



'We cannot solve our problems with the same level of thinking that created them'

# GLTECH

Cyber Security Professional Services

Our goal is to make it easy for organizations to navigate the complex nature of IT Management and Cyber security while ensuring the business goals are achieved. Our team of professionals that have hands-on experience and technical expertise will assist the organization plan and effectively execute the cyber security program.

## ABOUT US

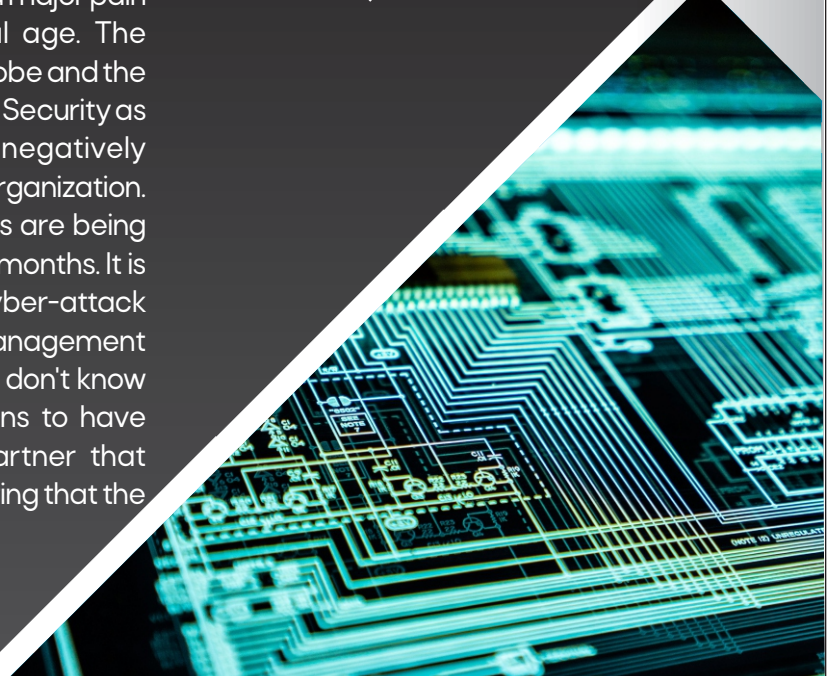
The GL-Tech consulting team brings in-depth cybersecurity expertise (our consultants have on average 15 years of experience in security specific roles). We provide the ideal combination of seasoned security experts backed by rigorous methodologies and leading-edge technology to assure success for Clients strategic initiatives. GL-Tech, as an organization, focuses with our clients on prevention and containment. We provide incident response and forensics services to help reduce incidents in your environment as well as proactive cybersecurity assessments to ensure risk mitigation. When an incident does occur – our Incident Response services are focused on containment as rapidly as possible. Our experience and that of our partners covers both IT cyber security incidents, Internet of Things (IoT) and Industrial Control Systems (ICS) incidents. GL-Tech implements software that predicts cyber-attacks and blocks them on the endpoint in real-time before they ever execute. This visionary approach to security permeates our consulting engagements and the technology is utilized in our incident response investigations.

## What Makes Us Unique

Each organization that we work for is given special attention and a deep dive is usually carried out to identify the unique peculiarities of the organization. Our team friendly disposition while working for our clients and the entrenched practice of going the extra mile in ensuring our client is satisfied is what stands us out.

## Cyber Security Challenge:

Information security and Cyber security risk is a major pain points for various organizations in a digital age. The heightened level of cyber-attack across the globe and the impact requires that organizations treat Cyber Security as a major strategic risk that is capable of negatively impacting the continuous existence of the organization. Targeted attacks are on the rise, organizations are being compromised and attacks go undetected for months. It is often said that no organization is immune to cyber-attack however, smart organizations know that risk management is a key part of all security decisions but many don't know how to start. It is necessary for organizations to have experienced and reliable cyber security partner that would guide them through the process of ensuring that the organization is secured.



