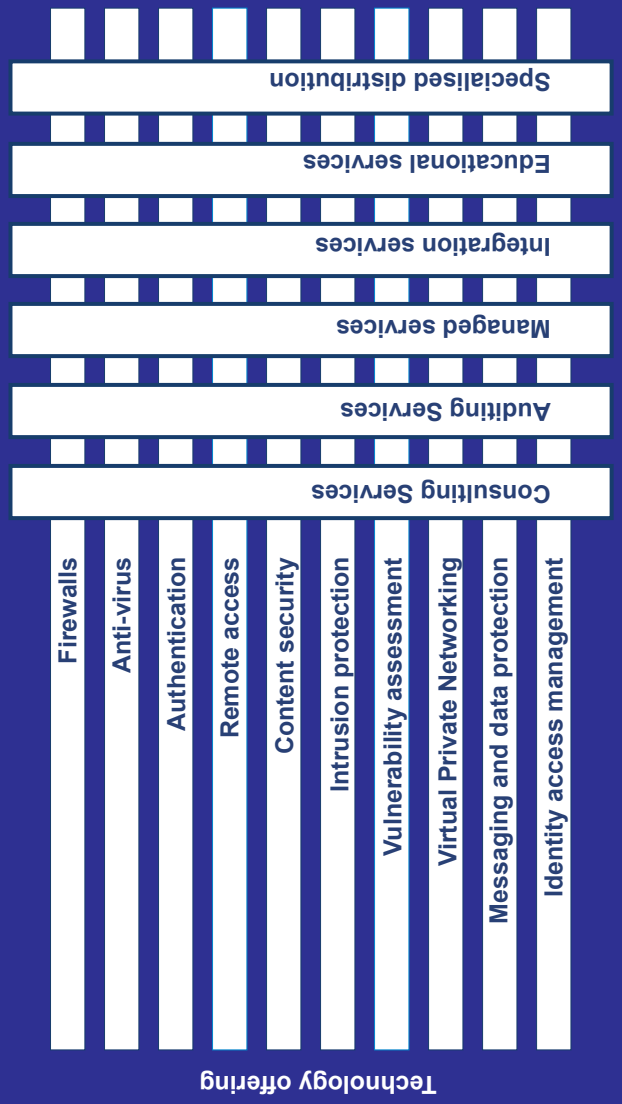

KEEP IT SECURE
Preferred Partner

CORPORATE BUSINESS SOLUTIONS

ISA
INFORMATION SECURITY ARCHITECTS
FOCUSED CONSULTANCY SERVICE

Data Privacy & Security Practitioners

REACH US

Information Security Architects Limited
#8 Lomo Adawu Street La-Accra, Ghana
P.O.B OS3082 Osu-Accra, Ghana

business@isa.com.gh
www.isa.com.gh
www.twitter.com/isaghana
www.facebook.com/isaghana

+233 302 760 912
+233 204 333 163
+233 264 284 133
+233 208 141 250

>>OVERVIEW <<

At ISA we ask; why buy products? Invest in solutions. Products are only fully effective if they are implemented and managed properly, that's a solution. An important and basic step in information security is the mapping of risks. Only with an understanding of these risks are you able to take informed decisions on whether or not to resolve them, and in which order. ISA provides regular training sessions where IT team learn how to organize security of their processes and data in an independent and proactive way.

OUR MISSION: *To exceed our customers' expectations with professional IT security consultation and solutions, allowing them to concentrate confidently on the development of their business activities.*

OUR VISION: *To be a world class provider of professional IT security services in developing and emerging countries.*

OUR VALUES: *Diligence | Integrity | Trust | Excellence | Fairness | Professionalism | Customer Care*

>> OUR SERVICES <<

FLAWSCOUTING

[Vulnerability Management/Penetration Testing]

To augment penetration testing, ISA offers FlawScouting: a subscription service, designed for frequent testing at a competitive price point. FlawScouting can accommodate several types of tests, including network, PCI, users and web applications. ISA believes our economic environment need more good-guy hackers out there if we are to keep up with the bad guys, so we do what we can to share our knowledge. This includes webcasts, recorded content, and full-fledged hands-on training.

