



Profile

MYRIAD VIEW Limited

Information Security and Digital Forensics

| | |
|----------------------------|---|
| Executive Summary | 3 |
| Capabilities and Expertise | 4 |
| Training | 7 |
| Key Staff Biographies | 8 |

OUR GOAL

Our goal at Myriad View is to establish strategic relationships with all our clients, resulting in a better understanding of your business objectives. This enables Myriad View to deliver services that are closely defined to meet your specific needs.

We feel the opportunities identified by our clients and the services offered by Myriad View are a complementary fit. We hope the information contained within this document will contribute to a valued and continuing relationship between our companies.

Our enviable experience and reputation in corporate, commercial and criminal investigations means our clients benefit from an efficient, cost effective, reliable, impartial and thorough service.

From digital forensic consultancy and services to INFOSEC policy reviews, forensic training to forensic process integration, internet investigations to mobile phone forensics, we can provide one of the most comprehensive solutions available.

As expert witnesses' we are called upon to present often complex technical evidence in a way that can be clearly understood by non-technical audiences. You can also benefit from this skill when we explain your options and the results of an investigation in clear, easy-to-understand language.

Our philosophy is simple:

- Work with you to provide the best level of service and technical competence
- Provide you with the right support, whenever and wherever you need it
- Keep the fee scales realistic

We look forward to working with you, when you need us, and to providing you with a professional, discreet, economic and reliable service.



OUR SKILLS AND STRENGTHS

ALL our staff are fully trained and experienced in the use of numerous forensic tools and utilities, and work to the latest standards for digital evidence handling, reporting and forensic analysis. Whether the casework we undertake for you is criminal or civil, we have the skills, training and practical experience to provide a comprehensive service.

Forensic Incident Response

We can provide rapid response on site (covert or overt) as well as lab-based forensic imaging of digital media including PCs, servers, networks and removable media. We use a number of industry-standard methodologies and forensic Applications including Encase FTK, Safeback and Linux DD.

Forensic Investigations

We conduct forensic examination and analysis of a wide range of digital media including hard disks, floppy disks, CD and DVD media, mobile phones, organisers (PDAs), digital storage cards (such as SmartDrive, CompactFlash and memory sticks) printers, fax machines, SANs, NASs, email systems and so on.

In fact, we pride ourselves on conducting leading edge research and developing forensic protocols for the examination of some of the more exotic forensic and

Unusual devices, such as satellite navigation systems, games consoles and television access control systems.

Internet Investigations

Working with our strategic partner, AccessData, we provide a comprehensive range of covert internet investigation and analysis including email analysis, packet capture, web profiling, identity determination, posting and visibility monitoring, domain control mapping, identification of malicious posting sources, intellectual property Intelligence services and internet risk/threat mitigation.

Using highly-specialised proprietary software and hardware, coupled with our sophisticated human intelligence operations, we have the capability to mine information from the parts of the net that are not normally open to public scrutiny.

We can correlate vast volumes of disparate intelligence into meaningful information, giving us the ability to investigate threats to your products, intellectual property, market and channels









Information Security Assessments

We conduct information security, IT security and physical security policy and procedure audits using trained and accredited staff.

Information Security Evaluations

External and internal penetration testing using NSA-approved technical consultants and methodologies.

(Typical Assignments)

-  Network Vulnerability Assessment
-  Attack and Penetration Testing
-  Security Vulnerability resolution Support
-  Security Architecture review and Development
-  Security Policy Development and Implementation
-  Intrusion Detection System Analysis and Implementation
-  Firewall Analysis and Implementation
-  Virtual Private Networking (VPN)

eDisclosure and eDiscovery Consultancy







Services assisting either applicants and/or respondents to meet their objectives efficiently and economically.

Data Recovery Services

In the event of either logical or physical damage, we have the capability to recover data from all types of digital media including all RAID configurations.

Particular Expertise

Myriad View Limited has built up considerable expertise in:

-  Internet-related investigation into email abuse — in particular in tracing the source of malicious emails — software, music and video piracy/counterfeiting, brand damage, grey market and product diversion
-  Theft and misuse of intellectual property
-  Proving access to inappropriate content including pornography. Significant involvement in the investigation of child pornography distribution
-  Abuse of corporate systems such as fraud and stock manipulation
-  Data recovery in the event of malicious acts or accidental loss
-  Password recovery and recovery of encrypted material following malicious acts or accidental loss

OUR STRATEGIC PARTNERS

We believe the best way of offering you the best services to meet all eventualities is to work with a small number of strategic partners who have been proven to deliver the best services in their fields at the most advantageous prices.

