In our previous two parts of this blog series, we got to know about managed SOC and XDR along with their features and challenges. This third part of the series focuses on why your SOC requires an XDR solution to boost the effectiveness of your managed SOC.

Why Choose Managed XDR For Managed SOC?

The SOC challenges that businesses are dealing with are tough to resolve. Managed XDR confronts these issues, including the growing security management complexity, rising analyst pay, security engineering, and management outsourcing expenses with its capabilities.

Managed XDR is the next level of security detection and response capabilities. It assists in boosting your SOC by:

- Enhance detection
- Improve Prioritization
- Advance Investigations
- Accelerate Response

Managed XDR is a proven solution that liberates analysts to focus on what counts, allowing them to get the most out of their existing security investments.

Therefore, most organizations are searching for the best extended detection and response (XDRs) and security automation capabilities to minimize security engineering costs, increase SOC performance & results, and boost employee morale. And Rewterz's Managed XDR is your answer to all security concerns and requirements.

Why Go For Rewterz Managed XDR?

Our Managed XDR improves the efficiency of the SOC by modifying the nature and cycle of alerts that reach it.

Also,

- Rewterz Managed XDR accelerates and enhances incident response and the Security Operations Center (SOC).
- Rewterz Managed XDR combines incident response methodologies with advanced context from security components.
- Rewterz Managed XDR response with more advanced methods than typical infrastructure control points such as networks and terminals.
- Rewterz Managed XDR detects complex threats automatically and with minimum adjustment.
- Rewterz Managed XDR automates repetitive procedures and saves analysts time.
- Rewterz Managed XDR offers a centralized workflow and management for all analyst tiers.

Rewterz's SOC

Our SOC evaluates an organization's networks and environment for vulnerabilities and liabilities and our remediation and incidence response plans provide a highly methodological and comprehensive solution to the detected vulnerabilities. This can expedite your organization's growth process, enabling them to focus on their core competencies while enjoying the benefits of having the most sophisticated engineering expertise on the cybersecurity front.