# OUR SERVICES



## **GL Technologies Limited (GLTech) Your Trusted Security Partner**

GLTech is your trusted Cyber Security Advisor. Our team of professionals and partners are bright minds with a combined experience of over 3 decades in the field of IT management, Cyber security and IT Auditing. We pride ourselves with qualified team that have managed Cyber security for top global Banks and also consulted for various sectors such as Banking, Payment system organizations, Telcos, Manufacturing sector etc.

- Cyber Security Consulting Services
- Establishing a Solid Information & Cyber Security program for clients.
- Conducting Cyber Security Assessment
- Implementing Relevant Security Controls for Clients
- Vulnerability Assessment and Penetration Testing
- PCIDSS Audit
- ISO 27001 Audit
- IT Audit
- IT Operations Security Assessment
- Governance & Compliance
- Managed Security Service
- Third-Party Due Diligence
- Cloud Security Assessment
- Establishment of SOC
- Cyber Incident Response
- Project management
- Training

### Specialized Services for Financial Institutions:

- Digital Banking Risk Management Assessment
- Development of Digital Banking Risk Management framework
- Design & implement unified Digital Banking Security program
- Secure Digital Banking Product Development consulting services
- Core Banking and Digital channels Security Hardening
- Implementation of Fraud Control on Digital Banking Products and Services
- Mobile Money Implementation and Integration Security Review
- Implementation of Enterprise fraud prevention and detection solution
- Online wisdom Cybersecurity awareness program for Bank Customers

# Cyber Security Consulting Services

## GL-Tech - Managed Detection and Response Services

GL-Tech - Managed Detection and Response Services is a 24x7 managed detection and response offering that provides actionable intelligence for customers to prevent threats quickly, while minimizing alert fatigue without requiring additional resources. GL-Tech has the strategy, expertise, and technology to analyze and guard an organization by preventing and containing threats as well as large scale breaches.

### Benefits:

- Discover Threats in No Time:
- Leverage our native AI platform 24X7 to detect known and zeroday threats
- Receive detailed and actionable threat intelligence whenever and wherever
- Respond to Threats in No Time:
- Implement effective countermeasures quickly
- Limit the impact of a breach

### Key Features:

It's hard to detect the true signal of a threat when you're drowning in a sea of extraneous alerts.



Threat Hunting



Transparent



Proactive

### Continuous Managed Detection and Response

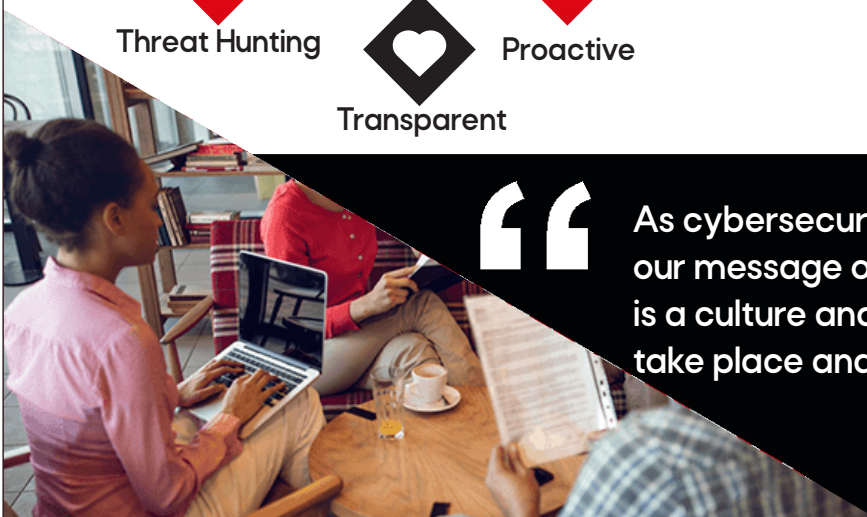
Adversaries don't keep office hours. That's why GL-Tech monitors your environment 24x7, triaging alerts, tracing threats, correlating data, facilitating remediation, and keeping you informed every step of the way via the monitoring portal and a convenient mobile app.

