Managed XDR — A quick rundown:

We saw a basic outline of what a security operations center (SOC) is and the challenges of SOC teams in the first part of this blog series. In this part, we'll take a look at the XDR solution and how this solution fills the gap or cover the pitfalls of SOC.

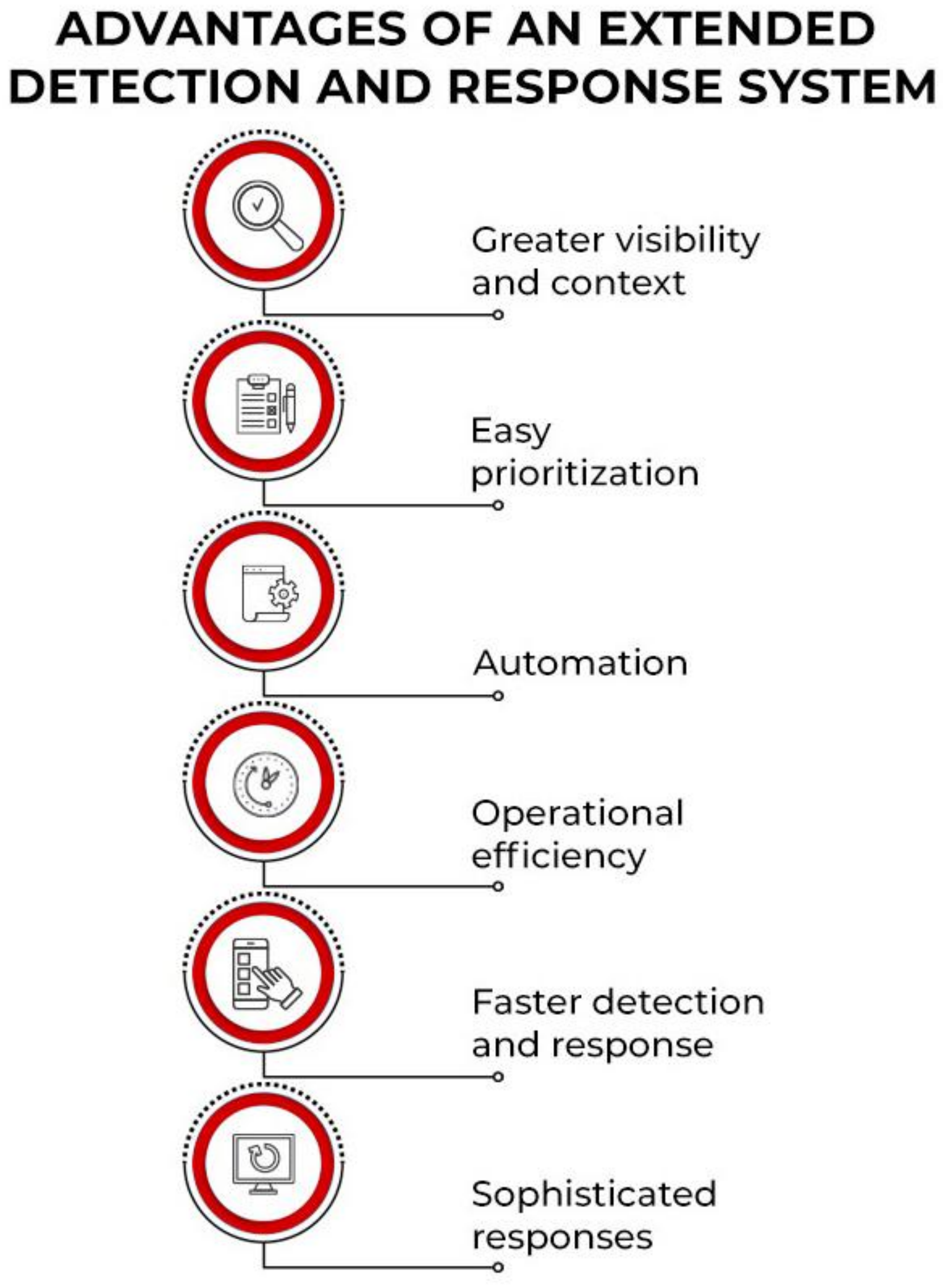
Managed XDR extends Managed Detection & Response (MDR) services throughout the organization to provide a fully managed solution that encompasses security analytics and operations, enhanced threat hunting, detection, and quick response across endpoint, network, and cloud environments.

XDR: a new & mature shape to security

The XDR platform significantly enhances your cybersecurity posture while also assisting you in maximizing the return on your security efforts.

It provides improved prevention capabilities, effective response, granular visibility, and better productivity. XDR assists security teams in the following ways:

- Identify complex or hidden threats
- Track threats across multiple system components
- Enhance detection and response rate
- Analyze threats more effectively and efficiently


ADVANTAGES OF AN EXTENDED DETECTION AND RESPONSE SYSTEM
Greater visibility and context
Easy prioritization
Automation
Operational efficiency
Faster detection and response
Sophisticated responses

Features Of an XDR

1. Dashboard

The Managed XDR provides a central dashboard that displays a prioritized list of suspicious activities and susceptible setups that need to be addressed immediately. The prioritized list allows administrators to focus on the most serious concerns and spend less time researching low-risk incidents. Suspicious actions are rated according to their seriousness. The timing of the event, related processes, executed command lines, file hashes, device, user, and more are all visible on the dashboard. Dashboards are beneficial because they make it simple to take additional action when diving into the specifics of a suspicious item by providing a context-aware list of further inquiry alternatives and rapid measures. A single-pane-of-glass view to all analytics also reduces the screen fatigue in analysts that arises from switching between multiple software and windows.

1. Automation

The Managed XDR solution provides SOC with automated and orchestrated malware prevention, threat detection, and response. It uses automated correlation and machine learning to reveal malicious behaviors that are difficult to detect, saving security staff time when spotting possible issues and detecting the full of an attack chain. Automated playbooks make manual labor obsolete as the menial tasks and alerts are generated automatically to make the life of analysts easier.

1. Mean Time

Managed XDR gives insight into Indicators of Compromise (IOCs) and breaches, allowing organizations to detect more subtle signals of a potential compromise sooner, without wasting time triaging alerts or investigating false positives. This enables security teams to minimize their average response time and reduce the mean time to respond (MTTR).

1. Threat Intelligence

Managed XDR delivers the comprehensive context required for an attack-centric view of an entire chain of events across security layers by leveraging powerful analytics and threat intelligence.

It combines network visibility and data analytics throughout the whole network infrastructure of a company. It provides the context needed for analysts to discover advanced threats on the network.

Companies can improve SOC performance and boost their capacity to discover and attack the worst of the worst threat actors with XDR’s combination of threat intelligence, automation, and machine learning.

1. Remediation

Managed XDR also offers consolidated and efficient incident response and remediation capabilities across the corporate network’s environments. This enables security analysts to respond quickly and effectively to mass attacks against the company, lowering the total impact and expense of the incident. It offers 24×7 alert monitoring, investigation, remediation, and response backed by resources and expertise.

Part 3 coming next week: Why Choose Managed XDR For Managed SOC?