Whether you need a full-scale Security Architecture Review or just an access to some security expertise, the ISA's consulting team is on standby to help. We believe strongly in a collaborative approach to security, and have used this approach consistently while working with development, business, management and IT security teams. ISA consultants work with each client to ensure they are providing quality, actionable recommendations. Our primary goal is to identify and prioritize security risks. The world is full of threats to networks, applications, data, and people. ISA 'FlawScouting' is a suite of vulnerability assessment service designed to help businesses keep up with regular testing.

Each ISA's FlawScouting service identifies:

- *Security concerns within the organization, provide the most actionable recommendations, and offer support in understanding the current security risks.*

#1 Passive-Scout - High-Level Site Scan (Free): Performs a passive assessment of any requested site. To do this, it will make a few normal web requests to the site. The requests will do the following:

- *Request the HTML for the home page of your site, context of robots.txt, content of crossdomain.xml and other resources as needed*

2# PCI-Scout -DSS Compliance Scans (ASV Scan): The PCI Security Standards Council requires certain organizations to use an Approved Scanning Vendor (ASV) on a quarterly basis in order to obtain and maintain PCI compliance with Data Security Standards (DSS). PCI-Scout from ISA is an approved scanning solution for PCI DSS compliance [QUALY'S]. PCI-Scout scans your externally-facing network for any security vulnerabilities that are relevant to your PCI DSS compliance status and provides a standard, actionable report.
Some of the benefits of PCI-Scout include:

- *Enumerate externally-facing assets that impact PCI DSS compliance, Identify externally-facing vulnerabilities, and Remediation steps for vulnerabilities.*

#3 Network-Scout: Fundamental Security Verification: Networks are in a constant state of flux as technology teams rush to meet the needs of their business operations. Many organizations have little idea what devices and applications are actually present on their networks or how they are connected internally or externally. Unfortunately what you don't know can hurt you. ISA Network-Scout can help fill that knowledge gap, thereby strengthening your security position.

Network Scout offers both internal and external network assessments. Using modern scanning techniques combined with manual verification techniques, Network-Scout provides organizations with an understanding of their existing security issues to:

- *Identify Existing Network Assets, Internal & External Options and Identify Security Weaknesses*

NB: Subscriptions are based on the size of the network being tested and is priced per scan on a subscription basis.

#4 Web-Scout: Dependable Application Scanning (OWASP): Today's web applications are more complex than ever and with these complexities come increased vulnerabilities. ISA Web-Scout is designed to help customers identify the vulnerabilities within their applications and give them the peace of mind that their applications are assessed regularly. **Web-Scout** is more than a simple scan of your web application. ISA security staff use manual testing techniques, combined with validation of automated scanning to provide a comprehensive vulnerability assessment. This combined testing allows ISA to provide Web-Scout customers with a better understanding of the flaws and risks their applications expose them too. Web-Scout undergo:

- *Automated & Manual Analysis, Consistent Scanning Schedules and Detailed Reporting Capabilities*

#5 User-Scout- Foundational Awareness Training: Your **organization's biggest asset and threat** is your **staff**. Regular awareness training is the industry

standard, but do you know if it's working? By using email and/or phone based social engineering attacks, User-Scout allows you to help your users understand the role that they play in the company's security posture. These phishing attacks are widely regarded as one of the top threats to cyber security today. ISA provides a regular testing pattern that ensures that the organization is able to measure its awareness while not becoming obvious to the employees.

- *User Awareness Testing, Phone & Email Assessments and Low Key Testing*

  mitigation; Penetration Testing, Patch Management *and* Service Management,

KNOWLEDGE TRANSFER & TRAINING

[Information Systems Vulnerability Management – (ISVM)]

Our flagship knowledge transfer services is a training course, developed and hosted by the ISA/Technology Lab. The ISA/Technology Lab has pursued a unique approach to InfoSec Technology Service by combining knowledge transfer with hands-on exercises. The exercises reinforce concepts by allowing participants to input commands into software applications and observe how they work. The Technology Lab is virtually outfitted with many applications and operating systems found in industry.

Training program runs intensively for 2-days, for system administrators, network engineers, application developers and IT security officers with information security responsibilities, but who may not have had training in ethical hacking or its related field. At least one year of field IT experience is preferred. This course provides participants with a technical grounding in networking concepts and technologies that are critical to IT operations in institutions, including TCP/IP networking protocols and common network infrastructures and configurations. The course examines key network perimeter security tools, including firewalls and intrusion detection systems (IDS).