### Stops Advanced and Emerging Threats

GL-Tech through implementing a 5th generation native AI platform stops zero-day payloads, polymorphic malware, APTs, and both file-based and fileless threats with proven 99.1% efficacy. GL-Tech solution prevents incidents from occurring, before they can compromise your data and reputation.



As cybersecurity leader, we have to create our message of influence because security is a culture and you need the business to take place and be part of that security culture.



## Staff Augmentation

GL-Tech will provide a consultant who will have the backing of all GL-Tech consultants for strategy, governance, and technical expertise.

The consultant will serve the Client as an independent security expert providing strategic development and oversight of the Client's security program. This role will include information security governance and strategic planning to position Client for a proactive approach to cybersecurity based on business goals. GL-Tech will assign a lead consultant, who in conjunction with other GL-Tech experts will provide Client executives and management the opportunity to brainstorm and receive advice in all the necessary domains of a risk-focused security program.

## Methodology Based Threat Hunting

Going beyond simple alert management and traditional MDR, GL-Tech employs intelligence and methodology-based processes to identify potential attacks, data exfiltration, unauthorized access, or other potential vectors of compromise.

## Expertise When, Where, and How You Need It

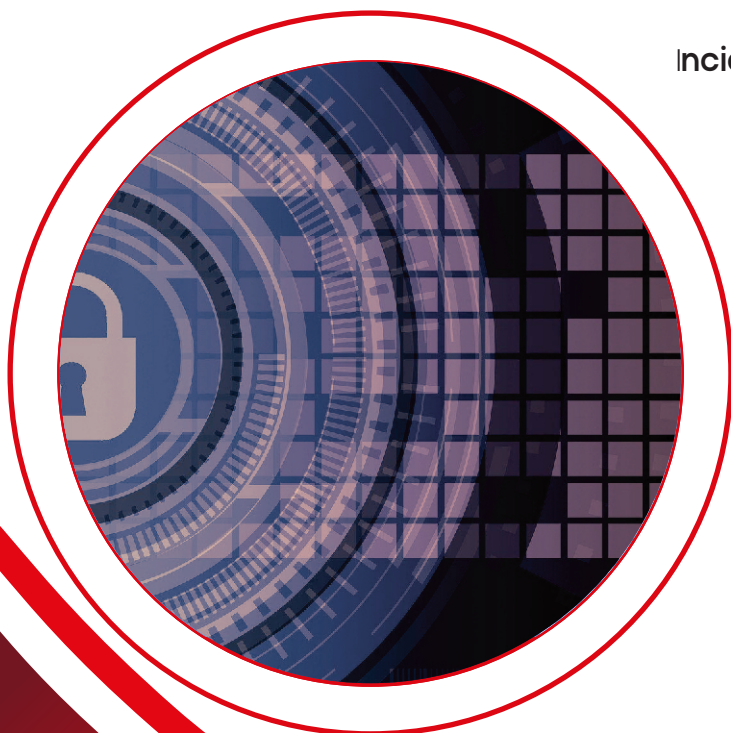
SOC teams are under-staffed and over-stressed due to a global security skills gap that shows no signs of abating. The solution? Augment your SOC through mobile interaction with a world-class team of GL-Tech and partners incident response and prevention experts

## Transition from Reactive to Preventative

The GL-Tech subscription is driven through a centralized AI platform that enhances the network effect of intelligence across your security ecosystem. GL-Tech helps you transition efficiently from a reactive to a prevention-first security posture.

## Automated Response and Containment

GL-Tech performs advanced orchestration for the triage, filtering, and response actions performed by analysts, and accelerates detailed incident response strategies that ensure threats are quickly detected, stopped, remediated, and prevented from recurring.



