BYTES

AN ESSENTIAL GUIDE TO XDR

CONTENTS

DEFINING XDR

Extended Detection and Response (XDR) is a consolidation of tools and data that provides extended visibility, analysis, and response capabilities across endpoints, workloads, users, and networks.

GARTNER DEFINES XDR AS ‘A SECURITY SOLUTION THAT UNIFIES MULTIPLE SECURITY TECHNOLOGIES INTO A SINGLE PLATFORM, PROVIDING GREATER VISIBILITY AND CONTROL OVER THREATS’.

XDR THE ANSWER TO MODERN ATTACKS

To tackle the nature of modern attacks crossing multiple domains and close security gaps, security teams need a unified solution that allows them to detect and respond to threats more efficiently across an organisation’s entire digital estate.

Using powerful intelligence that automates the correlation and analysis of data, as well as response actions, XDR can help the Security Operations Center (SOC) transition from a reactive approach to a proactive defense strategy, while improving threat detection, response times, and most importantly freeing up time for the SOC analysts to focus on proactive hunting and prevention.

Extended Detection and Response (XDR) solutions are designed to deliver a holistic, simplified, and efficient approach to protect organisations against advanced attacks. They give SOC teams a more complete view of the cyber kill chain for more effective investigation and provide auto remediation across multiple domains using vast sets of intelligence and built-in artificial intelligence (AI).

XDR VS EDR

XDR

- Holistic security and signal correlation across multiple risk vectors - often including identity, email, endpoint, and cloud app and data loss prevention (DLP) security.
- Incident-based investigation and response experience
- Protects against advanced attacks such as ransomware and business email compromise

EDR

- Endpoint device and user security
- Siloed endpoint alerts
- Helps fend off endpoint-specific attacks
- Lacks wider context surrounding advanced attacks

KEY BENEFITS

- Advanced kill chain visibility and protection
- Unified investigation and response
- Automation
- Broad intelligence and threat vector visibility
- Optimised total cost of ownership

KEY CONSIDERATIONS

Existing Tools

What tooling do you have in place already?

Do you require Log Managmeent Capabilities as part of your XDR strategy?

Alignment to Microsoft

Do you have access to Microsoft Security Solutions (Defender, Azure Sentinel)?

Preferred Commercial Model

User, Device or Data Volume based Commerical models?

Adoption

Internally Managed, or supported by an Expert 24/7 Service Provider?

SUMMARY

XDR pro-actively identifies incidents and threats across the environment and collates related occurrences, optimising the number of security alerts and allowing security teams to understand a cyberattack more clearly. XDR powerfully automates analysis of correlated incidents, facilitating quick and efficient response and remediation.

MANAGED XDR SERVICES

What it Means

Managed XDR provides your organisation with 24/7 access to human expertise for the purposes of threat hunting and incident management. Combined with world-leading AI & Automation technologies, Managed XDR delivers value through rapid detection, response and remediation of cyber incidents.

Key Benefits

- Coverage & context beyond the endpoints
- 24/7 coverage of your business's full IT ecosystem
- Actionable cyber threat intelligence (CTI)
- Reduced total cost of ownership
- Expert prioritisation of cybersecurity alerts and notifications

Keen to Learn More?

Reach out to your dedicated Bytes Account Manager to find out more about Bytes' Managed XDR services.

XDR VIRTUAL EVENT

Are you ready to transform your Cyber Threat Detection & Response Strategy?

Introducing XDR, a proactive approach that provides organisations with holistic, flexible and efficient protection against threats.

Join Bytes & Secureworks on Tuesday 5th March for our virtual event where a selection of Leading Experts will unpack & discuss how XDR & Managed XDR Services can transform your Cyber strategy.

- **Time + Date:** Tuesday 5th March @ 10 – 11am
- **Location:** Virtual
- **Registration Link:** Click Here

USEFUL RESOURCES

- What is XDR?
- Managed Detection & Response
- State of Threat Report

HOW BYTES CAN HELP

Book in a consultation with one of our in-house experts to discover how best Bytes can support your XDR journey and **transform your IT security to deliver maximum protection against today's threats**.

Reach out to your dedicated Bytes Account Manager, or email our friendly team via tellmemore@bytes.co.uk