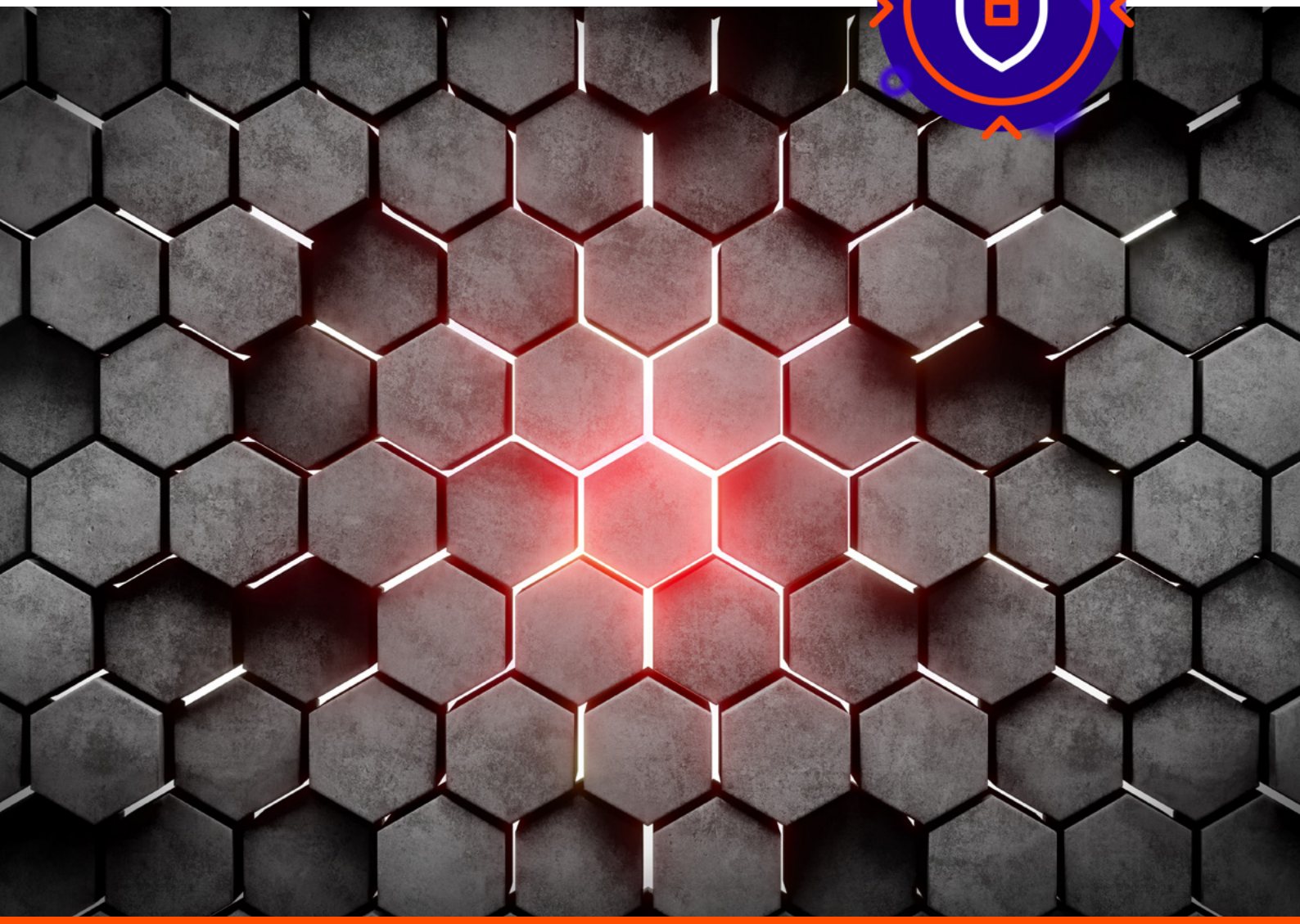
MANAGED DETECTION & RESPONSE (MDR)

TRUSTED CYBERSECURITY FOR AN UNCERTAIN WORLD



METCLOUD

GET CONNECTED • CYBER SAFE

WHAT IS MDR?

A managed detection and response (MDR) service enables organisations to significantly improve detection and remediation of security incidents. Another significant benefit of an MDR service is that it can help an organisation improve the return on investment (ROI) of the cybersecurity tools they already own.

Relying on traditional methods of cyber defense are no longer an option as the attack surfaces are constantly evolving and cyber criminals are becoming more sophisticated.