## Incident Response and Forensics Services

The GL-Tech & Partners team has responded to hundreds of high-profile breaches and routinely handles 30-40 incident response cases a week around the globe. Our team is highly trained, highly experienced and all of our responders are also developers who maintain our internally developed IR tools. Some of our responders have battled over 1,000 breaches in their career. We have worked with many clients on building out their Incident Response Program, by custom writing incident response plans, running incident response exercises and training IT Security staff. Our partners are one of the premier IR organizations in the world responding to some of the world's most complex breaches. We are known for our rapid and effective response to cyber security incidents.

## Compromise Assessment

A traditional security program includes a combination of frequent scanning and periodic penetration testing to identify ways that a hacker could gain access to a company's systems or data. While these processes represent good hygiene for a security program, they do not resolve the overwhelming concern that hidden malware may already exist in the environment or someone may be actively using user IDs and credentials to burrow further into the organization's systems in advance of a major breach or attack.

GL-Tech unique service, the Compromise Assessment, provides a mechanism to identify attacks currently underway as well as hidden malware and APTs in a way that other techniques such as penetration testing simply cannot achieve. Compromise Assessments are used to identify anomalous activity related to a potential compromise within your organization's managed IT estate.

The Compromise Assessment identifies environmental risks, security incidents, and threat actor activity in a network environment. The methodology allows GL-Tech to rapidly assess an organization's infrastructure for the items that provide evidence of an attack underway.

### Benefits

As sophisticated attackers utilize more advanced attacks including spear-phishing and combinations of known and unknown malware it is becoming increasingly more difficult for an organization to identify and shutdown an attack until it is too late. Oftentimes companies only learn of the attack when critical data is released or hundreds of their systems are wiped and inoperable. Traditional searches for malware and ongoing compromise were difficult, time-consuming, and typically could only examine a small sample of systems in an environment.

### Methodology

GL-Tech gathers, parses and analyzes key artifacts from an organization's environment in order to determine the extent of any compromise activity or suspicious behavior. The artifacts are collected from all systems across the environment, including all operating system types, utilizing a set of straight-forward scripts. These self-cleaning scripts utilize standard operating system commands to interrogate each system for a variety of system state and history data.

**The compromise assessment is performed in three phases:**

### Phase 1 - Diagnose

The SQL database that is constructed in this phase provides an opportunity to analyze data for coincidental determination of like artifacts (such as filenames or user profiles etc.) or attributes (such as date/time or file size and etc.).

### Phase 2 - Assess

The Assess Phase provides more in-depth data capture and analysis in order to determine whether the findings from the Diagnose Phase are false positives, or indicate malicious activities.

### Phase 3 - Collect

If certain computers are identified that according to internal corporate policies require retention for legal or other purposes; or if more scientific/technical analysis is necessary – then activities will include a full bit by bit disk copy (DD-image or E01) of those computers, including memory dump, for related analysis.

### Results and Recommendations

At the conclusion of the Compromise Assessment project GL-Tech delivers a summary of the project for the executive team that provides a high-level overview of the findings and risk state of their environment.

### Some unique items that GL-Tech & Partners brings to Incident Response engagements:

- GL-Tech tools and methodologies are completely Operating System
- Agnostic, we can respond to any environment.
- We leverage our award-winning AI technology during discovery as well as doing deep dive/forensic processes.
- GL-Tech team brings a unique speed and efficiency to the process with our emphasis on leveraging AI, and having 'silent' and 'self-dissolving' scripts that don't tip your hat to an attacker.
- We have the ability to contain an incident with our partner endpoint technology if and as needed during engagements.
- GL-Tech brings custom heavy-lifting forensics tools.
- Broad experience with the team having conducted over 2,500 IR investigations

### Incident Response Program Review and Development

This offering will provide assistance to clients to either develop or assess their entire incident response program. This is a comprehensive offering that will also include IR policy review and creation as well as a security tool assessment if deemed necessary.

