grant mcgregor
technology . people

Enhanced Security Service

Frequently Asked Questions

Enhanced Security Suite
(beyond GM Essential Bundle)

The Enhanced Security Service is a 12 Month term

Cyber Awareness Training

The managed Security Awareness Training includes several services which are targeted at increasing your people's awareness of cyber security threats and how to help them stay safe.

What is included with the Security Awareness Training month to month?
Access to a wide range of cyber training materials for all End Users, with automated training campaigns and scheduled email reminders. Also, fully automated, configurable simulated phishing attacks, with reporting of results. 'Virtual Risk Officer' which provides risk scores which can be reported by End User, groups of End Users or the whole organisation

Will there be ongoing management once the training has been set-up?
There will be a professional onboarding of the system provided by a GrMc partner. If you ever require to be retrained on the system this can be arranged. The service is constantly being updated in the background for you. Those who fall for phishing emails will be guided for additional training as well as reports of phishing email passes and fails reports will be sent.

Continuous Cyber Essentials Compliance

Cyber Essentials is not just a one point in time excise to receive a certificate but is continuous all year-round Compliancy. The Continuous Cyber Essentials Compliance Service allows you to demonstrate compliance against the standard all year round.

How does the Continuous Cyber Essentials Compliance Service differ from the once-a-year Cyber Essentials Service?
GM will make available a project manager as appropriate to act as a single point of contact for the Client for the duration of this Agreement. This will be provided in 15 to 20 mins blocks each month, totalling no more than (3 to 4 hours per year).

At the start of the service GM will provide the Client with a set of documentation and provide a single one-on-one briefing on Cyber Essentials to a representative of the Client. Following the briefing, Grant McGregor will provide access to the Self-Assessment Questionnaire, which the Client will complete with assistance from Grant McGregor.

Throughout the year GM will help the customer to keep the asset management register up to date for devices that are in scope each month. The project manager will also guide the customer within the CE framework, assessing the current compliance level and providing assistance with the assessment. All within the 15 -20 mins provided each month.

What policies are included and how often are they updated?
Grant McGregor will provide 10 Cyber Essentials Polices at the beginning of this agreement. They will be tailored per customer needs, but not rewritten. The policies will be updated when and if internal and external variables change to keep them update. All within 25 mins pe month or 5 hours per year. At the beginning of the new agreement year this will be repeated. The policies are as follows: -

· Information Security Policy
· Acceptable Use Policy
· Password Management Policy
· Joiners / Movers / Leavers Procedure
· Asset Management Procedure
· Asset Register / Software Register / Admins / Open Ports
· Access Control Policy & Register
· Patch Management and Vulnerability Policy
· Backup and Restore Policy
· Computer and Mobile Device Policy

What is included with the Computer Vulnerability Service?
GM will provide a 12-month licence for the Vulnerability Tool which will be downloaded to every endpoint in scope. During the month GM will provide remote device audits and software vulnerability management. Continuously scanning of the Endpoints to centrally report on vulnerabilities, allowing GM to gather and then address such vulnerabilities if software fixes are exist , all within 5mins per end point each month

What happens at the Cyber Essentials Renewal Anniversary date?
Prior to the customers Cyber Essentials expire date. The custom must complete the Self-Assessment Questionnaire, GM will Assess the completed Self-Assessment Questionnaire and report the result of the Assessment. If the Assessment result meets the criteria of the Scheme, GM will issue a Scheme Certificate. If an Assessment fails to meet the Scheme's criteria, the customer may submit one further Self-Assessment Questionnaire for Assessment.

Will there be an extra cost for the Submission of Cyber Essentials to IASME?
There will be, as normal, a separate certificate cost as charged to us by IASME.

Password Management

Password Management is a critical most important aspect of Cyber Essentials and good security hygiene. It allows you to manage and maintain all your passwords in one place, so that they are not all over the place in spreadsheets; word documents and located within peoples' personal browsers.

Will this help when people are off/on boarded?
This is a great solution for when people come and go. As you don't need to reset or locate who had what username and password. You just stop access to the one user account and reassign to another.

Advanced Threat Protection and Managed Detect and Respond Service

Think of MDR as having a house alarm system connected by a telephone line to a respond centre. They will know when the alarm is sounding to enabling them to respond and alert you. By having the MDR service they can provide you with a team of experts who monitor your computers and networks and respond to cyberthreats 24/7.

What is the Managed Detect and Respond Service?
The Managed Detect & Response service adds an expert security team (Cyber Intelligence Fusion Cell (CIFC)) on 24-hour overwatch to swiftly contain, resolve and remediate your EndPoint devices against known threats and provides intelligence & data from the MDR platform for security analysts to identify advance attacks and previously unknown threats. It is an integrated part of GM's Enhanced Security suite.

Do I need to provide any information and if so, what does the onboarding look like?
The Managed Detect and Response Team will affect real-time changes in your environment when a security incident is identified based on a asset of actions agreed.

We will work with you to complete a detailed "MDR Onboarding" form detailing your key people that need protected, Cyber Attack information, Network, Application lists and Storage locations to name a few.

Over a 30-to-90-day period Bitdefender will Baseline your EUD and Network i.e., what is normal and not suspicious activity at 3am in the morning or 20 computers being removed.

Who is behind this service in helping to keep my devices secure?

The Bitdefender Advanced Security Team is split into three groups: the Customer Success Team that works with us to serve as a central POC for all GM customer requests and serve as intermediary for Security Operations Centre; the Active Monitoring & Response (AMR) Team monitor/detect/respond to security events/alerts/incidents (24x7x365); and finally the Cyber Intelligence Fusion Cell (CIFC) team is responsible for supporting the AMR team with relevant and actionable cyber intelligence.

The SOC/CIFC will assess your threat landscape, conduct threat hunting (who, what and what there are doing) looking for evidence. They will also review the Dark Web, check for domain mimicking, password leakage, DNS changes and provide any actions to take. If you do have an attack, they will provide a report of what happened, what they did and a wrap up.