LE NOSTRE SOLUZIONI

XDR e MDR

XDR - eXtended Detection and Response
Detect threats through integrated monitoring of IT systems.

"XDR" or "eXtended Detection and Response" is an advanced cybersecurity solution designed to elevate the detection and response capabilities against cybersecurity threats beyond traditional endpoint security measures. XDR systems are engineered to provide comprehensive threat detection and response by amalgamating tools and data from multiple sources, encompassing endpoints (such as computers and mobile devices), networks, applications, and the cloud. Leveraging advanced analytics and artificial intelligence, XDR identifies suspicious behaviors and threats in real-time, empowering organizations to mount more efficient responses to cyberattacks. These proactive systems offer unified visibility across various attack vectors and present consolidated dashboards for comprehensive analysis. XDR solutions facilitate data analysis, malicious behavior detection, attack identification, and automated protective actions.

Key Elements of XDR

Advanced detection
Utilizes behavioral analysis and correlation techniques.

Broadened scope
Monitors the entire it infrastructure beyond endpoints.

Integration
Aggregates data from diverse sources for a holistic threat perspective.

Automation
Streamlines threat response to minimize reaction times.

In-depth analysis
Furnishes detailed threat analysis and insights into attackers' methodologies.

MDR - XDR

MDR (Managed Detection and Response) serves as an alternative to an internal Security Operations Center (SOC), offering continuous 24/7 network monitoring and human security analyst-driven security incident detection. Particularly beneficial for organizations initiating the construction of their security infrastructure, MDR typically presents a cost-effective solution with rapid activation. Both MDR and XDR assist security teams in navigating limited resources amid escalating threats, albeit through distinct approaches:

- MDR collaborates with the internal security team, providing SOC as a service that might encompass an XDR solution managed by MDR personnel.
- XDR automates security tasks and augments analyst efficiency, enhancing incident response effectiveness within organizations possessing an internal SOC.