GBMSTECH

SECURED BUSINESS CONTINUITY

Capabilities

enquiries@gbmstech.com

+44 (0) 207 993 6949

Registered in England and Wales.
Company No 09607559
1 Berkeley Street London W1J 8DJ
0207 993 6949 enquiries@gbmstec.
com www.gbmstech.com

Table of Contents

Selling to a variety of markets, GBMS Tech, Ltd has built its position in the marketplace with solid line of business continuity and cyber security products and services that the small to enterprise market segment can deploy to enhance their multi-layered approach to their defense in depth.

GBMS Tech, Ltd. strategically addresses the pressing needs of the Small to Medium Enterprise, providing a scalable, integrated and robust solution that increases continuity and cyber security to unmatched levels from the small office environment all the way up to the enterprise environment

"Our Security and Threat Operations Teams are always ready to provide you with top tier cyber security consulting, services, and products!"

"GBMS Tech, Ltd. provides cutting-edge cyber security services for commercial businesses ranging from small, ten-person shops to large 1,000+ end-user enterprise environments."

GBMS TECH, LTD.

Type of company	Commercial Cyber Security Consulting Firm
Certifications held	Certified Information Systems Security Professional (CISSP), Microsoft Certified Hadoop Admin, Microsoft Certified Systems Administration (MSCA), Microsoft Certified Professional, Microsoft Certified Systems Engineer (MCSE), Certified Novel Engineer (CNE), Network +, Security +, Certified Fraud Examiner (CFE), Certified Ethical Hacker (CEH), Certified Hacker Forensic Investigation (CHFI), Access Data Certified Examiner (ACE), Fortinet Engineer 4, Sophos Architect, Cisco Certified Network Associate (CCNA), Certified Information Security Manager (CISM), HIPAA Certified Auditor
Products	Trident CMP (Cyber Security Monitoring Platform), Kraken Firewall
Services	Cyber security consulting, insider threat monitoring, multifactor authentication, breach and malware detection, vulnerability scanning and validation, penetration testing, secure network design, encryption, firewall and security device management, incident response, secure network storage, and around-the-clock threat and security monitoring.

GBMSTECH
SECURED BUSINESS CONTINUITY

GBMSTECH
SECURED BUSINESS CONTINUITY

Security Operations Centre

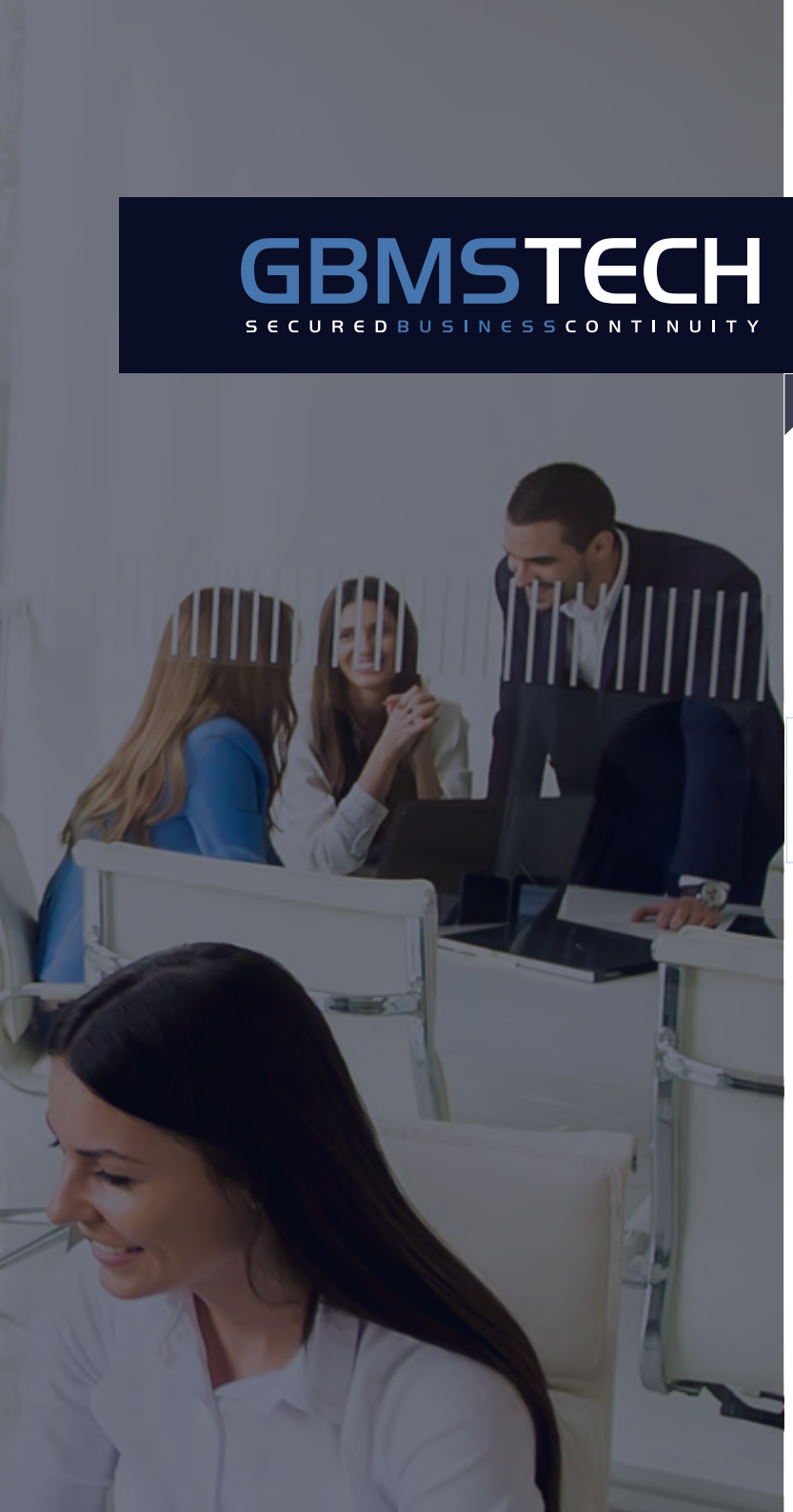
Our Security Operations Centre is staffed around-the-clock and has the ability to monitor and immediately respond to security incidents that are impacting your client's business.

