Service Catalogue

2011 - 2012

Executive Summary

As the world's first not-for-profit comprehensive global public-private partnership against cyber threats, the International Multilateral Partnership Against Cyber Threats (IMPACT) is the cybersecurity executing agent of the United Nations' specialized agency - the International Telecommunication Union (ITU). As the world's first comprehensive alliance against cyber threats, IMPACT brings together governments, academia and industry experts to enhance the global community's capabilities in dealing with cyber threats.

Based in Cyberjaya, Malaysia, IMPACT is the operational home of ITU's Global Cybersecurity Agenda (GCA). As ITU's cybersecurity executing agent, IMPACT provides ITU's 192 Member States access to expertise, facilities and resources to effectively address cyber threats, as well as assisting United Nations agencies in protecting their ICT infrastructures.

ITU - IMPACT

On 3rd September 2008, IMPACT and the ITU formally entered into a Memorandum of Understanding (MoU) in which IMPACT's state-of-the-art Global HQ in Cyberjaya, Malaysia, effectively became the physical and operational home of the GCA. Under this landmark collaboration, IMPACT provides the ITU's 192 Member States with the expertise, facilities and resources to effectively address the world's most serious cyber threats.

In May 2010, the relationships with IMPACT was further strengthened, in light with the outstanding results achieved in assisting ITU Member States (as of October 2011, 137 Member States have formally agreed to be part of the ITU IMPACT endeavor).

A new MoU was signed between ITU and IMPACT, identifying IMPACT as executing agent of ITU on Cybersecurity.

Overview of the SERVICES

The converged synergies between the five work areas of the GCA, the services and infrastructures provided by IMPACT made a joint partnership a logical next step in the global fight against cyber threats, cybercrime and other malicious uses of the Internet. ITU-IMPACT currently provides the following services:

- Vulnerability Assessment
- Penetration Testing
- External Penetration Testing
- Internal Penetration Testing
- Web Application Assessment
- On Demand Web Application Scanning Services
- Reactive Services
- Alerts & Warnings
- Incident Response Handling
- Proactive Services
- Log Retention & Management
- Data Leakage Prevention

- CSIMS (spell out)
- Honey Net
- CIRT (spell out)
- Human Capacity Building and training

Contents

ITU-IMPACT Profile

On the 3rd September 2008, the International Telecommunication Union (ITU) and the International Multilateral Partnership Against Cyber Threats (IMPACT) went into a Memorandum of Understanding (MoU) which subsequently made IMPACT the physical and operational home for ITU's Global Cybersecurity Agenda. In a landmark agreement signed in May 2011, IMPACT now is the cybersecurity executing agent for the United Nations' specialized agency, the International Telecommunication Union (ITU). With this cooperation, IMPACT will now provide cybersecurity services to ITU's 192 Member States as well as the United Nations' system.

The dangers of cyber threats continue to evolve and spike at a pervasive rate. The risks are further compounded as increasingly connected societies transcend geographical and physical borders, where stakeholders communicate in real-time. Utilizing the same networks and links that bind us globally, cyber threats and attacks are able to strike from virtually anywhere in the world, potentially causing catastrophic social and economic harm to countries that are oceans away.

Governments cannot contain these cyber threats singlehandedly through domestic measures alone. Neither should governments be left to grapple with this danger on their own any longer, as the expertise and skill to combat these cyber threats are largely dispersed across the globe. In many cases, the solution is in the private sector or academia.

There is an absolute need to converge and share the information as well as resources that will escalate the safety of our cybersecurity. Without expert collaboration and knowledge sharing, individual countries lessen their ability to respond to cyber threats and may potentially expose themselves and their neighbors to greater risks online, as perpetrators learn to exploit national, regional and global information and communication technology weaknesses one-by-one.

And this is the void IMPACT fills, enabling governments and stakeholders with vested interests in cybersecurity to converge, connect and collaborate for a tighter and a more cohesive more forward in the defense against adversaries online.

Through IMPACT and its GRC, partner countries can enhance their knowledge and awareness of the cyber threat landscape that affects them, while learning about possible solutions to overcome these malicious attacks. With IMPACT operationalizing ITU's GCA, current Member States of the ITU are eligible to become IMPACT's partner countries, enabling access to its GRC, intellectual property, consulting services, reports and more.

1.1 Global Cybersecurity Agenda

The GCA is the ITU framework for international cooperation aimed at proposing and implementing strategies for solutions to enhance confidence and security in the information society. The GCA intends to build on existing national and regional initiatives to avoid the duplication of work and encourage and foster collaboration amongst all relevant partners.

The GCA was launched by the ITU's Secretary-General, Dr. Hamadoun Touré on 17th May 2007 as framework for international cooperation in building confidence and security in the information society.

The GCA focuses on five main areas of cybersecurity:

- Legal measures
- Technical and procedural measures
- Organizational structures
- Capacity-building
- International cooperation

Together, these areas of cybersecurity provide a comprehensive and consistent approach towards a multi-stakeholder framework for a more secure and safer information society.

Vulnerability Assessment

Vulnerability assessment is a process of identifying, quantifying and prioritizing system weaknesses in order to apply a patch or fix to prevent a compromise. It is a comprehensive look at the security posture of your organization. We can safely assist you to perform external and internal scanning accurately to detect security vulnerabilities across your entire infrastructure before it is being exploited by an attacker. The completed assessment includes analysis of both internal and external threats and vulnerabilities.

2.1 Objectives

Some of the goals and objectives for an organization to perform a vulnerability assessment are as follows:

- To identify weakness or potential vulnerabilities on the IT infrastructure so that issues could be promptly rectified;
- To determine how secure your network is from malicious (or even unintentional) theft or damage due to un-patched, weak, or mis-configured security settings on the IT infrastructure;
- Known vulnerabilities can be prioritized based on impact or criticality of the IT or data asset;
- Remediation or mitigation of the identified vulnerabilities can be properly budgeted and planned according to the prioritization or criticality of IT and data assets; and
- Compliancy with information security laws, mandates, and regulations can be achieved by conducting a vulnerability assessment.

2.2 Service Offerings

ITU-IMPACT has a separate division within its Professional Services focused purely on vulnerability assessment. The vulnerability assessment is ideally a repetitive process which continues at least once a month to scan the systems to ensure that the configurations are correct and proper security patches are applied. ITU-IMPACT offers both Manual and Automated Vulnerability Assessment.

The services offered by ITU-IMPACT offers the following services in Vulnerability Assessment:

- Finding all the hosts on the network
- Fingerprinting their Operating Systems
- Detecting open ports on the system
- Mapping the ports to various network services
- Detecting the version of the services running
- Mapping the service version to various discovered security vulnerabilities
- Verifying if the service on the host is actually vulnerable to an attack or if it has been patched
- Prioritizing the vulnerabilities according to severity

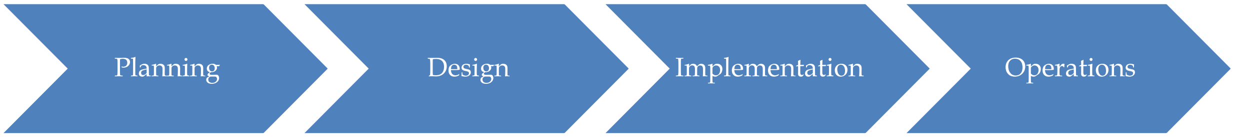
ITU-IMPACT offers two levels of vulnerability assessment

- External Level Vulnerability Assessment
- Internal Level Vulnerability Assessment

The assessments are carried out based on the organization side after identifying the critical infrastructures and interfaces.

2.3 Vulnerability Assessment Methodology

ITU-IMPACT approach to the implementation of Vulnerability Assessment analysis is delivered in four stages.



2.3.1 Planning (Stage 1)

Planning a vulnerability analysis requires determining the scope of systems and processes that represent the typical networking components as well as systems that are essential to providing security services. ITU-IMPACT will work closely with the organization's representatives to discover components and attributes of their environment that need evaluation.

Planning elements may include:

- Interview management and selected individuals to determine critical points within the network and identify appropriate samples of systems that adequately represent the infrastructure;
- Determining scope of the analysis and affected locations, systems, business units, or other environmental attributes that may impact the thoroughness of the analysis; and
- Collecting architectural and technical information to determine priorities and execution processes.

2.3.2 Design (Stage 2)

Based on the characteristics of the organization’s environment, our security professionals will establish an analysis process that will quickly locate and measure the vulnerabilities.

Design elements may include:

- Developing or leveraging information collection protocols and strategies to efficiently obtain the necessary information from system resources and networking elements;
- Creating an analysis process and initial testing procedures that reflect the internal systems and devices; and
- Establishing activities for interfacing with the client staff to obtain greater insight to operational practices to evaluate security operations.

2.3.3 Implementation (Stage 3)

Vulnerabilities information will be collected and reviewed to identify areas that need immediate attention as well as to communicate additional requirements needed for further investigation.

Analysis activities may include:

- Regular meetings and interviews with the staff; and
- Review of collected configurations and processes

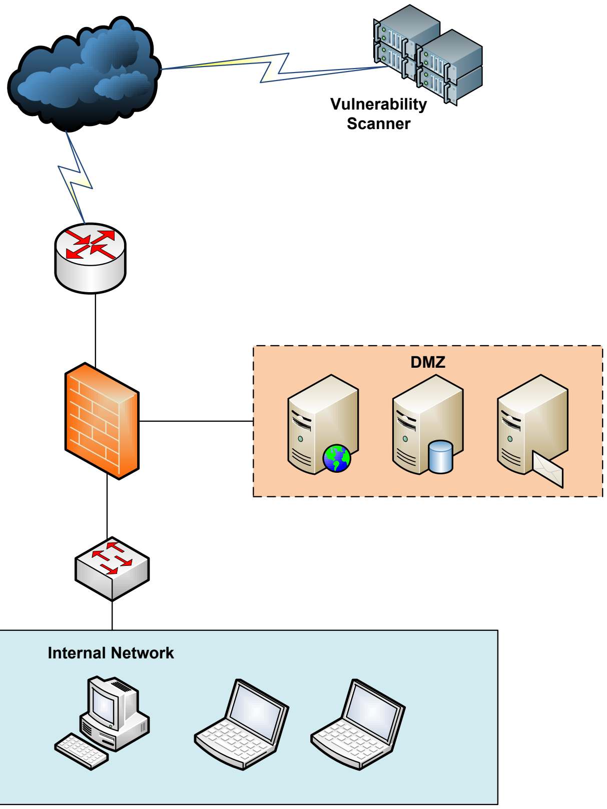
2.3.4 Operations (Stage 4)

As the vulnerabilities are identified, documented and prioritized, it is necessary to establish a plan for rectifying the vulnerabilities. Based on the information collected, ITU-IMPACT will work with the organization to create an initial outline of procedures required to reduce the number of security vulnerabilities found.

Operations elements may include:

- Initial plan for addressing the high priority vulnerabilities ;
- Preliminary process enhancements to improve security and reduce operational vulnerabilities; and
- Knowledge transfer of findings

2.4 Operation Paradigm



2.5 Scope

Scope of vulnerability assessment should include all network devices and application, primarily:

- Desktops
- Servers
- Operating Systems
- Applications
- Routers
- Firewalls
- PDA's
- Wireless devices

Penetration Testing

Penetration testing (also called pen testing) is the practice of testing a computer system or network to find vulnerabilities that an attacker could exploit. ITU-IMPACT provides two type of penetration testing

- Internal Penetration Testing
- External Penetration Testing

External penetration testing focuses on identifying and validating vulnerabilities that exist on all Internet-accessible services within your organization critical IT infrastructure such as web server, email server, DNS, etc. Only through penetration testing we can validate which vulnerabilities are the biggest risk to your environment and the highest priority to fix.

Internal penetration testing is a comprehensive security test of all systems related directly and indirectly to your business. It mimics the actions of an actual attacker exploiting weaknesses in network security without the usual danger. The test examines internal IT systems for any weakness that could be used to disrupt the confidentiality, availability, or integrity of the network, thereby allowing the organization to address each weakness.

3.1 Objectives

The Objectives for penetration testing are based on the type of pen test performed. They are different for external and internal penetration testing. External Penetration Testing focuses but not limited to the following objectives:

- To examine the current networks/systems from an external attacker’s perspective and how far they can get in once they've gained access.
- To execute a real-world attack on critical infrastructure and understand the level of risk that exists at a single moment in time;
- To validate all security vulnerabilities associated with your organization Internet-facing environment.
- To provide recommendations and details to facilitate a cost-effective and targeted mitigation approach.

On the other hand the objectives of internal penetration testing are:

- Perform information gathering on internal networks to discover live systems covering wired and wireless environment
- Iteratively identify and analyse accessible systems on identified networks.
- Analyze hosts for operating system, configuration and running services.
- Enumerate services and platforms.
- Identify known vulnerabilities on the running systems.
- Exploit, where appropriate, any security vulnerabilities which provide escalated privileges.

3.2 Service Offerings

External penetration testing techniques include, but are not limited to:

- Perform information gathering on networks associated with the victim organization using sources such as DNS, WHOIS, Usenet news and public websites;
- Iteratively identify and analyze accessible systems on identified networks;
- Analyze hosts for operating system, configuration and daemon vulnerabilities;
- Exploit, where appropriate, any security vulnerabilities which provide escalated privileges or network visibility, such as access to the DMZ or internal network; and
- Conduct a series of scenario analyses based on the information retrieved, such as attempting access to internal servers, customer records, or performing web site defacement.

Internal penetration testing techniques include, but are not limited to:

- Perform information gathering on internal networks to discover live systems covering wired and wireless environment.
- Iteratively identify and analyze accessible systems on identified networks.
- Analyze hosts for operating system, configuration and running services.
- Enumerate services and platforms.
- Identify known vulnerabilities on the running systems.
- Exploit, where appropriate, any security vulnerabilities which provide escalated privileges.

