced threats.

This Cybersecurity platform would initially support two key pillars:

- Secure remote work
- Endpoint protection

This platform would be managed at the service level by Cipher based on the most innovative technology from Microsoft and adapted to the needs of organizations.

Secure remote work

With Microsoft's Cloud security tools, we would support organizations to secure their infrastructures and their collaborative work tools. Implemented access control and information protection measures backed by Microsoft AI. This reduces the risks of security breaches and protects the privacy of users and organizations as much as possible. Advanced security and device management help sustain rapid customer growth and navigate change so businesses of all types can remain protected with minimal complexity.
With this solution, you get among others:

- Protection against lost or stolen passwords by using an extra layer of security through Multi Factor authentication
- Providing the right people with the right access to professional applications
- Enable secure access to virtual remote desktop

Because employees work from multiple locations and use personal and organization-owned devices, you need a way to manage and protect these devices and the work data on them.

End-point protection

The solution will include the following key elements:

- Behavior sensors on endpoints: These sensors collect and process operating system behavior signals and send this sensor data to a private, isolated, cloud instance.
- Cloud Security Analytics: Leverage the vast amount of data, device learning and unique cloud optics, enterprise cloud products and online assets, behavioral signals that translate into insights, detections, and recommended responses to advanced threats.
- Threat intelligence: Threat intelligence should make it possible to identify attacker tools, techniques, and procedures and generate alerts when viewed in collected sensor data.

With the service the organization will obtain:

- Vulnerability and threat management

    - Real-time detection
    - Intelligence-based prioritization
    - Smooth correction
- Reduction of the attack surface
- EDR
- Automated investigation and remediation
- Security score for devices and users

The service

This service will have the following characteristics:

- Deployment of the sensor on supported endpoints.
- 24x7 Alert Monitoring and Response from Cipher SOCs
- Manual Search of Threats and Enrichment with Cyber intelligence included.