24/7 Security Operations Centre Monitoring

Our state-of-the-art Security Operations Centre provides around-the-clock coverage using severity based alerting from our correlation analysis engines provided by our Trident CMP device or a SIEM already installed at a customer site. Our SOC analysts, are always "At the Ready" and watching your system to look for bad actors, malware, intrusions, and other security threats.

Incident Response

Our SOC analysts are trained to respond to incidents ranging from Ransomware infections to Denial of Service attacks. Our SOC analysts also assist your IT department, as they are usually the first line of defense. Coverage varies and is based on the service level agreement in place. In the event of a breach, a team will be on site as soon as possible and will stay until the problem is resolved.



GBMSTECH
SECURED BUSINESS CONTINUITY

Firewall Management

SOC analysts are trained on a variety of firewalls and follow the highest standards to ensure a limited threat vector from insider threats and external attackers. Firewalls can also have their syslog and intrusion detection event logs forwarded for collection, which allows for additional monitoring capabilities..

Intrusion Detection and Prevention System (IDPS) Management

SOC analysts are able to deploy sensors to remote locations throughout the world and can deploy an intrusion detection system within a day. If desired, this IDS can be transformed into an intrusion prevention system. Through custom rules and alerting, our SOC analysts are able to ensure the greatest level of protection available. Our SOC analysts make use of our Trident CMP for the most advanced and effective monitoring.

GBMSTECH
SECURED BUSINESS CONTINUITY

Threat Operations Centre

The GBMS Tech, Ltd. Threat Operations Centre is solely focused on uncovering the insider by identifying data leaks, potentially exposed data, and monitoring all employees with network access and access to sensitive data.

Employee Monitoring

TOC analysts are able to provide basic coverage with our employee monitoring suite. This line of products is intended for measuring the effectiveness and efficiency of employees during business hours and also to flag any issues or odd accesses during off hours. This services provides around-the-clock coverage for employers and corporate level staff to monitor employees.

Insider Threat Detection

TOC analysts are able to provide a service beyond the basic employee monitoring. This service is intended to monitor all communications within the company, any potential corporate espionage, embezzlement, time card fraud, and monitoring the corporate level staff, if desired. TOC analysts can provide deep forensics for investigations and even criminal prosecution.