3.3 Penetration Testing Methodology

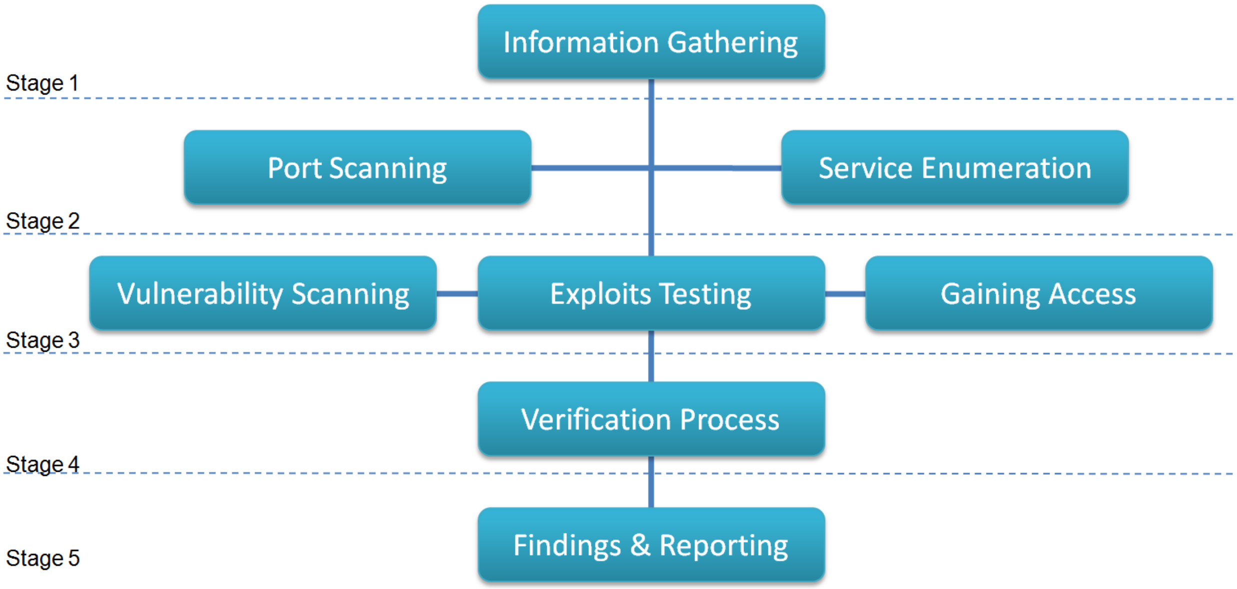
ITU-IMPACT penetration testing methodology is adopted from Open Source Security Testing Organization Methodology Manual (OSSTMM). The OSSTMM focuses on the technical details of exactly which items need to be tested, what to do before, during, and after a security test, and how to measure the results. The OSSTMM covers the whole process of risk assessment involved in a penetration test, from initial requirements analysis to report generation. The six areas of testing methodology covered are:

- Information security
- Process security
- Internet technology security
- Communications security
- Wireless security
- Physical security

Based on this framework, ITU-IMPACT is able to form a comprehensive baseline for testing that ensures a thorough and comprehensive penetration test has been undertaken.

The aim of penetration testing is to emulate hacker attacks on the IT environment and identify any weaknesses, which may provide unauthorized access to systems or data. We employ the same manual techniques used by hackers to perform the attack. This allows us to identify vulnerabilities and conditions which would be neglected by automated testing methods.

Our approach for conducting the infrastructure penetration testing is illustrated in the diagram below:



3.3.1 Information Gathering (Stage 1)

Information gathering is essentially using the Internet to find all the information required about the target (company and its resources) using both technical (DNS/WHOIS) and non-technical (search engines, news groups, mailing lists etc) methods. The objective of this exercise is to find the number of reachable systems to be tested without exceeding the legal limits. Information gathering does not require contact with the target system. Information is collected (mainly) from public sources on the Internet and organizations that hold public information.

3.3.2 Port Scanning & Enumeration (Stage 2)

This stage involves active probing of the target system to enumerate live hosts or accessible Internet services within the network range and to discover open port. We need to identify hosts that are within the scope of the test. This is crucial since we are bound by time constraint. It may not be possible for us to test every host that we found within the network. Once we have identified the hosts, we will perform further probing to look for responses that can distinguish unique systems to operating system and version level of running services.

3.3.3 Vulnerability Identification & Exploits Testing (Stage 3)

We will test for vulnerabilities using commercial and open source tools to determine existing holes and the system patch level. This stage is important for the Penetration Tester team to identify and incorporate current underground scripts/exploits into the test. We may attempt to exploit any vulnerable services found on the systems. Services that is prone to password cracking attack such as FTP, Windows Terminal Service, Web application with user login form, etc.

3.3.4 Verification Process (Stage 4)

Some reported vulnerabilities might be false positives. This stage is a process of verifying vulnerabilities found in Stage 3 to eliminate the false positives. Our qualified security experts will review reported vulnerabilities to verify whether it is a valid and real threat to the application. Only verified vulnerability will be documented in details as finding in the report.

3.3.5 Findings and Reporting (Stage 5)

Documentation is an essential part of every penetration test. During the pentest, all steps are thoroughly documented. This ensures that after the test all actions can be reconstructed in detail. At the end of the pentest, this documentation is used as a basis for the final report, which makes the results of the test comprehensible for the technical administration, as well as the management.

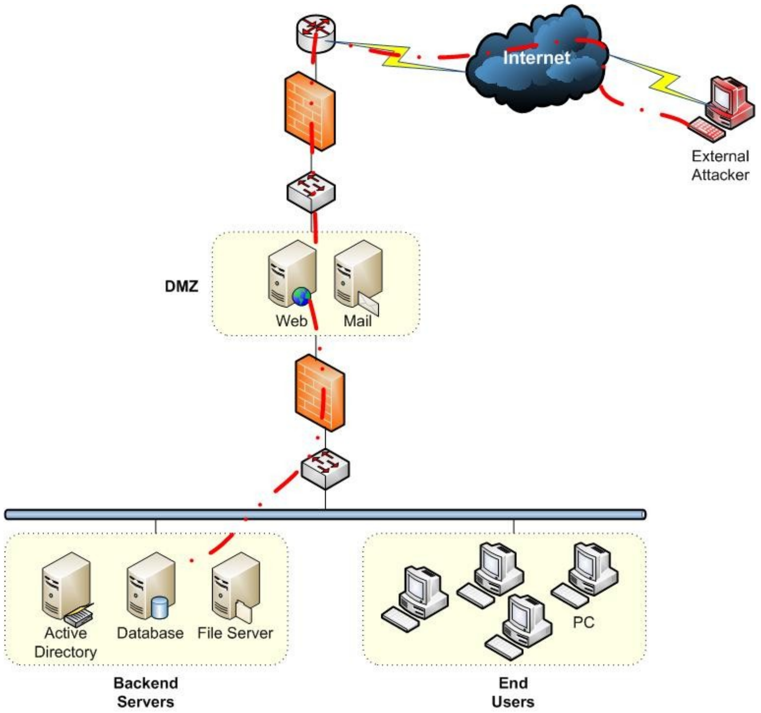
3.4 Testing Tools

The tools used for the security assessment are a mixture of commercially available and open source as depicted in the table below. We will use at least two (2) different tools to perform the test to ensure the accuracy of the result.

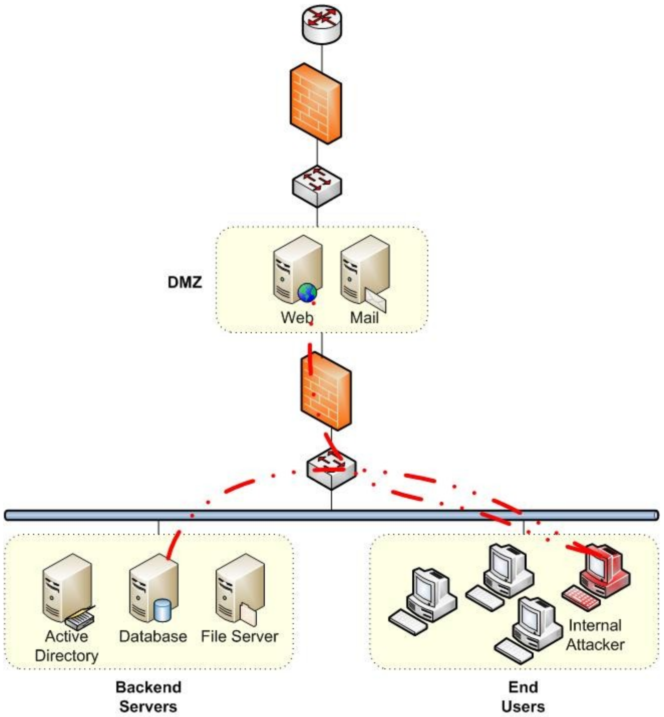
Function	Tool	Description
Network Scanner	**Nmap** http://insecure.org/nmap	Nmap is an open source tool for network exploration and security auditing. It was designed to rapidly scan large networks.
	ScanLine http://www.foundstone.com/us/resources/proddesc/scanline.htm	ScanLine is a command-line port scanner for all Windows platforms. It can handle huge numbers and ranges of IP addresses without a problem.

Web Application Scanner	**Acunetix** http://www.acunetix.com	Automatically scans web applications/website (shopping carts, forms, dynamic content, etc.) and web services for vulnerabilities to SQL injection, Blind SQL Injection, Cross site scripting, Google hacking, CRLF Injection & other web attacks.
SQL Injections	**Pangolin** http://www.nosec.org	Pangolin is an automatic SQL injection penetration testing tool used to detect and take advantage of SQL injection vulnerabilities on web applications.
Proxy	**Paros Proxy** http://www.parosproxy.org	Paros is a valuable testing tool for web security and vulnerability testing. It can be used to spider/crawl the entire site, and then execute scanned vulnerability scanner tests. Paros Proxy utility can be used to tamper or manipulate any http or https traffic on the fly.
Vulnerability Scanner	**Nessus** http://www.nessus.org	Nessus is the defacto Open-source vulnerability scanner utilized within the IT Security industry today. It is extensible with multiple platform support and ability to target all OS.
	Nexpose http://www.rapid7.com/products/vulnerability-management.jsp	NeXpose is vulnerability assessment software that accurately scans Web applications, databases, networks, operating systems and other software to find threats, assess their risk and devise a remediation plan to quickly mitigate these risks.
Exploits	**Metasploit** http://www.metasploit.com	Metasploit is designed as an automated penetration testing tool. It provides an attack platform with exploits for commonly known vulnerabilities.

3.5 Operation Paradigm



External Penetration Testing



Internal Penetration Testing

3.6 Scope

Scope of external penetration testing should include devices that are accessible via public IP addresses, such as:

- Firewalls
- Routers
- DNS
- External services including servers on your DMZ (for e.g. web server, mail server, FTP, etc.)
- Remote access services such as dial-up modems and IPSec endpoints.

Scope for internal penetration testing should include devices that are associated with the target environment, such as:

- Firewalls
- Routers and Switches
- Email and DNS Services
- Other Services
- Wireless Networks

Web Application Assessment

Web application penetration testing refers to a set of services used to detect various security issues with web applications and identify known vulnerabilities such as URL manipulation, SQL injection, cross-site scripting, back-end authentication, password in memory, session hijacking, buffer overflow, web server configuration, credential management, Click jacking, etc.

Web application assessment is aimed at identifying security vulnerabilities and exploitable element residing within the web application that could be used to affect the confidentiality, availability or integrity of information. The test is an attempt to simulate what an attacker can do on the web application from the external point of view. Our testing methodology is based on OWASP Top 10 web application vulnerabilities, which focus on the critical web application security risks.

Web applications are becoming more prevalent and increasingly more sophisticated, and as such they are critical to almost all major online businesses. As with most security issues involving organization/server communications, Web application vulnerabilities generally stem from improper handling of organization requests and/or a lack of input validation checking on the part of the developer.

The very nature of Web applications - their ability to collate, process and disseminate information over the Internet - exposes them in two ways. First and most obviously, they have total exposure by nature of being publicly accessible. This makes security through obscurity impossible and heightens the requirement for hardened code. Second and most critically from a penetration testing perspective, they process data elements from within HTTP requests - a protocol that can employ a myriad of encoding and encapsulation techniques.

The test will cover any web application that is accessible over a network such as the Internet or an intranet. Our standard application security assessments test the application from both unauthenticated and authenticated perspectives of user roles in scope. The test is an attempt to simulate what an attacker can do on the web application from the external point of view.

4.1 Objectives

The objectives of a Web Application Penetration Test are as follows:

- To discover vulnerabilities in a web application’s web interfaces from an external party browser point of view.
- To provide remediation or mitigation of the identified risks, threats, and vulnerabilities.
- To provide management with an understanding of the current level of security risk from web-based services.

4.2 Service Offerings

Web Application Penetration Testing Techniques include, but are not limited to:

- Application mapping to expose all known (and unknown) links within the web application
- Site crawling to understand structure and data-entry / login forms.
- Perform directory enumeration to find all directory paths and possibilities on the web server, including hidden directories which could possibly contain sensitive information
- Vulnerability identification and exploits testing

4.3 Web Application Assessment Methodology

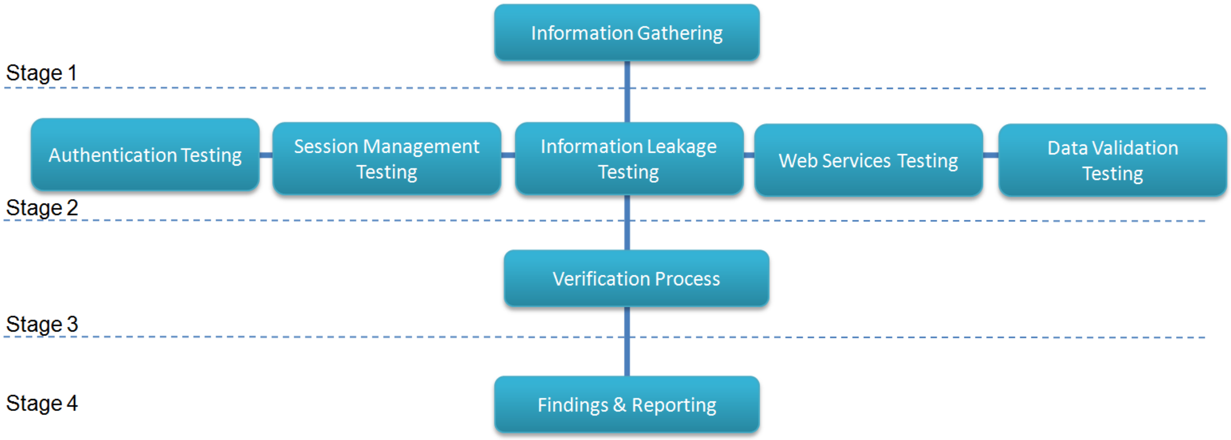
ITU-IMPACT testing methodology is based on Open Web Application Security Project (OWASP) Top 10 web application vulnerabilities, which focus on the critical web application security risks. OWASP testing methodology is the defacto web application security assessment guide and has been adopted by the international community's as standard for web application testing framework.