Participants should be able to demonstrate the following skills, after taking the course:

- *Recognize where and how vulnerability management fits in with the company's overall information security program and IT operations.*
- *Identify the role a vulnerability management program has in safeguarding information and assets.*
- *Assess the adequacy of a patch management, vulnerability scanning and assessment, and penetration testing tools and their limitations*
- *Evaluate the adequacy of an organization's testing program*
- *Recognize key elements of an incident response program*
- *Discuss key technology terms related to information systems vulnerability management*
- *Assess the key risks, controls and processes in a supervisory context, including regulatory compliance issue*
- *Identify what the institution must do to respond to new threats to be able to articulate a risk mitigation strategy; that is reviewed to ensure that new applications and/or systems are treated from a holistic perspective, and that controls for all systems are re-evaluated for effectiveness periodically.*

Some Benefits include:

- Instructor Interactions, Course Manual; Live Demonstrations; Access to World-Class Lab Tools; Skills on Privacy Regulatory Concerns; Risk

CAREPLUS 24Hr SUPPORT

[Endpoint Security- Vendor Independent Service]

ISA incorporates advances in technology, best practices and an exceptional consulting team to create solutions designed to meet your real-time demands for secure, accessible information. Our solutions are organized into focused practices, managed and delivered by subject matter experts. We help organizations build, implement, manage and support the infrastructure for their critical business functions. Our security competencies stream across the following platform enterprise-wide: This includes Antivirus, Antispyware, SiteAdvisors, Desktop Firewalls, Spam Protection, Intrusion Detection & Prevention Systems, Centralized Policy Servers for desktop user-restriction management, Security Consultancy/Training, Data surveillance and Policy Documentation development. We know what we do and do what we know.

CarePlus 24hr Support is our service, programmed to support the client with consultancy services for endpoint security solutions. This include:

- *On-site Customer Visit With Helpdesk 24 Hours X 7*
- *Vulnerability Assessment*
- *Network/Host Checks & Scanning*
- *Routine Disk Cleanup*
- *Temporary File Deletion & Machine Cleaning Spyware*
- *Monitoring Of Malware Entry Points*
- *Low Priority Service Requests*
- *Detailed Reporting On Endpoint Security*
- *Endpoint Security Software Deployment & Updates*
- *Software Administration On-site Support*

ENPOINT SECURITY SOLUTION

[Kaspersky | Avast | Symantec | Eset | McAfee | AVG]

Workstations, servers and networks are being exposed to malware at an ever-increasing rate in today's Internet business environment. Planning and designing an enterprise-wide ***Endpoint Security*** solution is not simple as companies require the right skills and experience to assess their network architecture, identify points of entry for virus threats and develop appropriate security policies. ISA offers endpoint security Policy, Planning and Design services, provided by a team of experienced security professionals, to help clients get the most from their endpoint security protection. This program educates customers on how to properly install and deploy

their endpoint security solutions in a way that works best for their unique computing environment. ISA's drive is to promote customer self-sufficiency and to work with companies to help implement the right endpoint security solutions in their networked environments.

ISA's Endpoint Security Policy, Planning and Design service enables customers to:

Reduce Exposure To Viruses Without Impacting Productivity >>	*ISA's service helps clients map their virus alert reporting structure to organizational needs, ensuring the right people receive virus alerts at the right time.*
Develop Staff Skills >>	*ISA provides valuable hands-on training and endpoint security knowledge, along with training materials and reference guides that can be used throughout an organization.*
Lower Total Cost Of Ownership For The Right Endpoint Security Solution >>	*ISA helps companies achieve the optimum balance between network performance and up-to-the-minute virus protection.*
Analysis Of The Current Environment >>	*Security experts review and assess a company's virus protection practices—including network topology, architecture, environment and organizational structure—to determine endpoint security implications.*
Documentation Of The Computing Environment >>	*ISA provides documentation describing how a client's network topology is structured and used.*
Fully Tested Pilot Implementation >>	*ISA recommends policies and pro c e d u res that provide maximum virus protection with minimum impact on customer network performance.*
Detailed Project Plan For A Full Deployment >>	*ISA advises clients on how to implement policy and technology decisions necessary for the successful integration of the endpoint security product. Customers get a detailed, step-by-step project plan to follow.*

ISA endpoint security solutions include data security, network security, advanced threat prevention, forensics, remote access VPN and cyber security for complete endpoint protection.

