Managed Detection and Response

Early Detection and Proactive Response for Incident Prevention

The cybersecurity market is shifting. Today's ever-evolving threat landscape is driving organizations to change how they address incident prevention. Capgemini's Managed Detection and Response Services (MDR) is a new breed of service that addresses this shift with a unique balance of monitoring, detection, and response capabilities. Capgemini MDR goes beyond traditional Managed Security Service Providers (MSSP) or Incident Response (IR) services to provide a continuous end-to-end approach that detects malicious threats earlier, provides comprehensive analysis of the intrusion, and delivers actionable guidance for future prevention based on intelligence gained.

Detecting and Responding to Cyber Incidents

Capgemini's MDR service is made up of two major components that deliver one big result; visibility and human analysis results in predictive prevention. We leverage technology, proven processes for analysis and experienced analysts to support your network defense team – together we discover threats sooner and respond to incidents faster, resulting in smarter protection for your enterprise.

Technology Enables Maximum Visibility

Effective analysis and an impactful defensive service require maximum visibility. Capgemini's MDR uses multiple technical approaches for achieving visibility across an organization's cyber footprint. Network-based sensors, Endpoint-based agents, and Log-based collectors provide broad visibility which is fed into a wide range of backend systems and platforms used by our team to analyze, detect, prevent, and report adversary activity. MDR analysts are experienced working with a wide range of technology deployed in client environments. Additionally, we can consult on appropriate solutions to achieve increased visibility.

- ***Network Visibility:*** Network sensors passively capture network streams, do protocol identification, metadata extraction from file attachments and are designed to provide network visibility and detection.
- ***End Point Visibility:*** Endpoint Detection and Response (EDR) technology uses behavioral analytics to identify post-compromise activity.
- ***Log Collection:*** Leveraging existing logs allows for a complete understanding of the client environment, providing context and visibility into existing security controls.

Capgemini MDR fuses this data providing our analysts an accurate view of the environment and visibility into adversarial activity.

MDR Service

- World-class cyber intelligence analysts supporting your team
- Implementation of consistent and repeatable analysis framework added to SOP
- Biweekly, non-customer specific threat intel summary
- Timely reports include
  - Escalated events with detailed, actionable analysis and prioritized recommendations
  - Details of analyst investigations that do not result in an actionable escalated events
  - Summary of service outcomes, trend analysis, and continuous improvement metrics and recommendations

MDR Service Benefits

- ✓ Improve situational awareness with maximum visibility and continuous monitoring
- ✓ Reduce distracting false positives and costly false negatives
- ✓ Prevent breaches through earlier detection and more effective responses
- ✓ Gain contextual intelligence to outpace adversaries and maintain your defensive advantage

An Advanced Approach to Detection and Response Leads to Incident Prevention.

Capgemini

Human Analysis for Enhanced Detection

Managed Security Services Providers (MSSP) are typically limited to detecting and reporting on malicious intrusion events at the firewall or IPS. Capgemini MDR service goes wider and deeper, providing continuous analysis across an organization's entire cyber footprint, including network activity, endpoint activity and logs. Successful cybersecurity analysis requires world-class analysts. Our MDR service staffs a team of skilled analysts experienced in detecting, tracking and preventing advanced threats against some of the most attacked networks in the world.

MDR analysts use consistent and repeatable analysis intrusion kill chain frameworks designed to provide a comprehensive understanding of the adversary and how their activities affect your environment. Acting as an extension of your security personnel, MDR analysts use their collective knowledge and decades of experience to develop actionable reports delivered to your team. MDR reports focus on prioritized activities your analysts can execute to enable maximum return on their efforts.

Why Partner with Capgemini

Partner with Capgemini to tackle one of the most difficult challenges facing cybersecurity organizations – incident prevention. For nearly two decades we have protected our enterprise and the cyber footprint of our clients worldwide with enhanced visibility and advanced human analysis. We continually monitor cyber landscape trends and adapt our approach to outpace cyber threat actors to defend our interests and those of our clients. Take advantage of our experience in the domain and our dedication to developing technology, processes, and methods to deliver effective network defense solutions.

- Improve situational awareness with maximum visibility and continuous monitoring
- Reduce distracting false positives and costly false negatives
- Prevent breaches through earlier detection and more effective responses
- Gain contextual intelligence to outpace adversaries and maintain your defensive advantage

MDR Threat Intelligence is Key to Incident Prevention

As part of the service, our team continually develops and reapplies threat intelligence through active, retrospective, and proactive means.

1. Situational awareness and readiness to respond is immediately improved. This deeper understanding creates new insight into how adversaries could adapt and evolve based on current capabilities which in turn informs forecasting potential risks for future incidents.

2. Threat activity previously unknown and undetected is revealed by continually evaluating new intelligence against historic data. Emerging trends and identified campaigns create context within which future attack indicators can be correlated to enable incident prevention.

3. New intelligence is used to identify and address gaps in cyber defenses before they are exploited by cyber threat actors. Once infused into detection and mitigation controls it enables the identification and prevention of future threats.

About Capgemini

A global leader in consulting, technology services and digital transformation, Capgemini is at the forefront of innovation to address the entire breadth of clients' opportunities in the evolving world of cloud, digital and platforms. Building on its strong 50-year heritage and deep industry-specific expertise, Capgemini enables organizations to realize their business ambitions through an array of services from strategy to operations. Capgemini is driven by the conviction that the business value of technology comes from and through people. It is a multicultural company of over 200,000 team members in more than 40 countries. The Group reported 2018 global revenues of EUR 13.2 billion.

Learn more about us at

www.capgemini.com/cybersecurity

For further information, please contact:
infra.global@capgemini.com

People matter, results count.

Capgemini