Professional Services

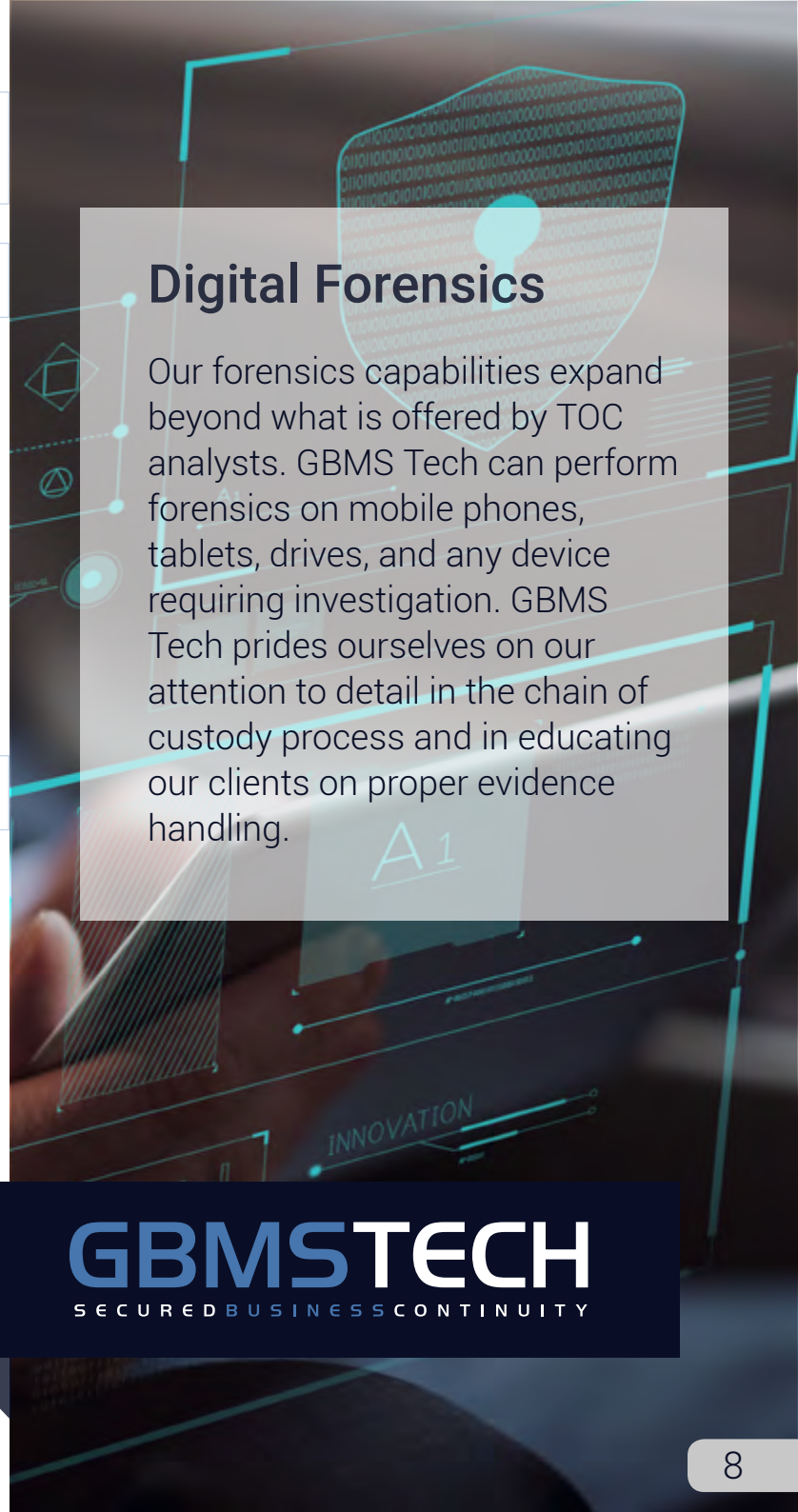
Vulnerability Assessments

Vulnerability assessments are intended to provide situational awareness on large networks to ensure patching is in place, proper hardening has been implemented, and to lower risk by using GBMS Tech, Ltd. State-of-the-art Assess, Remediate, and Monitor (ARM) process. The ARM process insures that the risk footprint is reduced and that continuous monitoring is in place to satisfy PCI and HIPAA requirements.