The framework for OWASP web application testing is summarized in the table below:

Application Threat	Vulnerability	Business Impact
Injection Flaws	Attacker can manipulate queries sent to the application to communicate directly with the database.	Attackers can access backend database information. All data could be stolen, modified or deleted. Injection can sometimes lead to complete host takeover.
Cross Site Scripting (XSS)	XSS flaws occur whenever an application takes untrusted data and sends it to a web browser without proper validation. XSS allows attackers to execute scripts in the victim's browser.	Attackers can execute scripts in a victim's browser to hijack user sessions, deface web sites, insert hostile content, redirect users, hijack the user's browser using malware, etc.
Broken Authentication & Session Management	Session tokens not guarded or invalidated properly by the application.	Attackers are able to compromise passwords, keys, session tokens, or exploit other implementation flaws to impersonate users. Privileged accounts are frequently targeted.

Insecure Direct Object Reference	Attacker can access sensitive files and resources within the application without authentication.	Without an access control check or other protection, attackers can manipulate these references to access unauthorized data.
Cross-Site Request Forgery	Attacker can invoke “blind” actions on web applications, impersonating as a trusted user.	This allows the attacker to force the victim’s browser to generate requests the vulnerable application thinks are legitimate requests from the victim.
Security Misconfiguration	This flaw such as default accounts, unused pages, unpatched flaws, unprotected files and directories can happen at any level of an application stack, including the platform, web server, application server, framework, and custom code.	Such flaws frequently give attackers unauthorized access to some system data or functionality. Occasionally, such flaws result in a complete system compromise.
Insecure Cryptographic Storage	Many web applications do not properly protect sensitive data, such as credit cards, SSNs, and authentication credentials, with appropriate encryption or hashing.	Attackers may steal or modify such weakly protected data to conduct identity theft, credit card fraud, or other crimes.
Failure to Restrict URL Access	Hacker can access unauthorized resources.	Hacker can forcefully browse and access a page past the login page.
Insufficient Transport Layer Protection	Sensitive info sent unencrypted over insecure channel.	Unencrypted credentials “sniffed” and used by hacker to impersonate users.
Unvalidated Redirects and Forwards	Web applications frequently redirect and forward users to other pages and websites, and use untrusted data to determine the destination pages.	Such redirects may attempt to install malware or trick victims into disclosing passwords or other sensitive information.

Our approach for conducting the web application assessment is illustrated in the diagram below:



4.3.1 Information Gathering (Stage 1)

This is the initial stage of any information security audit. We will attempt to explore every possible avenue to gain more understanding of the target and its resources. Some of the techniques include site crawling to understand the application structure and data-entry/login forms, application mapping to expose and follow all known (and unknown) links located on the site, perform directory enumeration to find all directory paths and possibilities on the web server, including hidden directories which could possibly contain sensitive information.

4.3.2 Vulnerability Identification & Exploits Testing (Stage 2)

In this stage, we will perform web application assessment to identify any known vulnerabilities. The test will be based on OWASP guidelines for testing web application security risks. Techniques include but are not limited to:

- Parameter Manipulation
- Cross-Site Scripting
- SQL Injections
- Directory Transversal
- Buffer Overflow
- Hidden Fields Manipulation
- Brute Force attack
- Cookie Manipulation

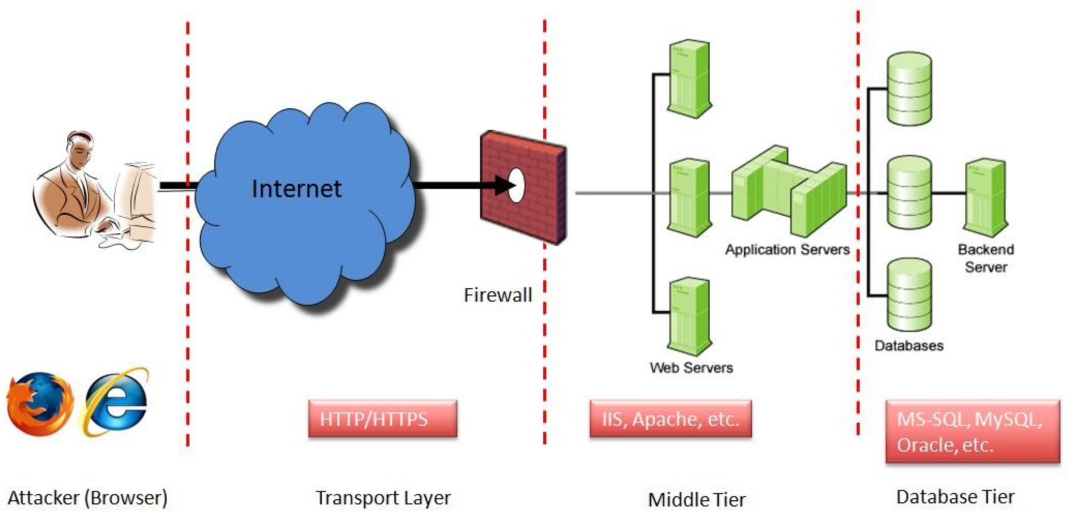
4.3.3 Verification Process (Stage 3)

Some reported vulnerabilities might be false positives. This stage is a process of verifying vulnerabilities found in Stage 2 to eliminate the false positives. Our qualified security experts will review reported vulnerabilities to verify whether it is a valid and real threat to the application. Only verified vulnerability will be documented in details as finding in the report.

4.3.4 Findings and Reporting (Stage 4)

Documentation is an essential part of every penetration test. During the pentest, all steps are thoroughly documented. This ensures that after the test all actions can be reconstructed in detail. At the end of the pentest, this documentation is used as a basis for the final report, which makes the results of the test comprehensible for the technical administration, as well as the management.

4.4 Operation Paradigm



4.5 Scope

Scope of web application assessment covers:

- Any web application that is accessible over a network such as the Internet or an intranet.
- Perform test on the application from both unauthenticated and authenticated perspectives of user roles in scope.

On-Demand Web Application Scanning Services

On-demand scan is the most accurate and cost-effective approach to conducing a vulnerability scan. It is cost-effective because it is an on-demand service, and not an expensive on-premises software solution. Our on-demand scan service is designed to proactively identify where vulnerabilities may exist from both network sources and web applications against hacker attacks. Unlike network based scanning tools, our On-Demand scanning service tests for security defects at the web application level, where most of hacking attacks actually occur, to detect and report on vulnerabilities before they get exploited by hackers.

5.1 Objectives

Some of the goals and objectives for an organization to subscribe for on-demand scan are as follows:

- To identify weakness or potential vulnerabilities on the IT infrastructure so that issues could be promptly rectified;
- To determine how secure your system is from malicious (or even unintentional) theft or damage due to un-patched, weak, or misconfigured security settings on the IT infrastructure; and
- Remediation or mitigation of the identified vulnerabilities can be properly budgeted and planned according to the prioritization or criticality of IT assets and data assets.

5.2 Service Offerings

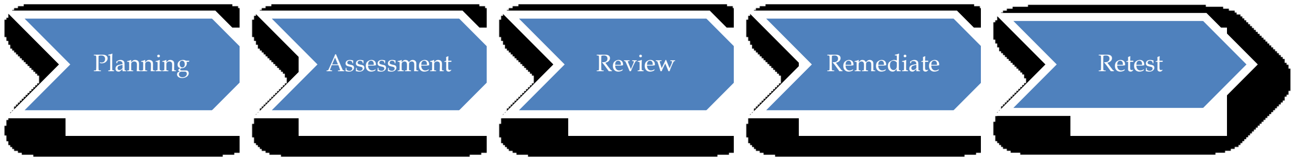
While most security technologies play a defensive role, consistent vulnerability scanning is proactive and is considered a vital part of your vulnerability risk management program. An attacker particularly ones that seek confidential or sensitive information, can spend time over the course of months testing defenses and determining the best course for a successful attack.

Our on-demand-scans service will probe all applications residing on your enterprise’s web servers, proxy servers, web application servers, as well as all active web services. The scanner crawls your entire website, analyzing each file it finds and displays the entire website structure. It then performs an automatic audit for common web security vulnerabilities by launching a series of Web attacks.

We will scan the customer’s Web application remotely from our data center and sends reports directly to the organization with details of the discovered security vulnerabilities. It is up to the organization to request the vulnerability assessment scans as needed or to set up scheduled scans (periodic scanning) at certain intervals.

5.3 On Demand Web Application Scanning Methodology

Our approach to the implementation of on demand web application scanning is based on the below model



5.3.1 Planning (Stage 1)

Planning stage involves reviewing the testing requirement and develop testing plan with stakeholders for implementing a web application scanning system which run whenever demanded.

5.3.2 Assessment (Stage 2)

In this stage the web application is thoroughly tested and assessed with potentially 100+ different categories of attack. The stage mainly focuses on identifying critical vulnerabilities. It also evaluates the underlying business risks.

5.3.3 Review (Stage 3)

During review accurate and actionable reports are created. All the uncovered vulnerabilities are met and reviewed and remedial steps are recommended.

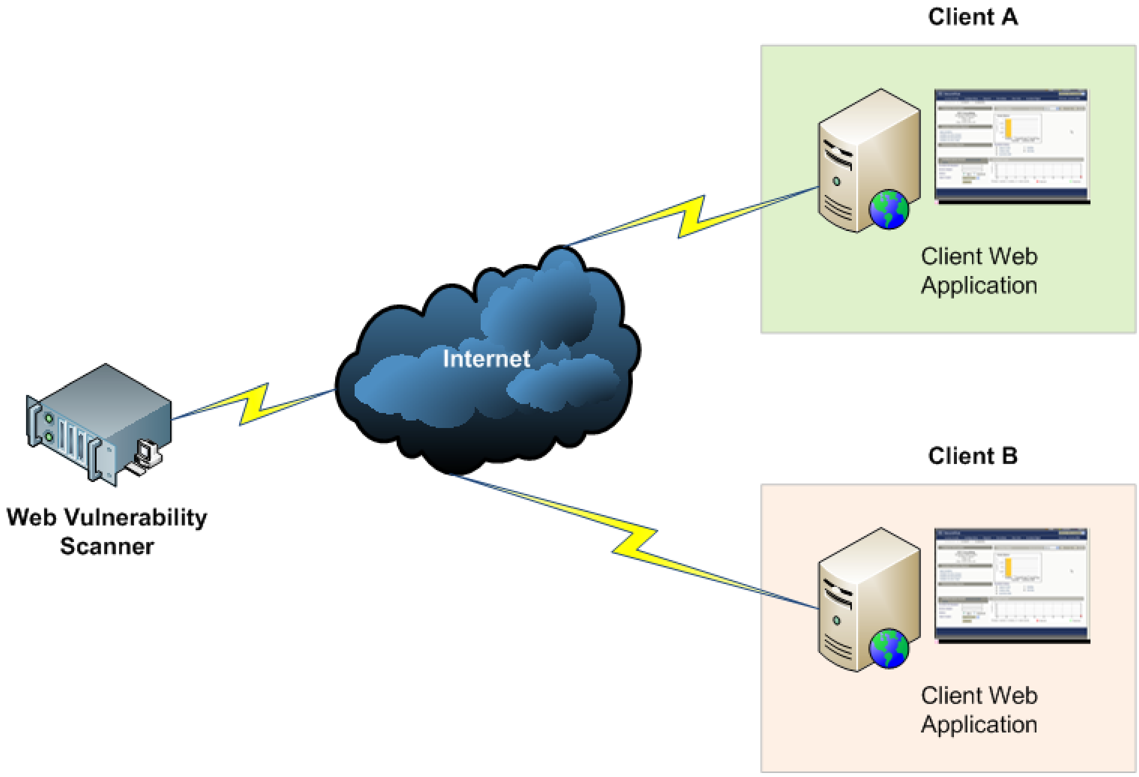
5.3.4 Remediate (Stage 4)

Advice and consultation is provided to remediate and fix all the issues that have been uncovered during the previous stages of execution.

5.3.5 Retest (Stage 5)

The application is then retested to ensure that all the vulnerabilities have been resolved and no issues exist in the application.

5.4 Operation Paradigm



5.5 Scope

Our on-demand-scans service complies with OWASP Top 10 Most Critical Web Application Security Risks. The scope of the service covers the following:

- Detects vulnerabilities from a current database of known existing flaws
- Deep scanning capabilities detect and report alerts for the following types of vulnerabilities:
  - Cross Site Scripting (XSS)
  - SQL Injection Flaws
  - Information Leakage and Improper Error Handling
  - Broken Authentication and Session Management
  - Failure to Restrict URL Access
  - Improper Data Validation
  - Cross Site Request Forgery (CSRF)
  - Insecure Direct Object Reference
  - Insecure Cryptographic Storage
  - Insecure Communications
  - Malicious File Execution
- Analyzes an application's code content, including PHP, ASP, .NET components, and JavaScript
- Detects sensitive content in HTML (transaction card data, SSNs)

- Crawls and analyzes all website components, including Flash objects, SOAP app-to-app communication links, and AJAX routines
- Finds SQL injection flaws, cross-site scripting
- Uses browser emulation to find and test all links
- Deep level scans and through coverage
- Low false positives/negatives ratio

Reactive Services

Reactive approaches are those procedures that organizations use once they discover that some of their systems have been compromised by an intruder or attack program.

Just as every company takes some measures to prevent future business losses, each also has plans in place to respond to such losses when the proactive measures either were not effective, or did not exist. Reactive methods include Disaster Recovery Plans, use of private investigation services and loss recovery specialists, reinstallation of operating systems and applications on compromised systems, or switching to alternate systems in other locations. Having an appropriate set of reactive responses prepared and ready to implement is just as important as having proactive measures in place.

A difficult set of decisions needs to be made in deciding how much resource (time, money, and people) to dedicate to proactive approaches and how much to reactive approaches. These decisions can be further complicated by decisions about whether to use in-house resources, or to outsource. The remainder of this paper discusses these issues and focuses specifically on computer and network technologies.

ITU-IMPACT offers different reactive services which provide support to its clients on understanding compromises in their system as well as affected regions like Ports, IP Addresses.