We are very pleased to count the following teams as long-term strategic partners.



AccessData provides a broad spectrum of stand-alone and enterprise-class solutions that enable digital investigations of any kind, including computer forensics, incident response, eDiscovery, legal review, IP theft, compliance auditing and information assurance



Privileged Access Management

Comprehensive, integrated privileged access management solutions that provide visibility and control over all privileged accounts and users in your environment.

Vulnerability Management

Vulnerability management solutions that reveal risks in the proper context and enable smarter decision making with unmatched reporting, scalability and coverage.

Auditing & Protection

Unified Windows auditing, security, and compliance solutions for Active Directory, File System, Exchange, and SQL.



Insider Threat Detection and Prevention

The biggest security challenge organizations face today is **people**. Whether its employees, privileged users, or third parties, insiders introduce risk to your organization because they must be given access to critical applications, systems, and data to do their jobs effectively.

It's vital to understand your insider threat risk as an organization, so that you can defend yourself. **ObserveIT** helps companies identify and eliminate insider threat risk by focusing on user activity. With complete visibility into all activity on your network, you can not only catch and stop insider threats, but meet and surpass all compliance and regulatory requirements with ease.



PixAlert has been protecting corporate reputation and brand integrity of financial, healthcare, pharma and public sector organizations since 1999 through its innovative and advanced portfolio of critical data and image detection and protection software solutions.



CounterTack provides organizations with the solutions and tools to perform key phases of incident response including detection and malware analysis. Yet as targeted attacks have risen and attackers find new ways to remain persistent in the network, organizations often need reliable, scalable expert services to keep up with the latest cyber threats.



VERACODE

With our powerful combination of automation, process and speed, Veracode seamlessly integrates application security into software development, effectively eliminating vulnerabilities during the lowest-cost point in the development/deployment chain. Without the need for additional staff or equipment, Veracode customers ramp up quickly, see results and prove value on day one, and consistently see improvement over time.

It is this unique combination of process, technology and security experts that helped one financial services institution scale its program more than 600%, reduce the cost to remediate vulnerabilities by 75% and reduce overall vulnerabilities by 60% for an overall return on investment of 192%.



The AlienVault Unified Security Management™ (USM) platform provides five essential security capabilities in a single console, giving you everything you need to manage both compliance and threats. Understanding the sensitive nature of IT environments, we include active, passive and host-based technologies so that you can match the requirements of your particular environment.



NNT Change Tracker Enterprise™ delivers market-leading File Integrity Monitoring for any security and compliance initiative. Approved by hundreds of independent Auditors, QSAs and security specialists operating in all countries across the globe, NNT Change Tracker Enterprise™ protects banks, government departments and agencies, financial services providers, retailers, gaming resorts and restaurant chains, as well as airlines, museums and not-for-profit organizations. NNT Change Tracker Enterprise™ audits your IT estate for compliance with best practices in security configuration, provides real-time, zero day malware protection and protects systems from any unauthorized changes. Easiest to use - Most Fully Featured - Most Affordable

OUR TRAINING COURSES

Our extensive experience of performing forensic examinations has brought us into contact with many different situations. Throughout this time, we have been struck by a recurring theme.

In 90% of cases, evidences to be investigated would have been “damaged” by the actions of the client before we are called in. This can make our job more difficult, time consuming and costly than it would normally be. Therefore we help companies prevent these issues by offering basic computer Forensics and Incident trainings. We run these training courses, either in-house or externally.

Mitigating Business Risk

This is a high impact training seminar

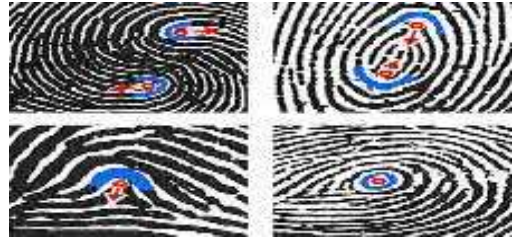
Entitled Mitigating Business risk using Digital Forensic Practices. It provides delegates with the knowledge they need to protect the evidence in the event of an incident and shows them how to integrate the principles and practices of computer Forensics into the policies and procedures of their organisations.