- IR Policy Review/Creation
- Incident Response Plan Review and Update
- Incident Response Playbooks
- Incident Response Tabletop Exercise
- Incident Response Readiness Assessment

### Business Email Compromise Assessment

Business Email Compromise fraud is a scheme whereby cybercriminals gain access to business email – often a senior executive or someone who can authorize payments – in order to transfer funds on their behalf. In a recent report from J.P. Morgan, 78% of companies were targets of payments fraud last year. GL-Tech's partner BEC Analysis Engine tool can quickly analyze Office 365 or other email logs to identify forwarding rules, failed or successful logins, what accounts were used, and how BEC attacks originated. *At the conclusion of the assessment, a comprehensive report is provided to the executive team that details:*

- A list of vulnerabilities detected
- The risk state of the environment
- Strategic and tactical recommendations for remediation

### Internal Penetration Assessment

GL-Tech performs internal network penetration testing from the perspective of an attacker who has gained an initial foothold in the client's internal environment. This could be through, for instance, phishing leading to client-side exploitation or physical intrusion into the facility. GL-Tech's two main goals in an internal penetration test are 'breadth' and 'depth'. Breadth, meaning the goal of discovering as many vulnerabilities as possible in the network that will allow an attacker to achieve system compromise. Depth, meaning how far will an attacker be able to penetrate into the network by leveraging those vulnerabilities, with the ultimate goal being domain admin level access and access to and/or exfiltration of, the organization's most sensitive data.



## Cybersecurity Operations Development

GL-Tech will be taking a multi-faceted approach to assisting Clients with this undertaking. GL-Tech will assist Clients in performing a Security Operations Center (SOC) capabilities assessment. This assessment will be conducted in a phase-based approach and rely on industry standard best practices. GL-Tech will outline what an industry standard SOC should possess in terms of capabilities, technology, implementation of said technology, security of the SOC itself as well as policies, processes and procedures that should be in place. This assessment will determine the capabilities that an industry standard SOC should possess and how to implement them.

1. Security Assessment of SOC
2. Security Controls Capability
3. Tools
4. Processes and Procedures
5. Personnel and training

The goal of this team is to transform the SOC. Responsibilities across this coordinated team will include:

- Monitoring and Management of the technology in place at Clients
- Log Management
- Development of Use Cases
- Threat Hunting
- Malware analysis
- Provide a plan for optimizing key security toolsets.
- Ensure technology in place is configured and maintained appropriately
- Managed the CMDB
- Utilizing existing Client tools to develop an incident management system





## Business Email Compromise Assessment

Business Email Compromise fraud is a scheme whereby cybercriminals gain access to business email – often a senior executive or someone who can authorize payments – in order to transfer funds on their behalf. In a recent report from J.P. Morgan, 78% of companies were targets of payments fraud last year. GL-Tech's partner BEC Analysis Engine tool can quickly analyze Office 365 or other email logs to identify forwarding rules, failed or successful logins, what accounts were used, and how BEC attacks originated. *At the conclusion of the assessment, a comprehensive report is provided to the executive team that details:*

- A list of vulnerabilities detected
- The risk state of the environment
- Strategic and tactical recommendations for remediation

## Strategic Services

Security Maturity Review Assessment GL-Tech will perform a holistic Security Program Maturity Assessment, measuring how the Client's security processes compare to the defined security standards it needs to meet. The nature of this assessment is to provide custom consulting and partnership on building a comprehensive security program in two phases.

### Phase 1:

GL-Tech will determine Client's current state for its IT and security environment and develop recommendations to close those gaps and improve the overall security posture of the information technology operation.

### Phase 2:

GL-Tech will work with client collaboratively to identify the best tactical and strategic remediation solutions for the gaps discovered during the first phase of the Security Program Maturity Assessment. GL-Tech will aid by providing product-agnostic insight acquired through many years of security consulting experience into the ideal strategies and technologies to implement in order to most effectively improve the security posture of Client's environment.