6.1 Objectives

The objectives of ITU-IMPACT reactive services are as follows:

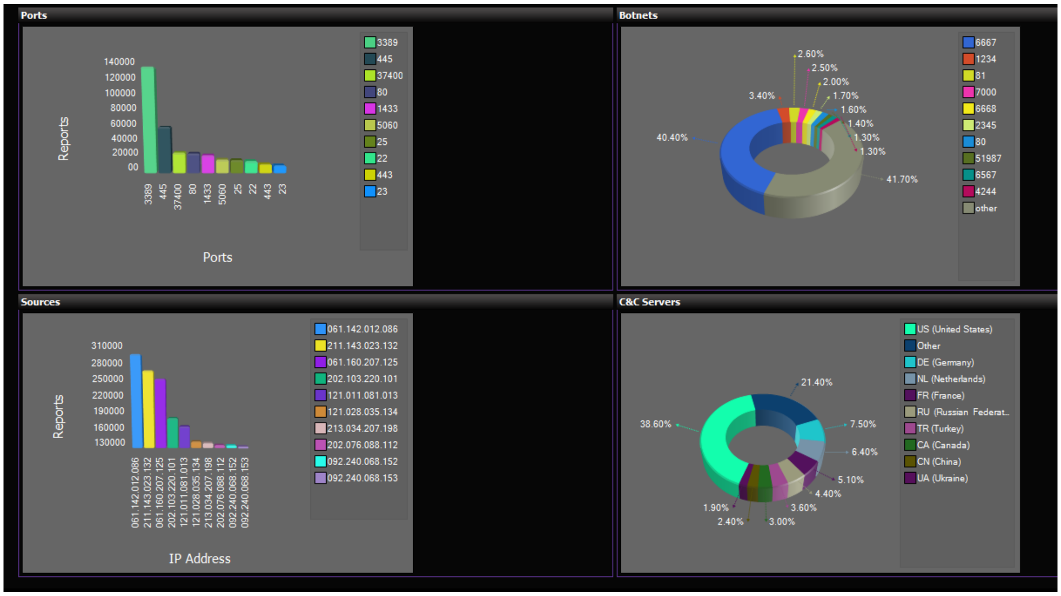
- To provide its subscribers with information on the vulnerabilities on the system.
- To alert the users with information on possible vulnerability in the system.
- To provide warning mechanism to its users about the possibility of vulnerabilities existing in the network as well probability of intrusion.
- Provide the subscribers with a knowledge base of their machine classified based on the risk present in the system.

6.2 Service Offerings

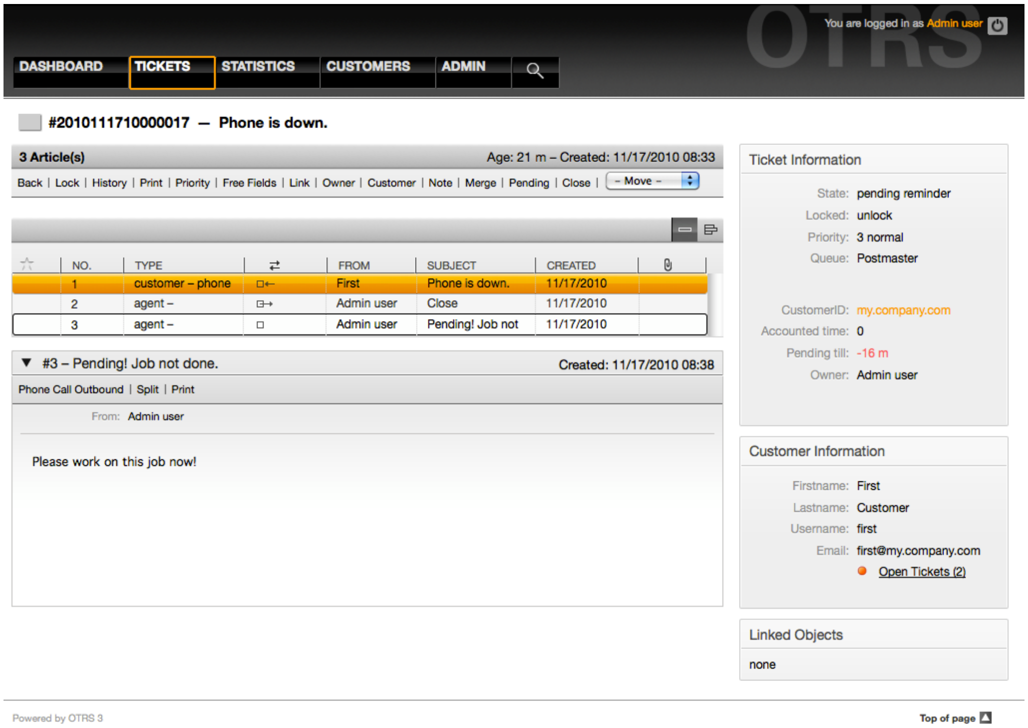
For reactive services the ITU-IMPACT provides the following offerings

- Alerts & Warning System for disseminating information related to computer security
- Incident Response Handling System for responding to request and analyzing incidents.
- Threat analysis system which provides the subscribers with access to threat analysis reports produced by ITU-IMPACT response centers' analysts.
- Solution to respond to requests and analyze incidents.

6.3 Screenshots



Alert & Warning System



#2010111710000017 — Phone is down.

3 Article(s) Age: 21 m – Created: 11/17/2010 08:33

Back | Lock | History | Print | Priority | Free Fields | Link | Owner | Customer | Note | Merge | Pending | Close | – Move –

☆	NO.	TYPE	⇄	FROM	SUBJECT	CREATED
	1	customer – phone	□←	First	Phone is down.	11/17/2010
	2	agent –	□→	Admin user	Close	11/17/2010
	3	agent –	□	Admin user	Pending! Job not	11/17/2010

▼ #3 – Pending! Job not done. Created: 11/17/2010 08:38

Phone Call Outbound | Split | Print

From: Admin user

Please work on this job now!

Ticket Information

State: pending reminder
Locked: unlock
Priority: 3 normal
Queue: Postmaster

CustomerID: my.company.com
Accounted time: 0
Pending till: -16 m
Owner: Admin user

Customer Information

Firstname: First
Lastname: Customer
Username: first
Email: first@my.company.com
● Open Tickets (2)

Linked Objects

none

Powered by OTRS 3

Top of page

Incident Handling System

6.4 Scope

The scope of the Reactive Services is limited to the constituencies that they serve for e.g. government agencies, UN system.

Proactive Services

Proactive approaches include all measures that are taken with the goal of preventing host-based or network-based attacks from successfully compromising systems.

Every modern organization realizes the value of dedicating some resources to the prevention of expensive damages that will likely occur if such preventive measures are not taken. Banks use thick steel and concrete vaults with advanced electronic systems to prevent and detect break-ins. Many companies, from convenience stores to casinos, use cameras to record business activities, the idea being that cameras both deter theft and help identify perpetrators when thefts do occur. Some organizations have started using Intrusion Detection and Response Systems (IDRSes) to try to detect computer intrusions and then activate defensive measures when an attack is detected.

Proactive Services also includes methodologies for retention and management for log and other information related to network's hardware like firewall's, servers, routers, switches, etc.

7.1 Objectives

The objective of ITU-IMPACT proactive services are:

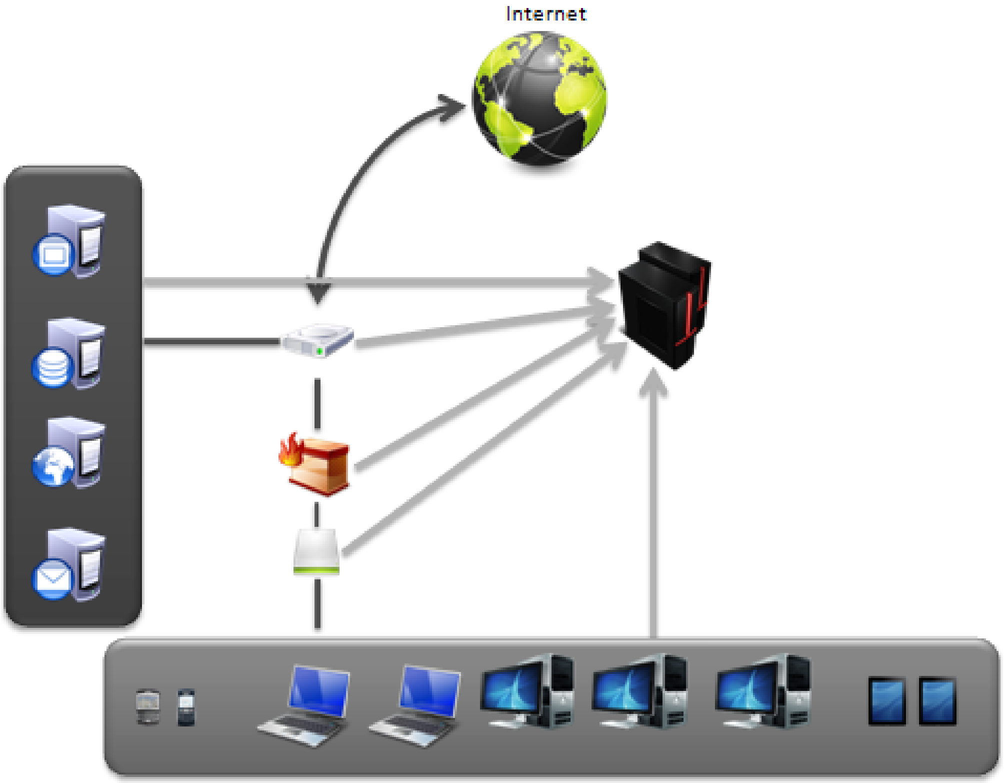
- To provide solution for log retention and Management.
- To provide methodologies for analysis of captured log and data.
- Provide real time monitoring and analysis of network environments.

7.2 Service Offerings

Offerings provided by ITU-IMPACT include:

- Solution for aggregation and storing of network and application logs for archival process and analysis.
- Real time security monitoring and analysis of network environments.

7.3 Operational paradigm



7.4 Scope

Scope for Proactive Services includes network devices that are associated with the user environment, such as:

- Firewalls
- Routers
- Intrusion Detection/Prevention System (IDS/IPS)

Data Leakage Prevention

Data leakage prevention (DLP) is a computer security term referring to systems that identify, monitor, and protect data in use (e.g. endpoint actions), data in motion (e.g. network actions), and data at rest (e.g. data storage) through deep content inspection, contextual security analysis of transaction (attributes of originator, data object, medium, timing, recipient/destination and so on) and with a centralized management framework. Data leakage prevention tools can be roughly compared to application-level firewalls. Like firewalls, they examine the content of outbound data, rather than just ports and packet types, and ultimately decide what can leave the organization.

Information is one of a business's most important assets. Organizations want to be able to access information from anywhere, on any device, and collaborate with almost anyone. The need for information to be 'free' presents many security and risk management challenges. Organizations have moved from securing the IT infrastructure to securing information. To do this, they must understand where critical data is used and where it is stored. Adding to this problem is the continuous pressure from corporate and regulatory compliance requirements, customer and employee privacy concerns, and the rising cost of a data loss incident.

Most organizations employ safeguards to control sensitive information. Often, however, these controls are inconsistent and are managed at different points in the organization with different levels of diligence and effectiveness. The result is that despite their efforts, organizations around the globe leak significant amounts of sensitive information. These leaks create significant risk to the organization, their customers and business partners with the potential to negatively impact an organization's reputation, compliance, competitive advantage, finances, and customer trust and business partnerships.

A comprehensive solution will help an organization find, classify, and control the use of sensitive data throughout the company while providing the benefits such as:

- Protect critical business data and intellectual property
- Identifying and analyzing data at all control points including at the endpoint, at rest, at the message server, and on the network.
- Preventing the inadvertent or malicious disclosure of sensitive information.
- Improve business processes with the development of new policies, controls and testing.
- Addressing government and industry information protection regulations.

8.1 Objectives

Most Data Leakage Prevention solutions include a suite of technologies that facilitates three key objectives:

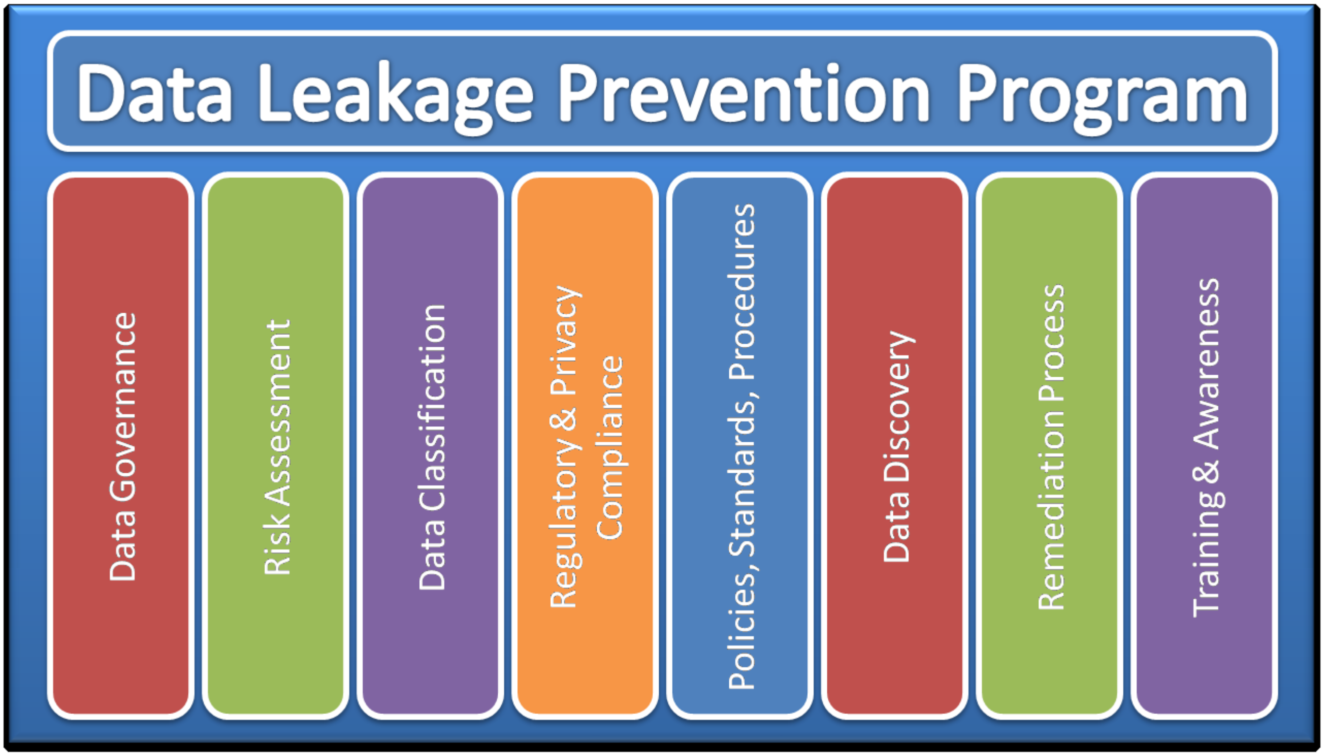
- Locate and catalogue sensitive information stored throughout the enterprise.
- Monitor and control the movement of sensitive information across corporate networks.
- Monitor and control the movement of sensitive information on end-user systems.