Building a Forensic First response

Designed for delegates who have completed Course ONE, this course provides the basic skills and knowledge to allow them to set up a basic digital forensic response capability. All the hardware and software required, plus two days of training on how to use it, are included in the fee.







Information Security awareness and training

Myriad View recognises that awareness of risks and available safeguard is the first line of defense for security of information systems and networks. Therefore, this training aims to provide practical advice for organisations to prepare and implement awareness raising initiatives to information security



ITIL

The Information Technology Infrastructure Library (ITIL) is a set of concepts and practices for Information Technology Services Management (ITSM), Information Technology (IT) development and IT operations. ITSM derives enormous benefit from a best practice approach as it is driven both by technology and the huge range of organisational environments in which it operates; it is in a state of constant evolution. Adopting ITIL can offer users a huge range of benefits that include:

-  Improved IT services
-  Reduced costs
-  Improved customer satisfaction through a more professional approach to service delivery
-  Improved productivity
-  Improved use of skills and experience
-  Improved delivery of third party service.

Lean & Six Sigma

Lean Six Sigma is a result of two powerful methodologies (Lean and Six Sigma) that have a complementary toolkit. Combining the two techniques with effective team skills has provided vast improvements








Lean

Is the elimination of waste, as seen from the customer and business perspective. Waste refers to the non-value-added tasks that a customer or employer would not pay for. Deployment of Lean is highly successful by using proven tools, properly

applying technology, getting things done systematically and quickly, and creating a high performance work environment.

Six Sigma

Is a measure of performance that strives for near perfection in all processes. Six Sigma is a systematic approach and information-driven methodology for eliminating process deficiencies and variation that increase costs and reduce revenues. Some of the benefits:

-  Dissatisfied customers
-  Poorly designed workflows to support changes in technology
-  Excessive waste and inefficiency
-  Declining revenue impacting cash flow and debt
-  Excessive number of process delays and work-arounds
-  Excessive costs
-  Multiple or inconsistent problem-solving approaches

Project Management Professional (PMP):

Project management is a discipline that can be applied to all industries, regardless of the product or service they are designed to deliver. Beyond its basic application across various industries, project management has tremendous value when effectively implemented to significantly increase the success of the product or service being delivered.

Certified Ethical Hacking

The **CEH** Program certifies individuals in the specific network security discipline of **Ethical Hacking** from a vendor-neutral perspective. The **Certified Ethical Hacker** certification will fortify the application knowledge of security officers, auditors, security professionals, site administrators, and anyone who is concerned about the integrity of the network infrastructure.

Digital Forensics for Legal Practitioners

This training introduces tech-challenged litigators to computer forensics and offer a host of practical strategies geared to helping you win your cases with the power of computer forensics and electronic discovery.

Network Fraud Analysis

The objective of network forensics is to identify malicious activities, discover their details, and to assess the damage. Network forensics begins by capturing network traffic and saving it in a useful format; the forensics analyst can then pores through the traffic logs to identify patterns and spot malicious activity.

Malware Forensics

This training is designed to help digital investigators identify malware on a computer system, pull malware apart to uncover its functionality and purpose, and determine the havoc malware wreaked on a subject system. Practical case scenarios are used throughout the training to demonstrate techniques and associated tools.

Log Management and Incident Response

One of the most challenging, yet rewarding, aspects of perimeter security is network log file analysis. This process involves trying to identify intrusions and intrusion attempts through vigilant monitoring and analysis of various log files and then correlating events among those files. Analyzing log files might sound a bit tedious to you, the techniques presented in this training can help you to gain a great deal of value from your files in a short amount of time.

Mobile Phone & E-mail Forensics

IT professionals need to take advantage of mobile forensics to help them crack cases and improve their investigations. Too many investigators are overlooking mobile phone forensics, and are missing out on a powerful source of forensic data.