## Red Team Services

External Penetration Assessment Protecting your internet facing infrastructure from external threats begins with identifying the attack surfaces of your external systems. GL-Tech identifies each external netblock and performs discovery to find each live host on those netblocks. GL-Tech then enumerates every open TCP and UDP port on each system and queries these ports to discover what services are listening on them. Vulnerability scans are conducted against each open port and the results of these scans manually verified. This is followed by manual penetration testing of each open port to search for vulnerabilities which cannot commonly be found by vulnerability scanners. The aim of this process is to ensure that every host, every open port and every listening service on your externally facing networks are thoroughly tested.

GL-Tech begins by taking a list of hosts and/or netblocks provided by the customer and verifying them against the five Regional Internet Registries (RIRs).




## Internal Penetration Assessment

GL-Tech performs internal network penetration testing from the perspective of an attacker who has gained an initial foothold in the client's internal environment. This could be through, for instance, phishing leading to client-side exploitation or physical intrusion into the facility. GL-Tech's two main goals in an internal penetration test are 'breadth' and 'depth'. Breadth, meaning the goal of discovering as many vulnerabilities as possible in the network that will allow an attacker to achieve system compromise. Depth, meaning how far will an attacker be able to penetrate into the network by leveraging those vulnerabilities, with the ultimate goal being domain admin level access and access to and/or exfiltration of, the organization's most sensitive data.

A white rocket icon inside a red diamond shape, which is itself inside a larger red envelope-like shape.

**Wireless  
Penetration Assessment**

A white heart icon inside a black diamond shape, which is itself inside a larger black envelope-like shape.

**Physical  
Penetration Assessment**


A white gear icon inside a red diamond shape, which is itself inside a larger red envelope-like shape.

**Social Engineering  
Penetration Assessment**


**Application  
Penetration Assessment**

A white bar chart icon with a line graph on top, inside a red diamond shape, which is itself inside a larger red envelope-like shape.

**Cloud Architecture  
Penetration Assessment**

A white lightbulb icon inside a black diamond shape, which is itself inside a larger black envelope-like shape.

**Red Team  
Penetration Assessment**

A white screwdriver and wrench icon inside a red diamond shape, which is itself inside a larger red envelope-like shape.

### **Incident Response Technical Training**

GL-Tech will educate Incident Response staff and any other Information Security individuals on the end-to-end incident response process (from preparation to lessons learned). GL-Tech will train users on tracking incidents and clearly identify roles and responsibilities during an incident. This will ensure that all team members will know when and how to transfer/request information and responsibilities between differing teams within the organization.

### **Project Management**

GL-Tech starts with well documented and time-honored project management principles, and tailors them to today's dynamic security environment. Your project will have a single project manager to coordinate activities throughout the project. This provides assurance that we will meet all your security requirements and ensure that the services you receive fit your needs precisely. All scheduling information and relevant planning will be completed during the kickoff process prior to the actual start of your engagement.

### **Our Professional Training Courses**

A series of on-demand training sessions or in person lunch-and-learns will follow to ensure that the playbooks are understood and are usable per the different tiers. These training sessions should at first be performed per role or tier.

“

*The knock-on effect of a data breach can be devastating for a company. When customers start taking their business-and their money- elsewhere, that can be a real body blow.*



# OUR PROFESSIONAL TRAINING COURSES

## 1. CISSP Course

a. Prepares the student to take the ISC2 CISSP course rev April 2018

## 2. Big Data Course

a. “Big data” is a field that treats ways to analyze, systematically extract information from, or otherwise deal with data sets that are too large or complex to be dealt with by traditional data-processing application software. Once referred to as the next “oil boom” Big data typically uses a software called Hadoop to “mine” these analytical goals allowing a company to analyze this data for business-based decisions.

## 3. Cloud Security Course

a. Prepares you for the CSA – Cloud Security Alliance Certification Test. Cloud Security Alliance is a not-for-profit organization with a mission to Promote the use of best practices for providing security assurance within Cloud Computing. Also, to provide education on the uses of Cloud Computing to help secure all other forms of computing.