Incident Response

Penetration Testing is similar to vulnerability assessments except that these tests are intended to exploit discovered vulnerabilities. There are four areas of focus:

1. **Gray Box:** This is a black box attack that includes some knowledge of the client's internal network. This level of testing may also require a test user account to assess the potential for user privilege escalation.
2. **White Box:** Penetration test that includes full knowledge of the client's product and/or internal network to assess the risk of insider threat and the potential for internal attacks.



Digital Forensics

Our forensics capabilities expand beyond what is offered by TOC analysts. GBMS Tech can perform forensics on mobile phones, tablets, drives, and any device requiring investigation. GBMS Tech prides ourselves on our attention to detail in the chain of custody process and in educating our clients on proper evidence handling.

GBMSTECH
SECURED BUSINESS CONTINUITY

GBMSTECH
SECURED BUSINESS CONTINUITY

Trident CMP®

Cybersecurity Monitoring Platform

The Trident CMPTM from GBMS Tech is an on premise or virtual micro appliance combined with expert monitoring through GBMS Tech Security Operations Centre (SOC). It can be installed, configured, and commissioned in minutes, providing notifications to you of any potential unknown devices, questionable traffic, or other network issues at your client sites.
Trident CMP is composed of multiple modules to allow for customization of security services and support.

Network Protection.
Physical or Virtual Appliance monitors the network for any potential intrusions, bad actors, bad data, etc. and alerts. Combined with the 24x7x365 real time SOC monitoring.

Host Protection.
Small form application installed on each host to prevent unwanted applications, programs, scripts, etc. from running on each installed host.

Employee Monitoring.
Our TOC analysts monitor your employees in near real time looking for potential insider threats to your organisation.

PAST PROJECTS

Federal Defense Contractor

# of Employees	40
Service Performed	Insider Threat Detection
Outcome	GBMS Tech Threat Operations team performed an exhaustive investigation into the operations and employees at a medium sized federal cyber security contractor. Our threat operations team was able to identify the follow breaches: • Key employee (Co-owner) embezzling cash disguised as payroll bonuses. • Recruitment staff downloading entire resume databases before resigning and taking positions at new companies. • Collusion amongst key employee and CFO against majority owner of the company. Due to the efforts of GBMS Tech Threat Operations team the majority owner of the company was able to prosecute recruiter for theft of IP, and lower a buyout for a key employee from $3.5 million dollars to $1.5 million dollars.

	Health Care System	E-Commerce Site
# of Employees	500	12
Service Performed	Vulnerability Scan and Assessment	Penetration Testing
Outcome	GBMS Tech Security Operations team performed a vulnerability scan and assessment on a large healthcare organisation. Our security operation team was able to identify the following: • Multiple open ports and vulnerable systems. • 12 forgotten Windows 2003 servers that were still sitting on the network. • Many Windows XP machines that had been replaced with newer machines, but were still powered on with full network connectivity. • Identified key areas of IT infrastructure that had not been upgraded, patched, or secured.	GBMS Tech Professional Services team performed a penetration test against a client's e-commerce site and Amazon AWS infrastructure. Our client had assured us that he had been getting penetration tests for years and that we would find his system top notch. The GBMS Tech penetration testing team was able to find: • Several high priority vulnerabilities within the first two hours of testing. • Overall the penetration test team found over 50 vulnerabilities of which 10 were high priority and had to be fixed.

Hospitality Client

# of Employees	700
Service Performed	Insider Threat Detection
Outcome	GBMS Tech Threat Operations team performed an exhaustive investigation into the operations and employees at a large hospitality client in the MD area. Our threat operations team was able to identify the follow breaches: • Employees hiding or masking e-mail addresses in order to send company IP back to personal Gmail accounts. • Employees downloading or printing entire customer spending patterns and lists without permission. • Employees stealing customer contact lists via e-mail and Dropbox. Due to the efforts of GBMS Tech Threat Operations team the company was able to go prosecute employees for breach of contract and theft of company information. GBMS Tech employees worked with legal counsel for the client to prepare cases for court.

GBMSTECH
SECURED BUSINESS CONTINUITY

For more information on
GBMS Tech Limited.
Please contact:

GBMSTECH
SECURED BUSINESS CONTINUITY


enquiries@gbmstech.com


+44 (0) 207 993 6949


www.gbmstech.com


1 Berkeley Street
London
W1J 8DJ