GTT MANAGED DETECTION AND RESPONSE (MDR)

GTT Managed Detection and Response (MDR) service combines people, process and systems to detect and remediate threats faster, saving time and resources and ensuring data and businesses are secure.

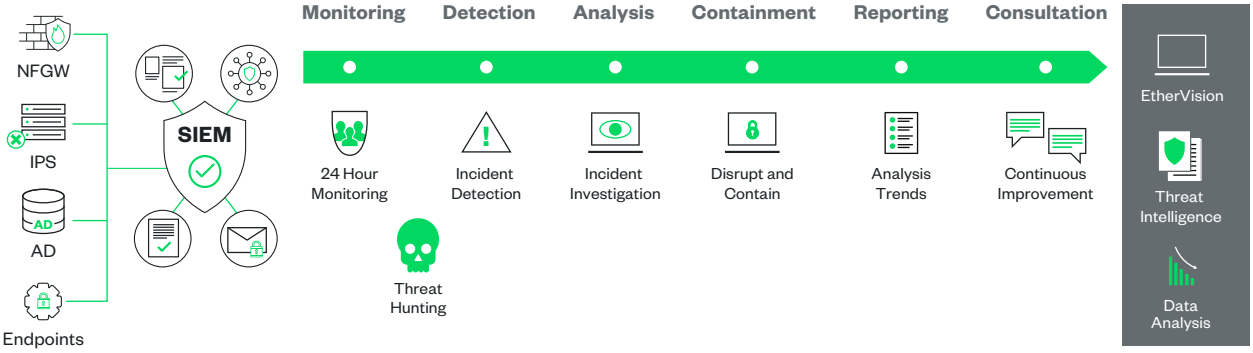
Cyber criminals are financially motivated and can bypass preventive controls and access networks for weeks, sometimes months, before they are detected. Every day a network remains compromised, the more expensive it will be to remediate. Businesses can no longer rely solely upon traditional security solutions such as firewalls and anti-virus software to protect their businesses from cyberattacks. Comprehensive security must combine advanced technology with skilled and dedicated security experts to deliver 24/7/365 detection and response.

The average breach lifecycle takes 287 days, with organizations taking 212 days to initially detect a breach and 75 days to contain it. Victims that respond to data breaches in under 200 days spend an average of $1.1 million less on data breach damages.[1]

WHAT IT IS

GTT MDR service provides customers with remotely delivered modern Security Operations Center (SOC) capabilities to rapidly detect, analyze, investigate and respond to threats that have bypassed traditional security controls.

Scope of MDR services



HOW WE DO IT

GTT's service provides a comprehensive turnkey experience to monitor customer assets including security assets, endpoints, networks, cloud services, operational technology (OT), internet of things (IoT) and other sources. Data is analyzed using a combination of custom and machine analytics, multiple layers of threat intelligence, and powerful human intelligence and threat hunting to eliminate false positives and detect and remediate threats faster.

GTT

75% of organizations can't respond to security incidents within one day, with the average cost of a data breach reaching a record high of US $4.35 million.[2]

GTT MDR service is designed to help customers meet the challenges of the constantly changing threat landscape by helping to detect threats posed from malware, ransomware, phishing attacks, data breaches, extrusion attempts, unauthorized access, insider threats, and more.

The service works by ingesting logs and data from customer key log sources in the customer environment whether on prem or in the cloud into a GTT hosted SIEM (Security Information and Event Management system) platform providing real time correlation and dynamic rule sets.

The SIEM platform stores, analyzes, and alerts on security event data collected from the customer's environment. The service is augmented with additional 3rd party threat intelligence feeds as well as analysis of potential Indicators of Compromise (IOCs) across multiple customer environments. Finally, security analysts in our Security Operation Center (SOC) add human intelligence to further support investigation of incidents to eliminate false positives, find actionable events, and provide remediation expertise for the customer.

Upon resolution, the SOC will provide an incident report containing all the relevant information pertaining to the incident. Monthly reports, real-time dashboards and ongoing SOC consultations ensure customers realize the full value of their service with GTT.

KEY FEATURES

- Global 24/7 certified SOC monitoring of events
- Concierge deployment based on customer needs
- Access to dedicated certified security experts
- Access to GTT managed SIEM
- Proactive threat hunting
- Multi-layer threat intelligence
- Real-time incident investigation and validation
- Customized incident response support
- Log retention and search
- Regular compliance reporting and strategic security guidance

KEY BENEFITS

Accelerate your security maturity and reduce dwell time saving your business time, money, and reputation

Meet compliance needs

Total coverage – Cloud, network, endpoints, SaaS

Mature SOC saves time and provides immediate ROI

Simple and predictable pricing for the fraction of the cost of doing it in-house

Scalable and flexible solution leverage existing infrastructure

Access to dedicated security professionals

Sources:
1. Blumira's 2022 State of Detection and Response.
2. IBM/Ponemon Institute – Cost of Data Breach report 2022.

GTT Making Exceptional Possible

For more information
Americas +1 512 592 4858
EMEA +44 020 7489 7200
APAC +852 8107 1088
www.gtt.net