8.2 Benefits

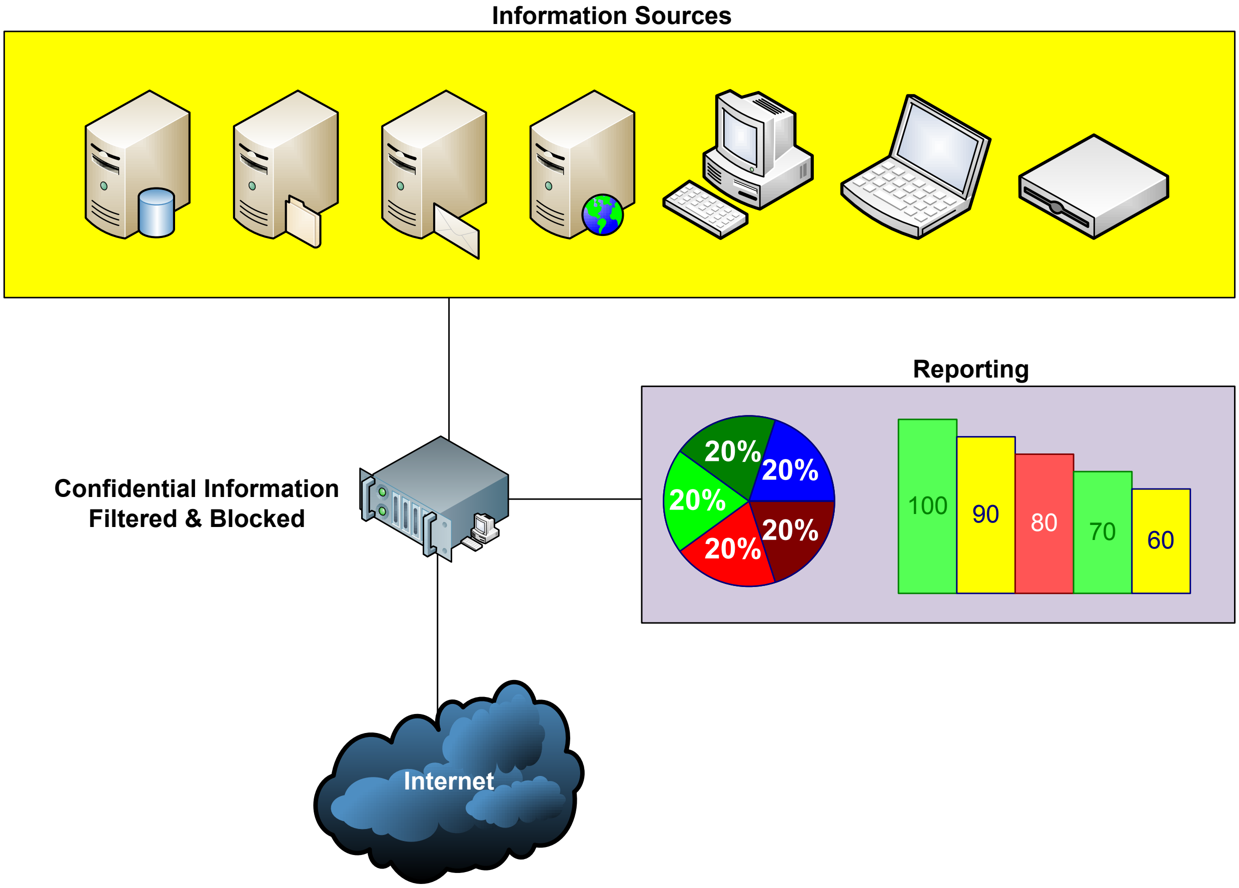
A comprehensive solution will help an organization find, classify, and control the use of sensitive data throughout the company while providing the benefits such as:

- Protect critical organization data and intellectual property
- Identifying and analyzing data at all control points including at the endpoint, at rest, at the message server, and on the network.
- Preventing the inadvertent or malicious disclosure of sensitive information.
- Improve business processes with the development of new policies, controls and testing.
- Addressing government and industry information protection regulations.

8.3 Service Offerings



8.4 Operation Paradigm



Cybersecurity Information Management System (CSIMS)

Most of the organizations have the contemporary security solutions like IDS /IPS, Antivirus and firewalls but still they suffer security breaches. The key issue with these individual security devices is that it takes a lot of effort to actively monitor and manage them. Since these devices work independent of each other, there would always be a chance where a well-crafted attack might breach the security perimeter. So despite of huge investments, the organization remains vulnerable to threats.

ITU IMPACT Cybersecurity Information Management System (CSIMS) aims to provision various security services to the organization by helping manage their security devices (firewall, IPS/ IDS, Anti- virus, etc):

- Real time monitoring- of all security incidents on a 24x7X365 basis
- Accurate Incident Detection – differentiate events from incidents via system automation and global correlation
- Quick Incident Response – By adopting International Standards of Incident Handling
- Mitigation of Risk – Proactive detection of threats and vulnerabilities.

9.1 Objectives

The objectives of the service offering are:

- Provide a centralized consolidation point for all perimeter defense security devices logs including:
    - Firewalls
    - Intrusion Detection System (IDS) / Intrusion Prevention System (IPS)
    - Antivirus Manager
    - Antispam Manager
    - Routers
    - Servers (Windows/Linux)
- Provide a correlation engine that identifies security threats based on device configuration rules and threat patterns
- Reduced response time for resolving security incidents
- Enhanced response for newly discovered vulnerabilities
- Access to security experts to resolve security incidents.

9.2 Service Offerings

ITU-IMPACT has designed and built the CSIMS to be used with data collection and correlation technologies from multiple vendors to provide comprehensive managed security services to organizations.

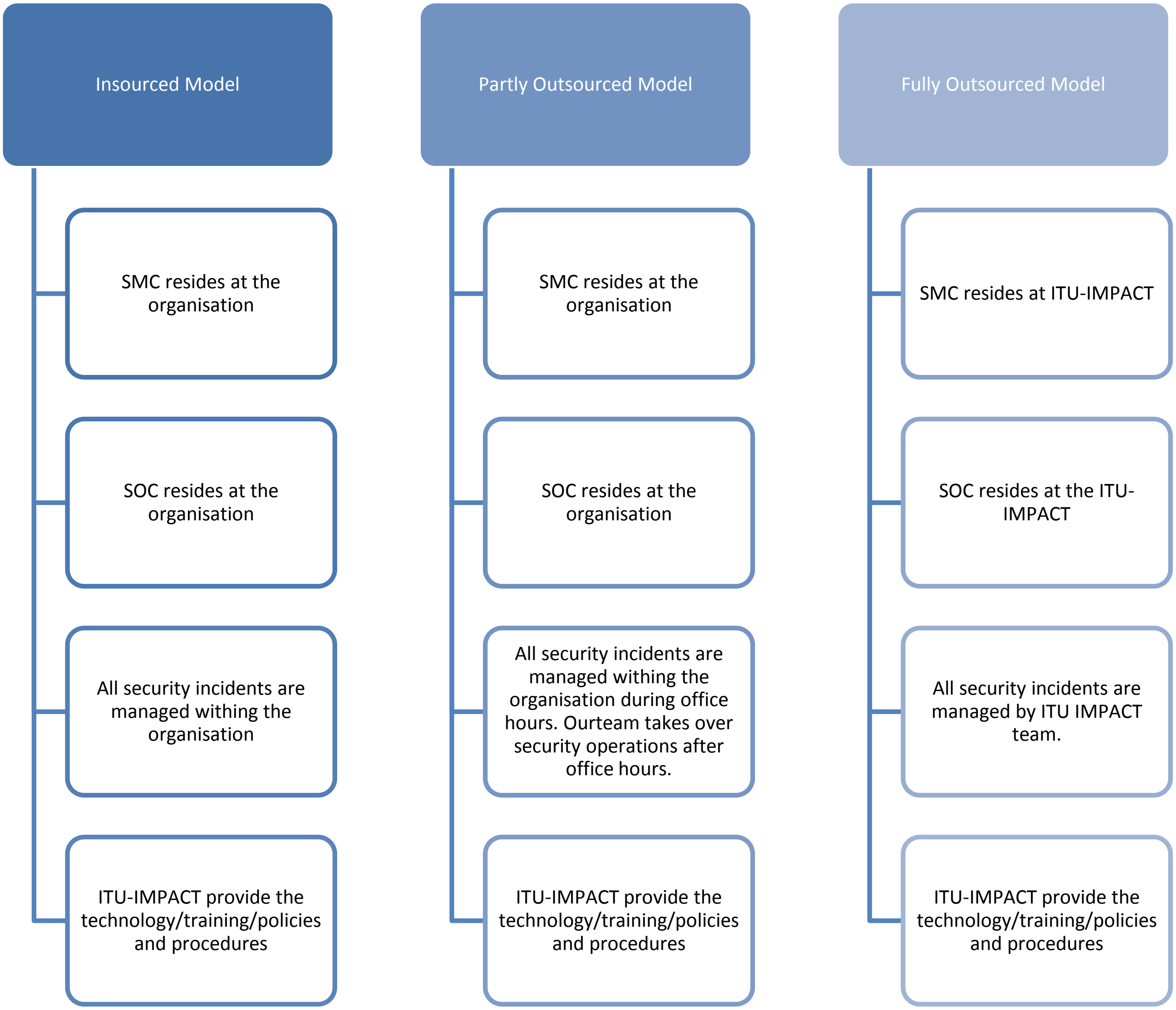
CSIMS is designed from ground up based on security policies and procedures. CSIMS provides proactive as well as reactive measures as a complete security management solution. Proactive measures are designed to stop attacks before they begin, reactive measures are designed to quickly detect and deal with security attacks.

Proactive measures: CSIMS provides services to provide early warning of attacks and vulnerabilities, so that organizations can proactively secure their networks and systems from impending attacks. These services are in the form of security threat advisories and vulnerability updates posted on the portal and/or sent via e-mail.

Reactive measures: CSIMS provides remote management of security devices with 24x7x365 real-time monitoring, protection and response – backed by a service level agreement. CSIMS is built on leading edge technologies in event analysis, ticketing and reporting. The organization events are collected and sent to a Security Operations Centre (SOC) where analysis is performed. Security experts at the SOC will determine the appropriate action to be taken, on a 24x7x365 basis.

All the core requirements, such as data ingress, business logic, process control, and database, trouble ticketing and reporting are built into the CSIMS solution.

9.3 Operation Paradigm



Insourced Model

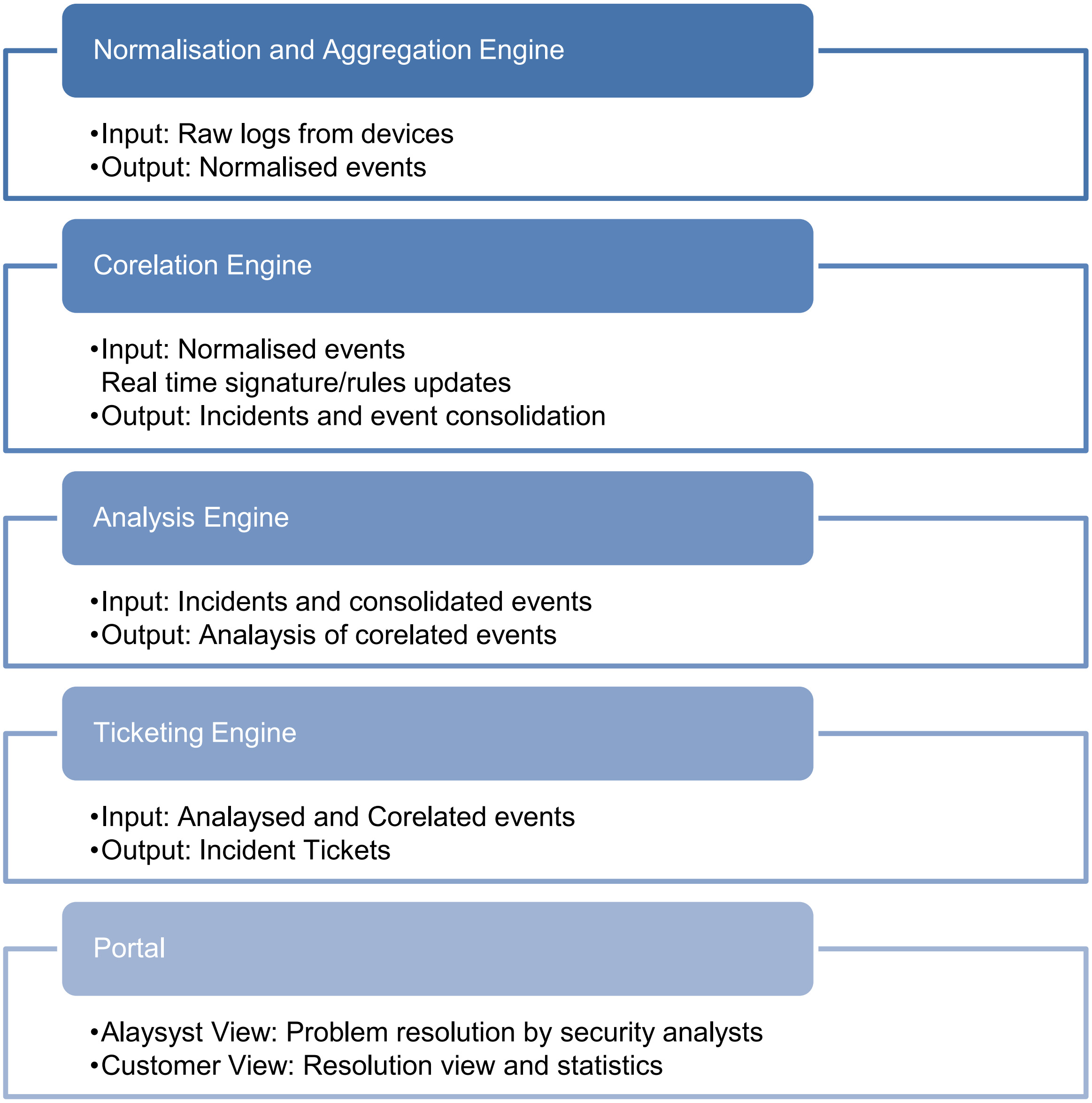
- SMC resides at the organisation
- SOC resides at the organisation
- All security incidents are managed withing the organisation
- ITU-IMPACT provide the technology/training/policies and procedures

Partly Outsourced Model

- SMC resides at the organisation
- SOC resides at the organisation
- All security incidents are managed withing the organisation during office hours. Ourteam takes over security operations after office hours.
- ITU-IMPACT provide the technology/training/policies and procedures