## 4. Advanced Tools for Exploiting Software

a. Vulnerabilities in modern operating systems such as Microsoft Windows 7/8, Server 2012, and the latest Linux distributions are often very complex and subtle. Yet, when exploited by very skilled attackers, these vulnerabilities can undermine an organization’s defenses and expose it to significant damage. Few security professionals have the skillset to discover, let alone even understand at a fundamental level, why the vulnerability exists and how to write an exploit to compromise it. Conversely, attackers must maintain this skillset regardless of the increased complexity. This course teaches the skills required to reverse-engineer 32-bit and 64-bit applications, perform remote user application and kernel debugging, analyze patches for 1-day exploits, and write complex exploit, such as use-after-free attacks against modern software and operating systems

## 5. Electronic Discovery and Forensic Techniques

a. Computer forensics is the application of investigation and analysis techniques to gather and preserve evidence from a particular computing device in a way that is suitable for presentation in a court of law. Prepares you for the CHFI exam

## 6. OSINT

a. In this course you will be learning about OSINT (Open-source intelligence) from a hacker’s point of view. Tools, techniques, setting up a virtual lab, and how to protect yourself. This is a comprehensive course that will be using free open source tools to investigate people and companies. No matter if you are totally new to the fascinating world of OSINT and hacking or have some experience, this course will walk you through how both hackers and investigators use these tools and why.

# OUR PROFESSIONAL TRAINING COURSES

## 7. Hacking and Hardening your Own Website

- a. This course is geared toward developers who are taught how hackers attack websites. They then go through all of the techniques a real hacker does to breach a website thus showing the developer how to code more effectively.
- b. This is a great course for Cyber Security students and Developer students as well.

## 8. Hacking and Hardening Windows Servers and Clients

- a. This course shows you all the ways to breach a Windows client and server. It is an extremely eye-opening course and a favorite of all the students. This course provides all of the things a system Admin needs to know in securely manage windows. The course covers all aspects of Windows infrastructure security from the hacker's mind point of view! The objective of the course is to show and teach you what kind of mechanisms are allowing attackers to get inside the infrastructure and operating systems. Finally, how to stop or prevent these things from happening. After the course you will gain penetration tester's knowledge and tools they may have used to achieve the breach.

## 9. Hacking and Hardening Mobile devices including iPhone and Android

- a. Mobile Device Attack Vectors. Hacking Mobile Platforms. Let us show you how Bad It is? Course covers Hacking Android. Hacking iOS. Hacking Other Mobile Platforms. Mobile Device Management, Guidelines, and Tools. Mobile Malware. Mobile Payments

## 10. PCI Course

- a. Payment Card Industry (PCI) Awareness training is for anyone interested in learning more about PCI – especially people working for organizations that must comply with PCI Data Security Standard (PCI DSS). By promoting employee awareness of security, organizations can improve their security posture and reduce risk to cardholder data

## 11. VMware System Administration Course

- a. You'll learn the basics such as vSphere equipment and hardware, and then more advanced topics such as using VMware to create cloud environments. Our VMware training videos also prepare learners to take VMware certification exams that are highly-valued in the IT industry. Prepares you for the VMware VCP Certification.

## 12. GIAC (SANS) Assessing and Securing Wireless Networks

- a. This course is designed for professionals seeking a comprehensive technical ability to understand, analyze, and defend the various wireless technologies that have become ubiquitous in our environments and, increasingly, key entrance points for attackers. Prepares you for the SEC617 Exam

# OUR PROFESSIONAL TRAINING COURSES

## 13. Practical Lock Picking

- a. The course concentrates on the most common type of locks that you encounter on a daily basis. The locks on your apartment or house, master keys, mailboxes etc. The principles and methods you learn in the course allow you pick all of these locks in a matter of minutes, and even seconds after you become a more seasoned lockpicker.
- b. Lock picking is a handy skill at the end of the day. In addition to helping your friends and neighbors when they get locked out, and lock picking for fun, you'll have a much better understanding at how locks work, and be able to make sure your home will be more secure. By trying out your newly acquired skills on your own property, you'll be able to determine how secure your lock is, and consider changing it if you find it very easy to pick.