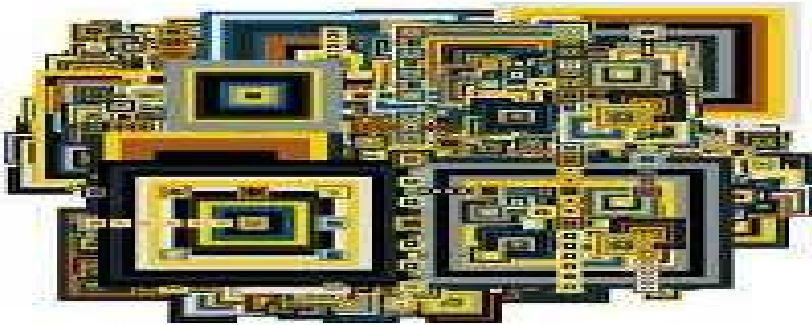
Penetration Testing guide & Methodology

This helps Companies to protect critical infrastructures, identify chinks in the armor, and prevent serious data breaches. This training is designed to teach you everything from the fundamentals of the Metasploit Framework to advanced techniques in exploitation

Computer Hacking Forensic Investigation

C|HFI v8 Program certifies individuals in the specific security discipline of computer forensics from a vendor-neutral perspective. The C|HFI certification will fortify the application knowledge of law enforcement personnel, system administrators, security officers, defense and military personal, legal professionals, bankers, security professionals, and anyone who is concerned about the integrity of the network infrastructure.

OUR TEAM



Adetunji Adeoje

Adetunji Adeoje (OCA, OCP, CEH CISA, ACFE, ESCA, CHFI, ACE, ACSE) is the president of Myriad View Limited, a leading information assurance and infrastructure architecture firm. Adetunji's specialty is network architecture, network security, and network intrusion investigations. His primary duties are to serve as project lead for security assessments helping businesses and government agencies secure their IT resources and assets. His skills and experience span Information Security, IT Governance, risk Management, Compliance, Computer Forensics and Business continuity. He has worked as IT security auditor, vulnerability Expert and system integrator at different capacities.

Ojo Olumide Ayoola

(MCT, MCSD, MCDDBA, MCTS, MCITP, OCA, CEH, CHFI, ECSA, ECSP, CSAD, LPT, CEI) In the field of ICT, Olumide's experience and skills are very much appealing. He has worked as I.T. Instructor and Solutions Consultant for the best I.T. companies and vendors in the world: Microsoft, Oracle, EC-Council, New Horizons, Aptech, Karox, NIIT, to mention just a few. In year 2010, he was honoured in the united States EC-Council Hackers Halted Hall of Fame with the Award of the African Ethical Hacker of the Year. He is the first West African to achieve the designation of Certified EC-Council Instructor (CEI). His accolade in the field of Information Technology cannot be over emphasized. He is still the best IT Security Expert in Africa today.

Ijeoma Okani

Ijeoma is an Industry Certified Holistic Information Security Professional with a background in Systems and Application Administration, and IT Management. She is experienced in Information Systems Security Design and Management with vast knowledge of developing and implementing IS security structures and processes for ensuring compliance to variant IS Security and Risk regulatory and voluntary standards. She is currently helping organisations in Nigeria achieve compliance to PCI DSS and ISO 27001 Standards. She is an experienced Trainer and facilitator of courses in Information Security and Risk Management, and Audit.

Ijeoma holds IT Security certifications including **CISSP, CRISC, CGEIT, CISA, CISM, ITIL** as well as an **MSc** in Information Security & Audit and an **MBA** in Human Resource Management. She is an IT security professional with vast experience in IT, and a well of knowledge in business management.

Olaoluwa B. Amudipe

Olaolu, with accounting and finance knowledge background at the Higher National Diploma (HND) program, he has served in numerous engagements as administrator cum project manager. He has some years of administrative and management experience, and He is committed to team work, he has teamed-up with numerous core IT security professionals in successful delivery of complex IT tasks as: ISO/IEC 27001:2013, Payment Cards Industry Data Security Standard certification and re-certification (PCI DSS) Projects in financial sector, holistic enterprise Networks, Web & Systems and Applications security assessment in financial sector, IT Vulnerability assessment and Penetration test and vulnerability remediation from the initiation to planning, execution, controlling and monitoring and to closing in accordance to Prince2 project management methodology and/or PMP Standard framework. He holds professional Certifications as: ISO/IEC 27001:2013 Lead Auditor (LA), Payment Cards Industry Professional (PCIP), Prince2, and CSE.

08096676514

www.myriadview.com

adetunji@myriadview.com