MDE SOC

Proactive monitoring on the MDE platform

VARGROUP

YARIX
a vargroup company

MDE SOC

The Security Operation Center (SOC) is a service, operating twenty-four hours a day, seven days a week: Yarix guarantees the physical, on-site availability of competent technicians at all times. The SOC service makes it possible to:
- Detect, from the first signs, cyber attacks that may compromise the continuity and/or security of the Customer's assets
- Counter the dangerousness of these attacks, through actions to be agreed with the Customer: direct intervention by Yarix or simple reporting to the Customer's IT Security.

The main components of the service are listed below:

Event Management - This is the main process of the SOC Service related to the monitoring and management of security events. The core of this process concerns the first classification of security events, which, starting from the identification on the consoles of the technology platforms used, will direct all subsequent actions.

Incident Handling - SOC services defined as "baseline" are complemented by "advanced" SOC services in "on-demand" mode, i.e., exclusively at the explicit request of the Customer. From this point of view with its CERT that also includes the Incident Response (YIR) team, Yarix is able to address the following activities:

- **Incident Response** - when there is a level of compromise affecting a specific system or set of IT systems of the Customer, it becomes necessary to declare that an Information Security Incident is in progress a unit of the Incident Response Team will be involved, which remotely and/or on-site will support the Customer's internal IT Managers in all phases of incident management.
- **Forensic Analysis** - Computer/Mobile Forensics activities involve the acquisition, preservation, data extraction, analysis and presentation of evidence reconstructed and/or recovered from storage systems such as hard drives, external storage devices or from mobile devices.
- **Malware Analysis** - in the case of an IT incident related to a malicious vector of unknown nature this service may be activated, which offers the advantage of a clear understanding about the consequences of activating malicious software in one's systems, through phases of:
  - Static analysis,
  - Dynamic or behavioral analysis.

Phase I: Scope analysis

The scope consists of the set of Client assets to be protected, both physical (hardware) and intellectual (software and information). The first phase will identify critical assets and business processes that require special attention and the activation of specific controls to detect potentially blocking security anomalies.

Phase II: Definition of the working group

This phase involves the definition of both the Yarix project team and the Client's business figures in charge of managing the SOC activation project. The figures who will intervene on the Yarix side in the service implementation phase will include:
- SOC Manager: manager of the SOC service
- Service Manager: point of reference for the customer during service delivery
- Technology Specialist Team: supports the customer in the initial deployment phase of the technologies used. It also manages the customization and tuning of the platforms.

Phase III: Definition of the technical solution

The technical solution that Yarix proposes is based on the implementation of technologies useful for detecting threats and security events, in this specific case on the Microsoft Defender for Endpoint solution.

The benefits brought by this solution are many:
- Threat and vulnerability management
- Reduction of the attack surface
- Next-generation protection
- Detection and response from endpoints
- Automated investigation and remediation
- Microsoft Secure Score for devices

Tracking of security-related events is done through a ticketing platform.

Phase IV: The security monitoring service

Yarix technicians are physically present on site twenty-four hours a day, seven days a week: the service is therefore guaranteed H24. Monitoring involves checking for anomalies detected by the technologies installed at the Customer's perimeter (in order to discard any false positives) and triggering procedures aimed at managing them.

VAR GROUP
Var Group is fully owned by Gruppo Sesa S.p.A., a leading Italian Group in the field of value-added IT solutions for business segment. The parent company Sesa S.p.A. is listed on the STAR segment of the MTA market of the Italian Stock Exchange.

YARIX
Yarix is the leading company in Var Group's Digital Security division and one of the most recognized, innovative and authoritative Italian companies in the IT security sector. It has one of the most advanced Cognitive Security Operation Center in Italy and benefits from teams of people specialized in defensive and offensive security, Cyber Threat Intelligence, Incident Response.

VARGROUP YARIX a vargroup company