
GBM
Managed Detection
& Response Services

• Managed Detection & Response Service •

Cyber threat is constantly evolving. It is our job to anticipate, respond to and protect you against the threat, in whatever form it may present itself. Our 24x7 managed detection and response service works to detect advanced threats and take the correct actions. Our expertise in threat hunting, incident response and security operations, combined with our focus on building a trusted relationship with you and your team, helps to strengthen your organization's security posture.

GBM CYBERSECURITY CENTER

GBM

We Secure your Digital Future

Benefits

Automation of Remediation

Quickly remove devices or systems from the network before they can cause any damage.

Investigate and Detect Threats Quickly

Network traffic analysis enhances traffic visibility, enabling rapid investigation and threat detection.

Understand Your Threat Coverage

Our proprietary Threat Coverage Model allows companies to understand their security monitoring coverage in the context of the methods a cyber attacker would use.

Benefits

Expose New Threats

Using our data lake capabilities and the expert knowledge of our analysts on how threat actors operate, we can perform automated and manual threat hunts across our entire dataset.

Quickly Detect Anomalous User Behavior

User and Entity Behavior Analytics (UEBA) uses machine learning and artificial intelligence to detect anomalous user behaviors that could represent an insider threat.

Understand the Threat from High-Risk Insiders

Enhanced user monitoring detects threats posed by high-risk insiders.

GBM CYBERSECURITY CENTER

GBM

Our service is based on the following key components:

- We provide all the necessary technologies, people, and processes to monitor and detect attacks before any real damage occurs.
- **IBM Security QRadar SIEM platform** that collects security event data and processes it using security logic developed and maintained by our analysts.
- AI driven cybersecurity from IBM through the exclusive use of **IBM QRadar Advisor with Watson** for automating repetitive tasks, helping to drive more consistent and in-depth investigations to obtain actionable insights on critical incidents, and reducing dwell times to help adopt a faster and more decisive escalation process.
- **IBM Security QRadar SOAR security orchestration**, automation, and response platform that provides workflow management to increase the speed, efficiency, and accuracy of security alert triage.

- Threat Intelligence Team with more than 20 intelligence sources, as well as our GBM MISP Threat Sharing and the **GBM HoneyPot Net Threat Detector** project, to identify, analyze, and notify global and regional security events and alerts.

- Early alerts in **Cyber Intelligence Bulletins** detailing the TTPs of identified criminal groups regionally and globally, revealing the IoCs and IoAs used.

- IT Service Management (ITSM) platform that provides secure management, including auditable logs of all actions and clear communication of any alerts we pass on to you.

- Combines detection and response capabilities with next-generation endpoint prevention from **IBM Security QRadar EDR** for comprehensive prevention, detection, and response.

- 24/7 team of security analysts available to ensure your networks and systems are protected. The team uses SIEM, SOAR, AI, and EDR platforms.

- Enhances your team's skill level through collaborative investigations and live chat with our analysts.
- Provides unlimited responses for assets within scope, and monthly threat hunting, with the option for continuous managed threat hunting.
- Improves your security posture while our security experts provide quarterly reviews of your defenses, and easy access to the consultative services of the **GBM Cybersecurity Center.**

Service Features:

- 24x7x365 service.
- Security Operations Center in Guatemala with availability in Costa Rica and Panama.
- Senior Leadership Team with over 20 years of experience.
- Our platform and security suite have been included in the Gartner Magic Quadrant for 16 consecutive years.
- We are experts in Security Orchestration and Automation, having developed over 200 orchestration playbooks in the last 5 years.
- We continuously develop relevant threat content, backed by threat intelligence and measured against SLAs.
- Transparent service that returns control to companies.
- Threat Coverage Modeling: a transparent way to understand where you are most vulnerable.
- Integrations with third parties to ensure coverage across your entire estate.
- Our MDR service is backed by a leading threat intelligence team.
- ISO/IEC 27001 certified data center.
- We operate a "Benefit One, Benefit All" service.
- Dedicated Service Delivery Manager.
- Member of Europol's European Cybercrime Centre (EC3) NoMoreRansom initiative.
- Member of FIRST.
- Member of the AEGIS Program.

Related Services:

GBM Extended Detection & Response

GBM XDR is an enhancement to our MDR service. XDR allows companies to begin automating corrective actions around their key security infrastructure. For example, by applying the XDR service to an endpoint solution, we can detect an issue on an endpoint and then use our Orchestration and Collaboration Platform to perform corrective actions, such as isolating the endpoint or blocking a misbehaving process, all automatically. This approach means that at-risk endpoints can be quickly removed from the network at any time of day before they can cause damage. GBM XDR is expanding to provide the same levels of automation in other protective security solutions such as firewalls, cloud, and identity access systems.

GBM CYBERSECURITY CENTER

GBM

Related Services:

GBM Network Detection & Response

Organizations are turning to Network Detection and Response (NDR) solutions to complement or replace traditional security tools. Many companies have a blind spot within their network. GBM NDR uses network traffic analysis to provide better visibility into network traffic, which in turn enables rapid investigation and threat detection. From the network, we offer a service that provides broad-spectrum detection capabilities powered by advanced machine learning, customized rules, and models to detect suspicious behaviors, prioritize high-risk threats, and automate/augment response activities.

GBM CYBERSECURITY CENTER

GBM

Related Services:

GBM Data Security as a Service

We detect security threats that could affect companies' sensitive data using our IBM Security Guardium platform. We address the needs of data discovery and classification, vulnerability management in databases, as well as active monitoring of data access activity and behavior analysis to provide a dynamic view of interactions with information, allowing for early detection of anomalies. Our service enables the assessment and understanding of risks present in data management, detection of data breaches or anomalous behavior, protection and control of access to sensitive data, and automation of incident response.

Related Services:

GBM Vulnerability Management

Security vulnerabilities remain one of the leading causes of severe data breaches. The Vulnerability Management Service (VMS) from **GBM Cybersecurity Center** helps companies implement vulnerability discovery capabilities without the need for software, hardware, or personnel. GBM VMS offers a managed service for: external and internal scanning, active scanning, daily vulnerability checks and updates, authenticated and unauthenticated scanning, compliance scanning for PCI-DSS and other regulatory frameworks. GBM VMS also has advanced functionalities to help companies prioritize their remediation efforts with probability prediction—machine learning to establish the likelihood of exploitation—and threat context—threat intelligence from our team to understand how attackers are exploiting a vulnerability.

GBM CYBERSECURITY CENTER

GBM

GBM CYBERSECURITY CENTER

GBM

In a digital world, security
is the key to success.

Let us be the digital guardians
of your company.

LEARN MORE **HERE!**

Call the office in your country

Ext **3840**

mercadeo@gbm.net | /gbmcorp

www.gbm.net

We**Secure**your**DigitalFuture**