Security Incident Event & Unified Threat Management Solution [SIEM/UTM]

[GFI / NNT / IPSwitch / Sophos / WatchGuard / Nexpose]

Our high-performance, powerful security information and event management [SIEM] solution focusses on event, threat, and risk data together to provide strong security intelligence, rapid incident respond, seamless log management, and compliance reporting- delivering the content required for adaptive security risk management. The SIEM is a complex set of technologies brought together to provide a holistic view into a unified view into not only your infrastructure but also workflow, compliance and log management. This solution provides a multitude of capabilities and services efficiently.

WHAT SIEM PROVIDES:

- *Log Management ; Event and Log collection*
- *Layered Centric Views or Heterogeneous:*
- *Normalization: a two-part function also referred to as "field mapping"*
- *Adaptability (Scalable): This dumbs down to being able to speak the language regardless of source vendor, format, type, and change or compliance requirement.*
- *Reporting and Alerting: provide automated verification of continuous monitoring, trends and auditing.*

BENEFITS OF SIEM

- *Provides centralized security event management.*
- *Provides correlation and normalization for context and alerting.*
- *Provides reporting on all ingested data.*
- *It can take in data from virtually any vendor or in-house applications.*

The Information Security Architects also render the next-generation cloud-service firewall solution: Unified threat management Service, known as UTM. This is a single security solution, and usually a single security appliance, that provides multiple security functions at a single point on the network. In simple terms, the service allows an administrator to monitor and manage a wide variety of security-related applications and infrastructure components through a single management console. Our UTM appliance solution protects the enterprise edge with the following bundled and integrated services in a single unit:

- *Antivirus, anti-spyware, anti-spam, network firewalling, intrusion detection & prevention, content filtering & leak prevention, load balancing, SSL & SSH inspection and Identity-based access control also known as layer-8 security. In addition to this base protection the UTM solution also cover remote routing, network address translation (NAT), and virtual private network (VPN) support*

WHAT UTM DOES TO MALWARE ATTACKS:

UTM appliances in its best capacity reduces such attacks effectively by creating a single point of defense and providing a single console, instead of using separate appliances and vendors for each specific security task, as each aspect has to be managed and updated individually in order to remain current in the face of the latest forms of malware and cybercrime.

Data Encryption Solution

[File Encryption / Full Disk Encryption / Encrypted USB Drives]

For our industry experience, possessing corporate information on a standard USB flash drive can easily get misplaced or stolen and the resulting data breach, can be ruinous. For these and many reasons we do provide for data privacy/security on an encrypted drive; our service solutions can support full-disk encryption across the corporate network, file encryption and removable drives. Through our solutions partners we provide one of the easiest way to ensure that data on flash drives is protected by encryption is to buy an encrypted flash drive, which encrypt data automatically in hardware and can be used on computers running Windows, Linux and Mac OS X.

Data Privacy Service

[Privacy Impact Assessment / Privacy Policy / Compliance]

This service involves a systematic assessment of a project and identifies the impact that the project might have on the privacy of individuals, and sets out recommendations for managing, minimizing or eliminating that impact. *It takes only one Product Manager unaware of the privacy requirement structure to cause a privacy incident.* The new employee is also liable to such attack. Information Security Architects,is well-skilled for a Privacy Impact Assessment (PIA); one of its purpose built intensive security tests for every company that:

- *Outdoors a new product,*
- *Embarks on global expansion, and/or*
- *Partake in merger and acquisition activities.*

Our service brings you…

- *A cornerstone for privacy compliance*
- *Address complex privacy compliance and risk management challenges*
- *Cost-effective way to ensure privacy compliance.*
- *Reduce risk and provide business with better visibility of privacy and security concerns.*
- *Decrease the risk of financial loss caused by compensation and penalties*
- *Decrease the risk of damage to reputation (Privacy Incident consequence)*
- *Part of implementing Privacy-by-design Principles. It must be included in the product or service development at every stage of production.*

From the diaries…




ISA Team members at various privacy and security engagements >>>>>>>

The Brands we work with…

Nessus vulnerability scanner · GFI LanGuard Network security scanner and patch management · RAPID7 · NNT Workplace Solutions

Cyberoam A SOPHOS Company · Symantec · KASPERSKY · AVG · eset Enjoy Safer Technology · Ipswitch WhatsUpGold · avast! be free

OUR PATNERS

Secure Reach · NETWATCH Technologies · BLACKCASTLE · ASD Africa Solution Distributor · BlackWall Solutions · AiTEK Delivering Technology · software distribution