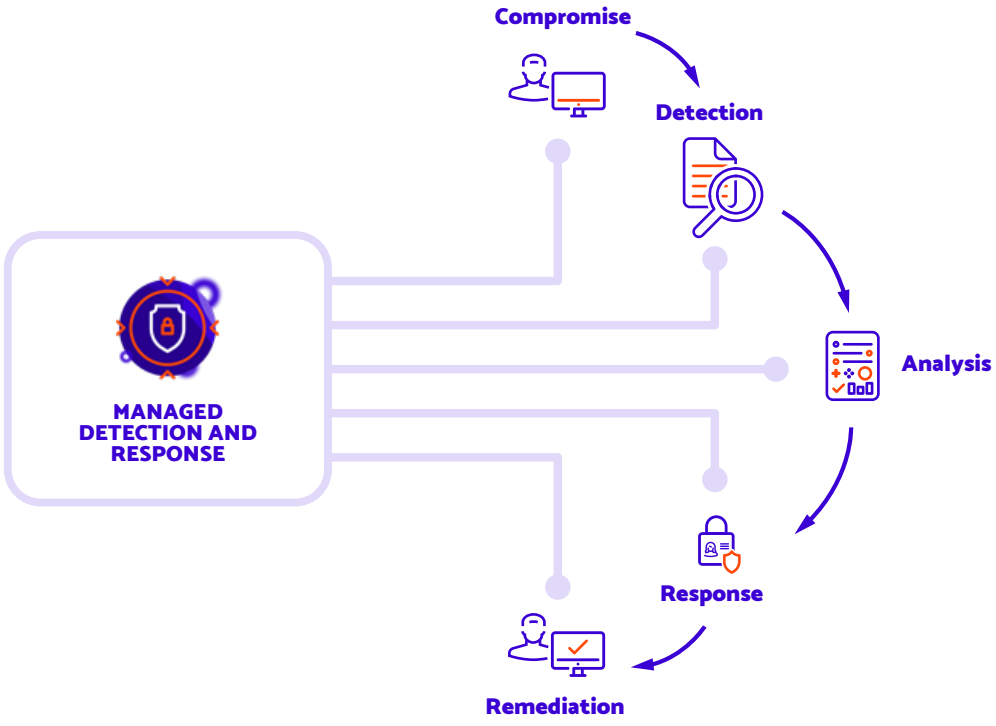
MDR is a combination of security technologies, as well as advanced analytics, threat intelligence and human expertise for investigation. These functions allow organisations to rapidly detect, analyse, investigate, and actively respond through threat mitigation and containment.

MDR acts as an extension of an organisation's security and or IT operations team. MDR provides your business with remotely delivered modern security operations center (MSOC) functions. A protected experience, using a predefined technology stack (covering areas such as endpoint, network, and cloud services) to collect relevant logs, data, and contextual information.

WHY IS MDR ESSENTIAL?

Delivering a robust cybersecurity capability requires the combination of many security technologies coupled with excellent management, support, and security expertise. Most organisations simply do not have the human capital and budgets to deliver a robust capability at a time when it has never been more important. As result, thousands of organisations are comprised daily.

The goal of MDR service is to rapidly identify and limit the impact of security incidents. These services are focused on 24/7 threat monitoring, detection, and targeted response activities.



HOW IT WORKS

DETECTION

Threat detection is the foundation of the MDR service. Mainly focuses on detection of attacks that have bypassed existing preventative security controls. This may be the result of attackers using new tactics, techniques, and procedures (TTPs), or it could be the result of the victim organisation's misconfiguration or lack of implementation of prevention capabilities inherent within the endpoint protection technical stack. However, some attacks are ultimately driven by human adversaries, who understand well the counter measures used to detect their activities and work actively to evade them and remain hidden.

PRIORITISATION

The reality for many organisations is that they will be faced with a large number of alerts to investigate across a wide group of endpoints. To handle this mounting workload efficiently and effectively, prioritising is essential. To achieve this, is the additional context, derived from threat intelligence and advanced data analytics. At a minimum, is important to know which data and assets are most sensitive and most in need of protection.

ANALYSIS

Once prioritised, the alert will need to be analysed to determine if it is a true or false positive. This is a critical step as it both informs and determines what security measures need to be undertaken.

Parts of the threat analysis process can be automated using sandboxing and behavioral analysis techniques, which deliver actionable intelligence and custom indicators of compromise (IOCs) specifically tailored for the threats encountered. Many tasks within the analysis phase can be automated, but to understand the veracity, scope and implications of an attack, human assessment is required to grasp the outputs of automated workloads.

RESPONSE & REMEDIATION

Alerts for true threats to the organisation require a response. The analysis and investigation phases should provide the context necessary to determine what form of response is needed. Response can take many forms, such as requiring that an endpoint be removed from the environment and contained, with the objective of reverting to a known good state. However, with good context, skilled experts and effective tooling, remediation can be undertaken to return the system to a known good state without recreating it.

WHY METCLOUD'S MDR

Our award-winning expertise in cyber security and compliance can help put you in the best possible position today and for the future. METCLOUD's MDR will provide significant protection in a world where the methods and sophistication of cyber adversaries is evolving daily.

Why METCLOUD?

Award winning company for cybersecurity, innovation, and excellence. Our vision is to be the global brand of choice for next generation cybersecure cloud services. Our services have been architected with security by design. Ransomware, Cloud vulnerabilities, Phishing attacks Social engineering and vulnerability management are the five top global security threats. METCLOUD's portfolio of cyber security and cloud services will ensure that you protect, defend, and mitigate any potential cyber attack irrespective of how it was carried out.

Let’s get connected.

Call 0121 227 0730
and speak to one
of our experts.

Email the team.
hello@metcloud.com

Visit our website for
more information.
metcloud.com

METCLOUD

GET CONNECTED • CYBER SAFE

02/2022/V1