Demystifying EDR, SIEM, XDR, MDR & MXDR

As cyber threats grow more frequent and sophisticated, there's been a rapid evolution in defensive security tools and services aiming to keep pace. With complex titles like EDR, SIEM, XDR, MDR, and MXDR—it can be confusing to determine what capabilities each provides and when to leverage them for your organisation.

Technology

EDR (Endpoint Detection and Response)

EDR tools utilise agents installed across endpoints like laptops, servers, and mobile devices to provide deep visibility into activity and behaviours, detecting potential incidents through analytics. Robust EDR solutions can automatically take actions like isolating compromised endpoints when risks are identified.

SIEM (Security Incident and Event Management)

SIEM platforms aggregate activity data and alerts from across your security tools to correlate insights and provide a unified dashboard for monitoring, prioritising, and responding to threats. Powered by automated workflows through security orchestration automation and response (SOAR), leading platforms enable response capabilities to keep pace with an ever-evolving threat landscape.

XDR (eXtended Detection and Response)

XDR provides expanded detection and response beyond EDR across more systems like cloud workloads, identities, and networks, driven by AI to automatically correlate alerts and take measures to neutralise threats. XDR breaks down security silos through a streamlined architecture and reduces the number of security tools required to provide end-to-end visibility across your environment.

Services

MDR (Managed Detection and Response)

MDR services provide 24/7/365 security monitoring, threat hunting, and response capabilities delivered by teams of experts, leveraging leading technologies like EDR and SIEM. MDR teams function as an extension of internal security staff, taking on the response burden.

MXDR (Managed XDR)

MXDR combines the most advanced detection technologies with specialised human expertise across domains endpoints, networks, cloud workloads, identities, email, and SaaS applications.

Powered by XDR capabilities, expert analysts, automation, and threat hunting oriented around client-specific priority risk vectors.

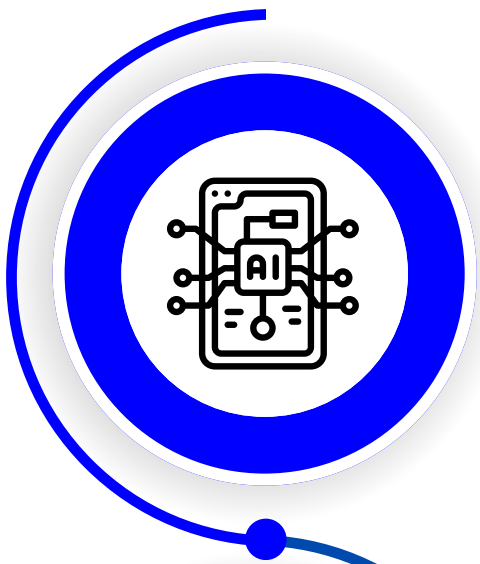
Delivered 24/7/365, analysts handle incident alerting and response, whether an emerging campaign, false positive triage, or containment of compromised assets.

MXDR services take immediate targeted actions while sharing insights that strengthen longer-term security posture.

Choosing the right solution

When deciding which solutions to adopt, it is essential to assess your organisation's current capabilities and determine which option best suits your needs.

Key Considerations include:

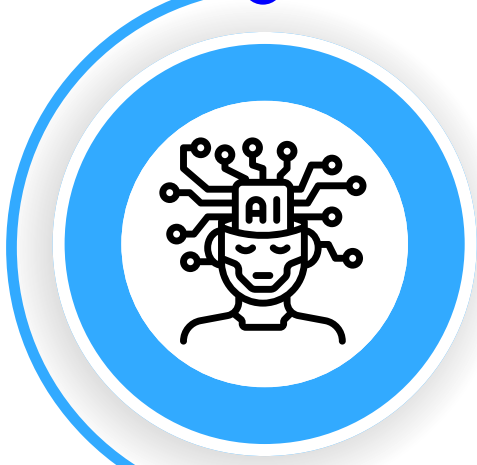


INTERNAL SECURITY STAFF

Can your internal team effectively manage the volume of alerts and incidents the solutions generate? if not, MDR/MXDR services can be a valuable extension of your team, allowing you to maximise your investment in security tools.

CURRENT INFRASTRUCTURE

What assets are you protecting? Do you have cloud resources or a large network? Do you mainly bring-your-own-device endpoints? It's important to choose tools that meet the actual needs of your organisation, rather than theoretical ones.



EXISTING SOLUTIONS

When considering implementing a new security solution, it is important to evaluate if it addresses security gaps or if multiple solutions can be streamlined to provide enhanced return on investment.

ACCESS TO EXPERTISE

EDR, SIEM and XDR solutions require security expertise for deployment and operation. If you have limited internal resource, MSSP's can take over the responsibility of this to allow your team to focus on core business activities.

PROACTIVE RESPONSE

Incident response and threat hunting are crucial for proactively managing cybersecurity risk. EDR, SIEM, and XDR tools provide strong support, but in-house expertise or partnership with an MDR/MXDR provider is necessary to ensure robust services.

Improving Your Security with MXDR

The number of alerts generated by EDR, SIEM, XDR, and other security tools can be overwhelming for IT and security personnel, reaching staggering heights of up to 10,000 alerts per day. Fortunately, MXDR services can alleviate this burden by promptly responding to alerts and reducing noise through tuning.

Exploring Managed Extended Detection and Response (MXDR)

Why MXDR?

Exploring the Benefits of MXDR for your organisation:

01 24/7/365 Detection & Response

02 Achieving Growth and Ensuring ROI Security

03 Prioritise Core Business Activities

04 Leveraging Automation & Orchestration

05 Reduced Time to Detect & Respond

06 Scalable & Flexible Service

How can we help?

If you need a reliable cybersecurity partner to help you navigate through MXDR and SIEM services, SCC is here to support you. Our highly accredited team provides end-to-end support and protection across your organisation, with innovative solutions tailored to your specific needs.

Not sure where to start? Our funded Pathfinders led by our team of experts can guide you in selecting the right solution for your business. Trust SCC to meet you wherever you are in your cybersecurity journey.

All enquiries online@scc.com
Contact our team 0121 766 7000
Visit scc.com