Fully Outsourced Model

- SMC resides at ITU-IMPACT
- SOC resides at the ITU-IMPACT
- All security incidents are managed by ITU IMPACT team.
- ITU-IMPACT provide the technology/training/policies and procedures



Normalisation and Aggregation Engine

- Input: Raw logs from devices
- Output: Normalised events

Corelation Engine

- Input: Normalised events
  Real time signature/rules updates
- Output: Incidents and event consolidation

Analysis Engine

- Input: Incidents and consolidated events
- Output: Analaysis of corelated events

Ticketing Engine

- Input: Analaysed and Corelated events
- Output: Incident Tickets

Portal

- Alaysyst View: Problem resolution by security analysts
- Customer View: Resolution view and statistics

CSIMS Workflow

9.4 Scope

Supported list of devices that can be remotely monitored and/or managed by CSIMS

Device Type	Company
Firewall, Routers & VPN	BIG-IP®, Check Point®, CISCO® ASA, CISCO® IOS, CISCO® Router, CISCO® VPN, D-Link®, Ipchains, IpFw, Juniper Networks® NetScreen, Linksys® WAP11, ModSecurity®, Netfilter, SonicGuard SonicWall®
Switches	CISCO® CSS
IDS	CISCO® IPS, Portsentry, Shadow, Tripwire®
Monitoring	APC®-EMU, ArpWatch, Dell® OpenManage, Nagios®
AntiVirus/AntiSpam	ClamAV®, P3Scan, SpamAssassin
Database	Microsoft® SQL Server, Oracle®
SMTP/POP Server	Exim, Postfix®, Qpopper®, Sendmail®, Vpopmail
FTP Server	ProFTPD, WU-FTPD.
Web Server	Apache®
Vulnerability Scanner	Nessus®
HoneyNets	Honeyd, Honeytrap, Kojoney
Authentication	OpenSSH, su
Applications	Asterisk, Cacti, Libsafe, Shadow Utils, Squid, Sudo
OS (security tools)	GrSecurity, PaX, SELinux
Miscellaneous	Unix® specific logs, Webmin, Windows® Server, Arbor, Linux® bonding, Microsoft® Cluster Service, NetApp® ONTAP®, NTSyslog, OpenHostAPD, Rishi, Suhosin

HoneyNet

HoneyNet is a decoy system set up to lure malicious users or activities to penetrate into the computer system. In the case of a low interaction HoneyNet environment, it does this by providing emulated services that attackers think are real services. For example, several common services like mail services, web services, and database services can be emulated purposely with vulnerabilities to make them a good target for computer system compromise. Once the emulated services have been compromised, the attackers will attempt to leave a backdoor by leaving behind a malicious software (malware) to allow them to revisit bypassing all security measures. Since the services are emulated, no real damage can be done to the system being attacked.

Organization implementing HoneyNets in their network system enjoys the following benefits but not limited due to other possibilities of its application:

- HoneyNets are cheaper to build
- HoneyNets are not expensive to deploy
- HoneyNets are easy to deploy
- HoneyNets require minimum maintenance
- HoneyNets are managed by IMPACT's staff, for example availability of HoneyNet services through our monitoring system
- Can be used for detecting bots
- A more targeted with no false positive since every attempt is classified as a suspect
- On-site HoneyNet data analysis is not required as IMPACT will perform the analysis
- Provide valuable information in the event of an infection within your organization
- Observe spread of virus or worms

10.1 Objectives

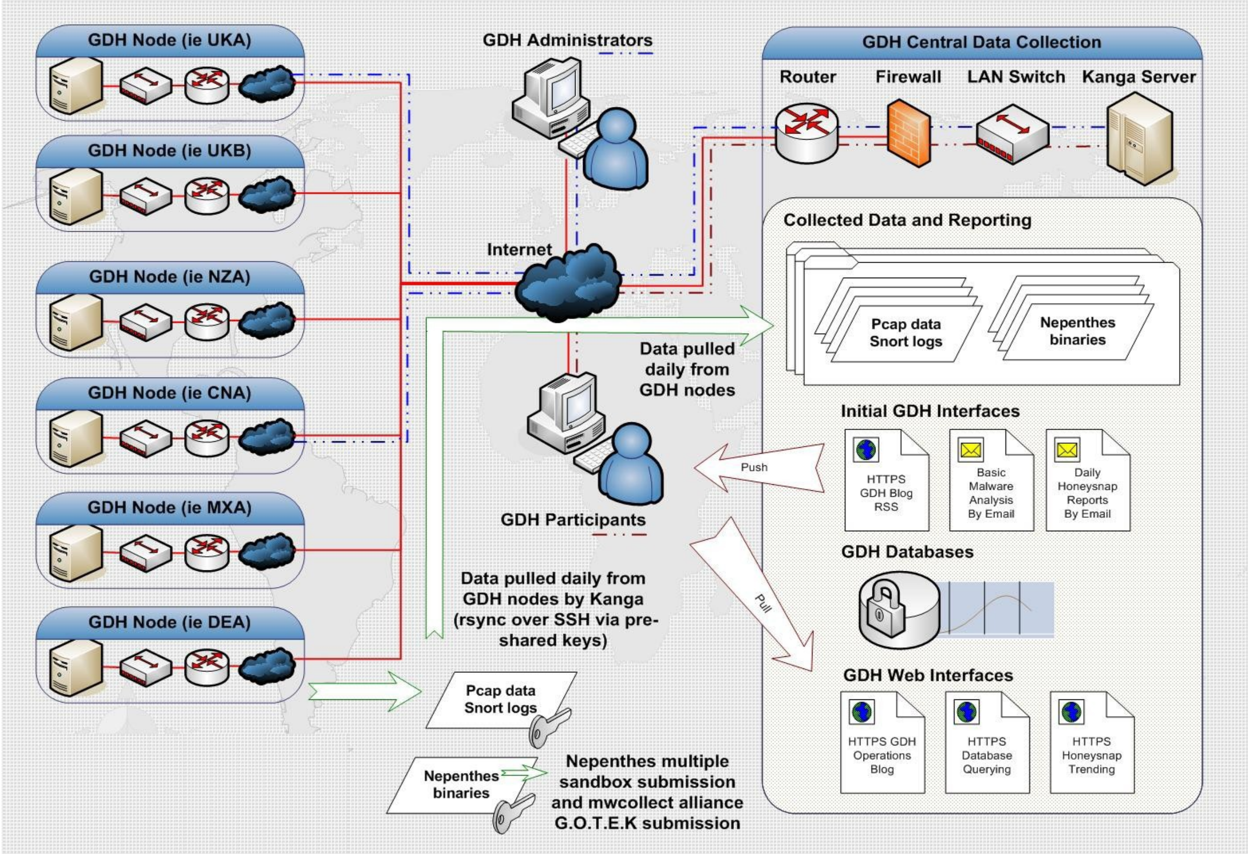
The features offered by the combined HoneyNet security device and IMPACT HoneyNet Infrastructure can provide the following information depending on how it is implemented:

- Capture network data and traffic
- Capture malicious software (malware)
- Ability to emulate a range of vulnerabilities selection
- Binary files comparison to detect similarities or uniqueness
- Analyzing of binary files behavior through sandboxing
- Classifying of malware through multiple anti-virus scanning
- Online overall reports on security threats and attacks, for example source of attack by IP address, country, binary files

10.2 Service Offerings

No single computer security system can provide full protection and overall picture of level of security threats that many organizations are really facing. HoneyNet, an addition to the computer line of security systems like anti-virus, firewalls, intrusion detection system, have proven to provide wealth of security threats information drawn from a deployment in a computer network environment. With managed HoneyNet services provided by IMPACT, an organization will be able to take advantage of security threats essentials such as regular security threats reports, early warning information, malicious software identification and classification, data and trends analysis of data captured from HoneyNet all over the world. Leveraging on HoneyNet infrastructure built by IMPACT, a cost-effective way of quickly deploying HoneyNet in any organization is possible to enhance an organizations network security perimeter. Plus, with wealth of information provided by IMPACT's key industry partners in computer security, data is further enriched to give the most up-to-date information on security news, advisories and resolutions every organization needs.

10.3 Operation Paradigm



10.4 Scope

The sensor build phase can be broken down into the following tasks:

- Build and customize base platform
- Build package installation
- Build of test harness
- Installation packaging
- Definition of deployment requirements
- Deployment documentation and media for remote installation

Once the hardware platform and operating system have been selected, we will develop a standard build that appropriately configures the sensor system for deployment. This will include:

- Hardening the system, to minimize the potential non-HoneyNet attack surface
- Installing pre-shared keys for remote management and data transfer

We will build standard packages for the required applications. These will be built and tested against the hardware and operating system choices made above. Packages will include:

- Nepenthes Low Interaction malware collector
- Net flow agent (e.g. nfdump/nfsen)
- Custom software for management, deployment, update and data collection

We will package both the operating system and standard packages in such a way that they can be deployed from USB based installation media.

We will carry out the following tasks in the project initiation phase:

- Definition of the sensor deployment workflow processes
- Assist in the preparation of legal documentation that will be used between IMPACT and recipient organizations (data sharing agreements, NDAs, etc.)
- Assist in the negotiation of purchase of the sensor node hardware
- Manage shipping and tracking of nodes to recipient organizations

Computer Incident Response Team (CIRT)

The internet continues to expand and there is a continuing movement towards distributed, n-tier and heterogeneous configurations. As the technology is distributed, it is often the case that the management of the technology is distributed as well.

This framework of a fully organized and operationalized CIRT model is beginning to be realized and shared by many national governments today in their national information security master plan or equivalent. IMPACT proposes to help establish for countries, its own National Computer Incident Response Team. The National CIRT shall:

- Have a phased implementation plan for setting up the CIRT.
- Be affiliated with other CIRTs and relevant authorities to better serve its constituencies.
- Be affiliated with IMPACT.

Collectively, with the integration of best practices and process, experienced people and proven technology, IMPACT believes that National CIRTs can play the role of maintaining round-the-clock vigilance to defend critical national infrastructure and assets against cyberattacks, and also serve as a critical cyber-nerve center in analyzing threat information; which can extend towards alerting private sector agencies pre-emptively in enhancing their security awareness, assist in remediation of identified vulnerabilities, and improving overall security posture in the country.

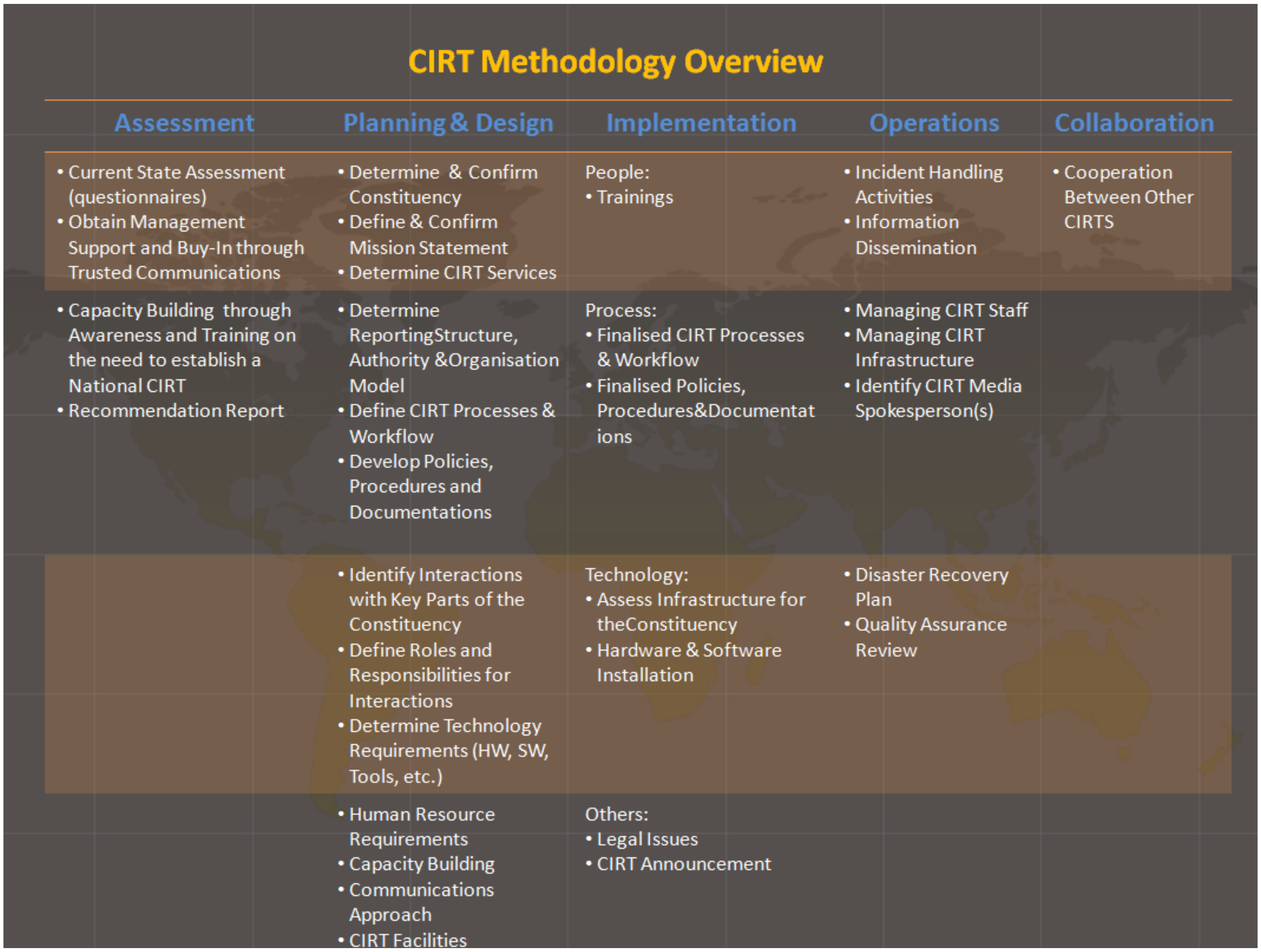
11.1 Objectives

The main objective of this project is to assist the governments in establishing and further developing Cybersecurity capabilities, such as Computer Incident Response Team with nation-wide responsibility (National CIRT). The overall vision is to facilitate the process towards a global Cybersecurity strategy for the country. Key objectives are:

- Facilitate the establishment of watch-warning and incident response capabilities to better identify, respond and manage Cyber threats
- Facilitate the country to identify its National Critical Information Infrastructure Sectors and layout a foundation to further elaborate and implement national cybersecurity strategies
- Build the cybersecurity capacity and transfer know-how in order to facilitate further developments on National CII Protection, such as establishing Sector CIRT's, National PKI, etc