## 14. Live Pen Testing Course

- a. This course follows a Professional Pen tester and provides the student a live look over his shoulder as he does a Penetration Test on a LIVE target. Videos and Images are sanitized to remove all traces of PII (Personally Identifiable Information) to protect the LIVE Business. The course goes through the entire process including a Physical Pen Test, and Scanning, and Pen Testing techniques from the initial Scoping information, to pricing the pen test, running the OSINT, Scanning for Vulnerabilities, providing a Post Exploitation Report as well as writing the final report.
- b. This course is sure to be a popular course

## 15. Red Team Field Manual

- a. The Red Team Field Manual (RTFM) is a no fluff, but thorough reference guide for serious Red Team members who routinely find themselves on a mission without Google or the time to scan through a man page. The RTFM contains the basic syntax for commonly used Linux and Windows command line tools, but it also encapsulates unique use cases for powerful tools such as Python and Windows PowerShell. The RTFM will repeatedly save you time looking up the hard to remember Windows nuances such as Windows wmic and ds query command line tools, key registry values, scheduled tasks syntax, startup locations and Windows scripting. More importantly, it should teach you some new red team techniques.

## 16. Metasploit from Scratch

- a. In this course, you will start as a beginner without any previous knowledge about the hacking, the course focuses on the practical side and the theoretical side to ensure that you understand the idea before you apply it. This course is intended for beginners and professionals, if you are a beginner you will start from zero until you become an expert level, and if you are a professional so this course will increase your knowledge about the hacking. in this course you'll learn how the black hat hackers' hacks Windows OS using advanced techniques, and also, you'll learn how the white hat hackers Secure Windows OS by analyzing it, and how to detect the hacker's identity. This is complete guide to using Metasploit

# OUR PROFESSIONAL TRAINING COURSES

## 17. Hacking and Hardening Mobile Devices in the Enterprise

a. This course prepares the system admin to roll out Mobile devices in the enterprise and how to deal with a BYOD policy.

## 18. Diversity in the Workplace

a. This course is taught on our video platform and can be contracted to be provided to your employees. Our instructor is Otis Felton FDIC (Ret'd) and both offers these courses worldwide and has written many books on the subject as well.

## 19. Psychology of Fraud

a. We provide a new and technological approach to combating fraud in your organization. We do this by not only identifying a potential subject it at a very early stage or by using behaviorisms to identify an ongoing problem. Dr. Trivedi, our instructor, has been providing these classes for years and has recently joined our team. He is available for in person classes and is also a part of our online library of courses.

## 20. Block Chain

a. We have on staff one of the most talented individuals in the field of Block Chain and Crypto Currency. Aamir Lakhani is not only an instructor for us but is also on our Advisory Board.

## 21. Artificial Intelligence

a. This is one of the most compelling new buzz words of business. It is predicted that we will achieve a singularity (Machines matching what can be done by the Human Brain) in the next few years. Our instructors speak about the technology and how to use it to our advantage.

## 22. Neural Link

a. This is the concept of linking the thoughts of a human by way of an extremely small (less than 1/10 the size of a human hair) implanted device in our subcutaneous skin near the brain at the back of the ear which can be used to both read and write thoughts to the human brain all linked wirelessly to what looks like a hearing aid that is powered by a battery and is used to remotely control a computer device such as a cell phone or laptop. The technological advantages to this are mind boggling. We offer an in-depth look at this new technology which is said to be available in less than 2 years!

## 23. Social Engineering Testing and Auditing

a. We provide in our library, one of the greatest social engineers of our time. Jason Street. He is considered to be the top speaker at all of the hacking conferences worldwide. We offer his services both as an in-person consulting/Social Engineering testing for your organization or by way of videos in our vast library of educational titles.



Hello!  
We Are  
Creative

## Contact Us

---



+2348056156142, +2347039992021



sam.okenye@gltechlimited.com  
info@gltechlimited.com



36, Olakunle Selesi Street  
Ajao Estate, Lagos State

For detailed proposal  
click [HERE](#)