11.2 Service Offerings

The service offerings offered by ITU-IMPACT can be represented by the below chart



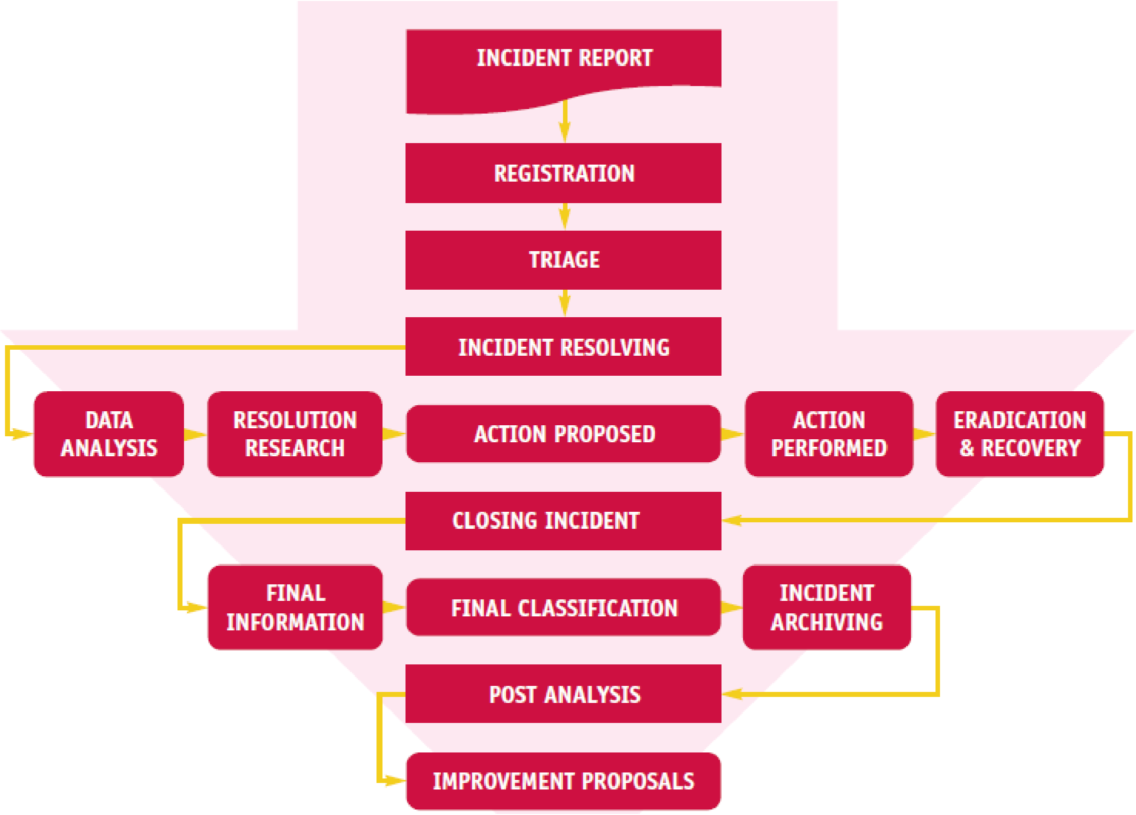
CIRT Methodology Overview

Assessment	Planning & Design	Implementation	Operations	Collaboration
• Current State Assessment (questionnaires) • Obtain Management Support and Buy-In through Trusted Communications	• Determine & Confirm Constituency • Define & Confirm Mission Statement • Determine CIRT Services	People: • Trainings	• Incident Handling Activities • Information Dissemination	• Cooperation Between Other CIRTS
• Capacity Building through Awareness and Training on the need to establish a National CIRT • Recommendation Report	• Determine ReportingStructure, Authority &Organisation Model • Define CIRT Processes & Workflow • Develop Policies, Procedures and Documentations	Process: • Finalised CIRT Processes & Workflow • Finalised Policies, Procedures&Documentations	• Managing CIRT Staff • Managing CIRT Infrastructure • Identify CIRT Media Spokesperson(s)	
	• Identify Interactions with Key Parts of the Constituency • Define Roles and Responsibilities for Interactions • Determine Technology Requirements (HW, SW, Tools, etc.)	Technology: • Assess Infrastructure for theConstituency • Hardware & Software Installation	• Disaster Recovery Plan • Quality Assurance Review	
	• Human Resource Requirements • Capacity Building • Communications Approach • CIRT Facilities	Others: • Legal Issues • CIRT Announcement		

In general the entire service offerings offered by ITU-IMPACT for CIRT deployment covers:

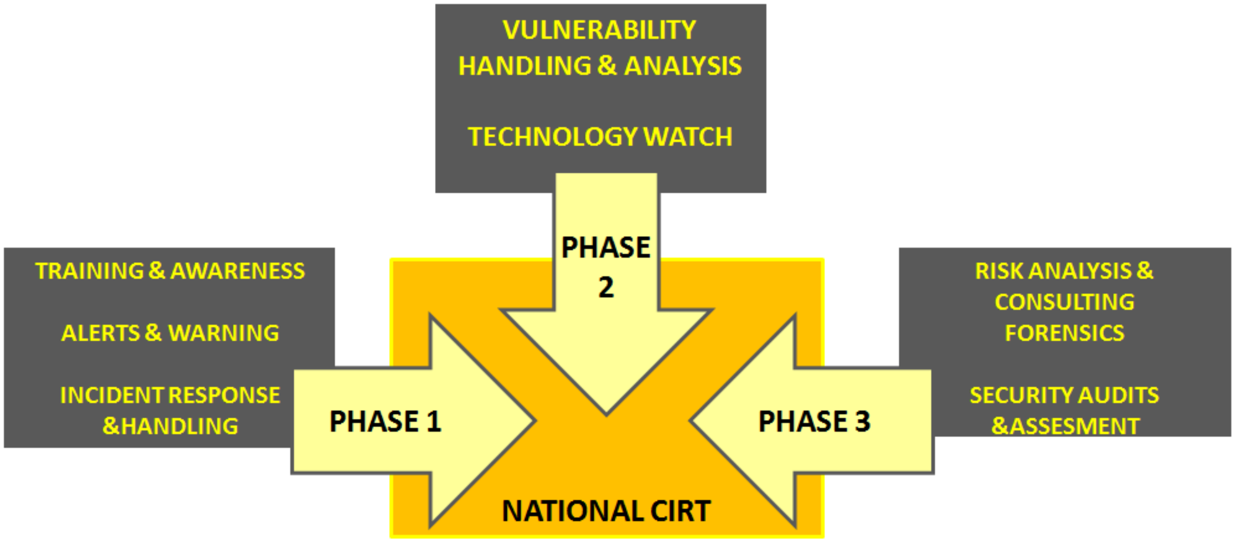
Assessment
Planning & Design
Implementation
Operations
Collaboration

11.3 Operation Paradigms



11.4 Scope

The scope of the project covers 3 phases for a total period of approximately 24 months as depicted in the below diagram.


VULNERABILITY HANDLING & ANALYSIS
TECHNOLOGY WATCH
PHASE 2
TRAINING & AWARENESS
ALERTS & WARNING
INCIDENT RESPONSE &HANDLING
PHASE 1
RISK ANALYSIS & CONSULTING
FORENSICS
SECURITY AUDITS &ASSESMENT
PHASE 3
NATIONAL CIRT

Human Capacity Building

ITU-IMPACT is committed to deliver high-quality, professional information security training to all its clients. A wide range of courses are available, divided into management and technical tracks in the ITU-IMPACT training calendar and will be conducted at client's site. Specific courses and courses with customized content related to information security can be arranged at any time.

ITU-IMPACT also conducts specialized workshops and seminars for its clients based on their needs to address specific areas in information security.

- Professional information security training with certifications where applicable
- Trainings are conducted by highly qualified and certified trainers
- Training is on- site and will avoids travel and other related costs
- Networking/Peering opportunities for client staff
- Course content can be tailored to meet specific requirements

ITU-IMPACT have established partnership with the top three (3) international certification body in information security; (ISC)^2, SANS & EC-Council. This has allowed ITU-IMPACT to negotiate a special discounted rate for ITU-IMPACT constituencies.

These certification courses are categorized into management and technical tracks and applicable for all levels of staff within the organization. The courses available are based on partner's current catalogue. Client can choose to have these courses conducted on-site provided the minimum number of participants are met or attend the public schedule classes as per partner's global training calendar.

ITU-IMPACT will interact with one training focal point for each of the client's organization who will receive course schedules, and making and managing reservations. Participant substitutions may be made at any time prior to the start of the class.

ITU-IMPACT courses are based on one fee for the course up to a maximum number of participants as stipulated in the table below. Once a course has been confirmed a deposit that has been agreed upon will be made by client. Cancellation of the course by client must be made 30 working days prior to commencement of course. Should the cancellation be made less than 30 days, full reimbursement for trainer flight and accommodation will be made by client to ITU-IMPACT. All correspondence related to training should be made to training@impact-alliance.org.

12.1 Service Offerings

ITU IMPACT offers the following training programs to its partner countries and organizations.

12.1.1 ITU-IMPACT SecurityCORE

Track: Foundation
Specialism: Information Security Foundation
Course Level: Foundation
Target Audience: IT Managers/Executives, IT Systems Administrators, Security Administrators, Access Control Administrators, Systems Analysts and Designers, Application Developers, Business Analysts and user representatives
Course Duration: 4 Days
Delivery Mode: Lectures with presentation slides and extensive hands on sessions

Course Overview

ITU-IMPACT SecurityCORE is a comprehensive course that prepares IT professionals and practitioners for the most up-to-date developments in cybersecurity. This course will cover the key concepts, definitions, principles and goals of information security considering both the management and technological aspects. Key topics include firewalls, intrusion detection and prevention systems, risk management models including ISO/IEC 27001, standards, security policies, tools and techniques used in cyber threats, security risks to networks, defending against attacks through the implementation of proper security mechanisms, encryption, authentication and authorization technologies.

Course Aims & Objectives

This course sets a core foundation of IT security knowledge for all attendees. It is suitable for any member of the IT community from the newest member of the team to the most experienced professional. Describing the core fundamentals of information security in an interesting, relevant manner, this course describes the close alignment of information security with ever-changing business requirements and enables the attendees to effectively understand information security concepts and build them into all business processes and design. In order to be a credible and authoritative program, this course is based on the ISO/IEC27002:2005, and other internationally recognized standards and practices.

Course Pre-Requisite/s

Having some basic knowledge and skills in Information Security will be an added advantage.

Module 1 - Introduction to Information and Information Security

- The relationship between Information and Business
- The Core Fundamentals of Information Security
- What is the role of information in today's economy?
- What is Information Security?
- What is Risk and how does it relate to Information Security?
-

Module 2 - The Core Fundamentals of Information Security

- Key Security Principles
- Introduction of 11 Major Security Areas of ISO 27002
- Security Policy
- Organizing Information Security
- Human Resources, Physical and Environmental Maintenance
- Information Security Incident Management
- Business Continuity Management

Module 3 - Designing and Implementing Security

- Designing Security Requirements
- Information Classification (case study/discussion)
- Building Security in to Systems and Business Processes
- Security Versus Productivity
- Detecting and Preventing Social Engineering
-

Module 4 - Assurance and Compliance

- Monitoring, Logs and Audit trails
- Incident Management
- Preventing Incidents
- Technical Countermeasures
- Effective use of tools (firewall, IDS, etc.)
- Scans and Penetration Tests
- Simple Security Solutions

12.1.2 BCM (Business Continuity Management) Principles and Practices

Track: Management

Specialism: Security Management

Course Level: Intermediate

Target Audience: Business Continuity Coordinators, Disaster Recovery Coordinators, Line Managers, Risk Managers, Operations Manager

Course Duration: 4 Days

Delivery Mode: This course will be presented as a lecture using PowerPoint slides. This lecture will be supplemented with group exercises and case studies for participants to better understand the concepts and principles taught in this course

Course Overview

BCM Principles and Practices is an introductory course in business continuity management suitable for all levels of participants. It is good for a novice in BCM as well as a refresher for practitioners. This course explains the building blocks of BCM and the best practices in designing, developing and implementing BCM in an organization. This course also discusses the BCM Project Planning activities in detail to assist organization prepare for a BCM project.

Course Aims & Objectives

This course will cover the basic principles and practices of BCM. The aim of this course is to provide a good foundation for participants in business continuity management and provide them a path for intermediate and advanced courses. Another objective of this course is to prepare the participants for implementing BCM in their respective organizations.

Course Pre-Requisite/s

Having some basic knowledge and skills in Information Security will be an added advantage.

Module 1 – Fundamentals and Concepts

- History of Business Continuity
- Explanation of Common Terminologies
- BCM Drivers
- Benefits of implementing BCM
- Recognized Standards / Guidelines in BCM
- BCM Players and their respective responsibilities
- Relationship of BCM with Risk Management, Information Security, Corporate Governance & Corporate Social Responsibilities

Module 2 – BCM Development Process – Planning & Control

- Identifying the needs for BCM in your organization
- Determining the Scope and Boundaries of the project
- Establishing the Project Organization Structure and Terms of Reference
- Preparing and executing a BCM request for proposal
- Project Planning and Scheduling
- Project Monitoring and Controls
- Documenting a Project Management Plan
-

Module 3 – BCM Development Process – Risk Assessment

- Understanding the purpose for conducting a Risk Assessment
- Exploring a Risk Assessment Methodology
- Reviewing some data gathering techniques
- Analyzing Risk to identify vulnerabilities
- Reviewing a sample risk assessment report
-

Module 4 – BCM Development Process – Business Impact Analysis

- Understanding the purpose for conducting a Business Impact Analysis
- Exploring a Business Impact Analysis Methodology
- Reviewing some data gathering techniques
- Analyzing impact and determining critical services
- Reviewing a sample business impact report
-
- Module 5 – BCM Development Process – Strategy
- Exploring some basic business continuity strategies
- Understanding the governance strategies relating to BCM
- Reviewing some operational strategies
- Exploring maintenance strategies to keep BCM up to date
-

Module 6 – BCM Implementation Process –Documentation

- Understanding the contents of a Crisis Management Plan
- Understanding the contents of an Emergency Response Plan
- Reviewing a sample Business Resumption Plan
- Reviewing a sample Disaster Recovery Plan
- Understanding the contents of a Damage Restoration Plan
-

Module 7 – BCM Implementation Process – Training

- Establishing a training needs matrix
- Reviewing skills / knowledge levels
- Preparing a training program

-
- Module 8 – BCM Implementation Process – Testing
- Understanding the purpose for testing
- Exploring the different testing techniques
- Understanding the need for a Testing Program
- Understanding the Testing Processes.
- Review a sample Test Plan
- Conducting a Post Test Review and Reporting on a BCM Test

12.1.3 Developing Security Policies

Track: Management

Course Level: Intermediate

Target Audience: Security Managers/Executives, Dept. Head/Managers, CISOs, CSOs, and anyone responsible for developing and managing security policies

Course Duration: 3 Days

Delivery Mode: This course will be presented as a lecture using PowerPoint slides. This lecture will be supplemented with group exercises and case studies for participants to better understand the concepts and principles taught in this course.

Course Overview

Business needs change, the environment changes, new risks are always on the horizon, and critical systems are continually exposed to new vulnerabilities. Policy development and assessment are a continual process. This is a hands-on intensive course on writing, implementing and assessing security policies.

Course Aims & Objectives

This is a hands-on intensive course on writing, implementing and assessing security policies. This course is suitable for professionals responsible for writing cybersecurity policies and procedures. This course is also suitable for IT professionals manage cybersecurity duties which include responsibility for creating and maintaining policy and procedures. It focuses on how to write basic security policies that are business or system specific. The student will have a hands-on practical assignment writing a policy template.

Course Pre-Requisite/s

Having some basic knowledge and skills in Information Security will be an added advantage.

Module 1: Concept of Security Policies

Defining Security Policies

Gaining Management Support

Defining Policies. Procedures and Guidelines

Organizing Information Security

Module 2: Security policy components

Content and Structure of Security Policy

Definition

Objectives

Scope

Define control objectives

Statement of management commitment

Module 3: Security Policy Structure

Development considerations of Security policy

Compliance with legal and contractual requirements.

Protection of company's assets.

The overall objectives of the policy

A management statement supporting the goals and objectives of policy.

Responsibilities defined within the policy.

Policy monitoring and enforcement

Policy review and timeline

Module 4: Developing Security Policies in line with International Standards

ISO/IEC27001 related policies

Creating organizational policy

Sample policy statements and documents

Modifying and updating sample policies

Module 5: Review of Key Policies

Information Classification Policy

Acceptable Use Policy

Email Policy

Information Security Policy

Network Security Policy

Password Policy

Physical Access Policy

Data Protection and Privacy Act

12.1.4 ISO/IEC 27001 (ISMS) Implementation

Track: Management

Specialism: Security Management

Course Level: Intermediate

Target Audience: Business Head/Managers/Executives, Dept. Head/Managers, CISOs, CSOs, IT Heads/Managers/Executive, Audit and Compliance Personnel and anyone responsible for implementing ISMS.

Course Duration: 4 Days

Delivery Mode: This course will be presented as a lecture using PowerPoint slides. This lecture will be supplemented with group exercises and case studies for participants to better understand the concepts and principles taught in this course.

Course Overview

Recent high-profile information security breaches and increased awareness of the value of information are highlighting the ever-increasing need for organizations to protect their information assets. ISO/IEC 27001 Information Security Management System (ISMS) is a risk management approach to maintaining the confidentiality, integrity and availability of the organization’s information

Course Aims & Objectives

This course is designed to teach participants the requirements of (i) ISO 27001 for ISMS establishment, implementation, operation, monitoring, review, maintenance and improvement. It also provides an insight into the emerging ISO 27000 series of standards. This course leads participants through a series of exercises following the requirements of ISO 27001 for ISMS implementation. Key implementation exercises are supplemented by case study examples of techniques using cost effective tools.

Course Pre-Requisite/s

This is not a technical IT security course; rather, it concerns information security management and is suitable for managers from a wide range of disciplines. Attendees should have a basic knowledge of business information system

Module 1 : ISMS Concept and Principles

Introduction to information security management systems\

ISO 27001 and ISO 27002 standards

Fundamental principles of information security

Business and compliance requirements

Types of laws, regulations and crimes

PDCA Model

Module 2: ISO 27001 Awareness

Scope

Normative References

Terms and Definitions

Information Security Management System

Management Responsibility

Internal ISMS Audits

Management Review of the ISMS

ISMS Improvement

Module 3: Defining Scope and Develop Security Policy

- Understand the requirement of the standard
- Define the scope of ISMS
- Identify Management's intent to implement ISMS
- Determine various roles and responsibilities
- Defining the scope
- Establish ISMS – Define Risk Assessment Approach
- Risk Assessment Concepts
- Understand Risk Analysis techniques
- Define Risk Assessment approach

Module 4: Identify, Analyze and Evaluate Risks

- Identification of Assets
- Classification of Assets
- Identify threats and vulnerabilities
- Estimate risk levels and impacts
- Establish a criteria for risk acceptance

Module 5: Identify and plan for Risk Treatment

- Develop Risk Treatment Plans
- Selecting appropriate Control Objectives and Controls
- Prepare Statement of Applicability

Module 6: ISMS Documentation

- Understand ISMS Documentation Requirements
- ISMS Mandatory Documents, Policy Framework, Procedures
- Developing a sample Policy)

Module 7: Implement and Operate ISMS

- ISMS implementation planning
- Security Awareness planning and implementation
- Security incident response

Module 8: Monitor and review ISMS

- Internal audit planning
- Internal audit policy
- Internal Audit program
- Management review

Module 9: Maintain and Improve ISMS

- Corrective Actions
- Preventive Actions
- Continual Improvement

Module 10: Certification Audit

- Accreditation Schemes
- Certification Body
- Certification process for ISO 27001

12.1.5 Malware Analysis and Reverse Engineering

Track: Technical

Specialism: Malware Analysis

Course Level: Intermediate

Target Audience: Incident Responders, Network and System Administrators, CIRT/CSIRT Personnel, IT Security, Malware Researchers, Malware Investigators and Anti-virus Analysts.

Course Duration: 5 Days

Delivery Mode: Lectures with presentation slides and extensive hands-on exercises

Course Overview

Cybercriminals are becoming more sophisticated and creative, distributing more aggressive forms of malware. Malwares are continuing to spread rapidly and compromising countless number of computers, causing serious problems in both user and corporate environments. While malwares come in varied forms and functionalities, IT Security, Systems and Network Practitioners need to acquire a deeper understanding and the required skill set to identify, analyze and mitigate malicious activities from a compromised system.

Course Aims & Objectives

The course will examine malware in both static and runtime environments and take into account the viewpoint of a CIRT, security team or incident responder, who are attempting to identify, analyze and mitigate malicious activities on a compromised system. The course also accounts for network defenders attempting to create signatures that will allow for identification of malware on other compromised systems. The course will cover static, runtime malware analysis techniques and the use of reverse engineering tools such as IDA Pro and Ollydbg.

Course Pre-Requisite/s

Have some basic knowledge and skills in Windows and Linux operating environments. Knowledge in VMware Workstation and Key programming concepts such as variables, loops and functions will be an advantage.

Module 1

- Introduction to Malware
- Malware and Incident Response
- Types of Malware
- Malware installation techniques and propagation
- Autostart techniques
- Determining Malicious installations
- Malware network traffic

Module 2

- Win32 Assembly review
- Win32 Assembly programming
- Disassembling Win32 programs
- PE file format

Module 3

- Tools (Ida, Ollydbg)
- Static Analysis
- Runtime analysis/debugging

Module 4

- Unpacking and/or unprotecting malwares
- Trojan/Backdoor
- Worm
- Viruses

Module 5

- In the wild, Malware

12.1.6 Network Investigation for Law Enforcement

Track: Technical

Course Level: Intermediate

Target Audience: Law Enforcement Officers & Support staff, Cyber Investigation & Forensics Staff

Course Duration: 5 Days

Delivery Mode: Lectures with presentation slides and extensive hands-on exercises

Course Overview

Cyber criminals today are targeting organizations with the intent of unlawfully gaining confidential and financial information to commit crimes. Traditionally, this was illegal but with the Internet platform this is now highly possible due to unsecured applications, systems and networks. When these cyber criminals fall in the hands of law enforcement, officers must be well versed in conducting investigation, analysis and reporting using tools and techniques. They should also understand the motive behind these attacks.

Course Aims & Objectives

The objective of the course is to give law enforcement officers a full set of tools and knowledge needed for performing effective cybercrime investigations and reporting. The course begins by reviewing the common types of cybercrimes, how criminal activities are conducted on the Internet, and the tools and motivations driving the Internet as a medium for criminal activity. The course will investigate how Internet crime is conducted using tools such as Botnets, DDoS attacks, illicit file hosting, underground economy marketplaces, spam, phishing, extortion, and more. The course will also demonstrate how common hacking activity takes place through web application exploits, remote operating system and application exploits, social engineering, and web drive by attacks.

Course Pre-Requisite/s

The core of the course will be focused on how law enforcement officers can conduct effective investigations using the Internet. The course does not assume prior knowledge of network investigations, and will cover basic topics from email tracing to advanced topics such as network wiretapping and investigation of suspects who masking their identity using multiple proxies.

Module 1

- Understanding the Landscape of Internet Crime such as Internet Fraud, Phishing, Botnet, E-Banking, Malware, Virus, Social Networking and Cloud Computing
- Understanding of Internet Technology Domain, Skype, Wireless, Proxies, VOIP
- Compliance and Law Enforcement Support Programmes
- Understanding of Registrants, DNS, Dynamic DNS, Autonomous System

Module 2

- Investigation of event log files such as Application, System and security logs
- Understand of differences in Firewall and types of logs for auditing and cybercrime investigation
- Understanding of TCP/IP controls, MAC Address, packet routing
- Basic online commands-netstat, nslookup, traceroute for reference to online investigations
- Understanding IIS web logs for understanding sequel injection and web-traverse attacks
- Basic Tracing mail header
- Using of network packet monitor such as Fiddler or Networkminer to investigate Phishing sites

Module 3

- Using Process Explorer and collection of PSTools, for analysing of network rouge processes and identifying communication links
- Understanding Windows 7 BitLocker and NTFS File System
- Understanding COFEE – Online Incident Response Tool
- USING QCAT/Qmail to conduct online enquiry of suspected activities

Module 4

- Systematic approach to Website Investigations
- Memory Analysis
- Windows Registry and System Restore points
- Timeline analysis in investigations
- Systematic approach to Live systems investigations

12.1.7 Securing Networks

Track: Technical

Specialism: Network Security

Course Level: Beginner - Intermediate

Target Audience: Network Administrators and Managers, System Administrators, Computer Emergency Response Team / Computer Security Incident Response Team personnel.

Course Duration: 4 Days

Delivery Mode: Lectures with presentation slides, case studies and extensive hands-on exercises

Course Overview

Network Security courses are designed to equip IT professionals and practitioners with the knowledge and skills required for implementing, designing, configuring, maintaining and reviewing a secure network system to prevent and manage network vulnerabilities. Participants will learn the skills needed to identify and analyze common internal and external security threats against a network so proactive security and audit strategies can be implemented to protect the organization's information assets and systems from weaknesses.

Course Aims & Objectives

This course will cover network security best practices developed over years to better manage and secure network systems. The course will be focused on methods of helping organizations to run cleaner and more cost-effective networks to provide better service. Topics such as secure router configuration, secure network routing design, secure DNS design and implementation, botnet discovery and mitigation, DDoS detection and mitigation, spam detection and anti-phishing techniques will be covered in depth.

Course Pre-Requisite/s

Good knowledge in Network Systems and Protocols is essential, and having basic knowledge and skills in Information Security will be an added advantage. Participants are required to bring their own laptop.

Module 1: Information Security Practices and Management

- Information Security Principles
- Security Planning & Security Management Practices
- Network Infrastructure and Vulnerabilities
- Risk Response and Recovery

Module 2: Security Architecture and Design

- Security Architecture and Design Framework
- Security Architecture Component
- Security Models
- Secure Network Routing Design

Module 3: Security Operation and Administration

- Data Classification
- Identity Management
- Configuration Management
- Change Management
- Service Level Management
- Security Policy Implementation and Best Practices

Module 4: Security Essentials and Attacks

- Essentials of Security Auditing, Security Controls, Testing and Monitoring
- Understanding the type of Attacks (DDOS, Spamming, Phishing, Botnets)
- Incident Detection Tools and Techniques
- Attack Prevention Tools and Techniques

12.1.8 Network Forensics and Investigations

Track: Technical

Specialism: Digital Forensics

Course Level: Intermediate

Target Audience: IT Security Practitioner, Forensic Analyst, Incident Handlers, Network Administrators, Law Enforcement Officers and Support Staff

Course Duration: 5 Days

Delivery Mode: Lectures with presentation slides and extensive hands-on exercises

Course Overview

The ability to preserve and analyze data found on digital storage media, computer systems and networks is essential for understanding and mitigating cyberattack against IT infrastructures. The ability to forensically analyze these devices and systems in a manner that preserves critical information is essential. The forensics professional must be highly competent in collecting, examining, analysing and reporting on digital evidence. The use of real-world scenarios would enable the target audience not only to learn the required skills, but also gain experience in their practical application.

Course Aims & Objectives

Participants will gain real world knowledge and skills to analyze network traffic, improve network security and reliability, and protect networks from malicious and criminal attacks. Participants will learn techniques to identify suspect traffic pattern, identify a breached host, identify signs of Bots running in a network and the techniques to deal with and manage compromised machines.

Course Pre-Requisite/s

The core of the course will be focused on how an information security practitioner can identify, analyze and report malicious activities over a network system. The course does not assume prior knowledge of network investigations, and will cover basic topics from basics of network forensics to advanced topics such malware analysis.

Module 1

- Driving factors behind modern malicious Internet activity
- Common attack vectors: from remote buffer overflow to Web 2.0
- Motivations of cyber attackers
- Botnets as a threat: A tool for Internet crime

Module 2

- Botnet creation methods, attack vectors, and trends
- Hands-on exercises focused on initial infection vectors, propagation, and Botnet functions.
- Botnet functionality: banking credential theft, spam, phishing, DDoS attacks, proxies, network sniffing, malware hosting, key logging, etc.
- Create and administer IRC and HTTP Botnets.

Module 3

- Introduction to Network Forensics
- Identifying and analyzing botnet activity: Finding Botnet C&Cs and compromised hosts
- Effectively identify compromised hosts, malicious internet activity, and Botnets using:
    - Intrusion Detection Systems
    - Network Flow Analysis
    - Host-based Monitoring
- Run and administer IDS, network flow, and host-based monitoring system

Module 4

- Network Forensics: Hands-on Exercises
- The future of Botnet technology: Advanced topics
- Network traces of common attack vectors
- Collecting malware using HoneyNets to find compromised hosts and Botnets
- Running server-side and client-side HoneyNets

Module 5

- Malware analysis to investigate malicious activity
- Introduction to dynamic and static malware analysis
- Performing dynamic and static malware analysis