Who we are

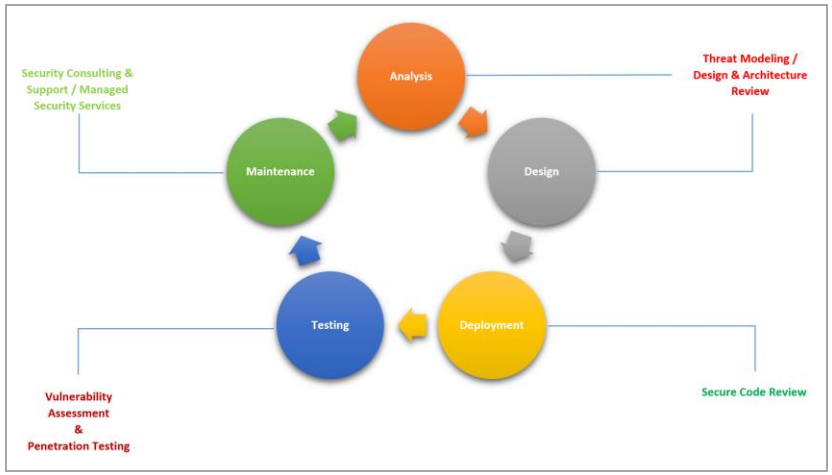
We are a team of dedicated security professionals, committed towards providing insight driven security solutions to our clients. We understand that every organization is unique, so are their security requirements. We provide customized security solutions to suit your business and infrastructure requirements so that security never become an overhead.

Contact Us

Email: sales@affluxconsulting.com
contact@affluxconsulting.com

Web: affluxconsulting.com

Information Security Service Offerings



AFFLUX CONSULTING

Insight driven security

AFFLUX CONSULTING
Insight Driven Security

Table of Contents

On-demand Security solutions

Leverage our specialized experience to improve your cyber security posture –

- ✓ Application Security
- ✓ Network Security
- ✓ Incident Response
- ✓ Cloud Security
- ✓ IoT Security
- ✓ Digital Profiling
- ✓ Social Engineering Attack Simulation

Our Services

Governance, Risk & Compliance

Our solutions are in-line with leading industry and regional security standards and compliance requirements –

- ✓ PCI DSS
- ✓ ISO 27001:2015
- ✓ HIPAA
- ✓ Data Privacy

Training & Awareness

We have detailed training programs to cater to all audiences, from the senior IT manager to in-depth trainings for developers –

- ✓ Technical Training for Developers & Security Analysts
- ✓ Information Security Management Training
- ✓ General Awareness Sessions for End Users

Security Research & Advisory

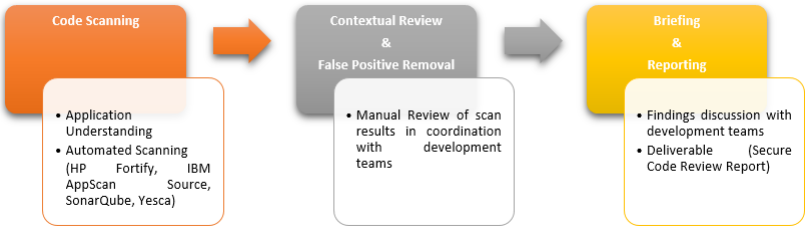
Our commitment towards continuous security research enable in offering insight driven security –

- ✓ Security Advisory
- ✓ Vulnerability Research
- ✓ Threat intelligence

Application Security

Secure Code Review

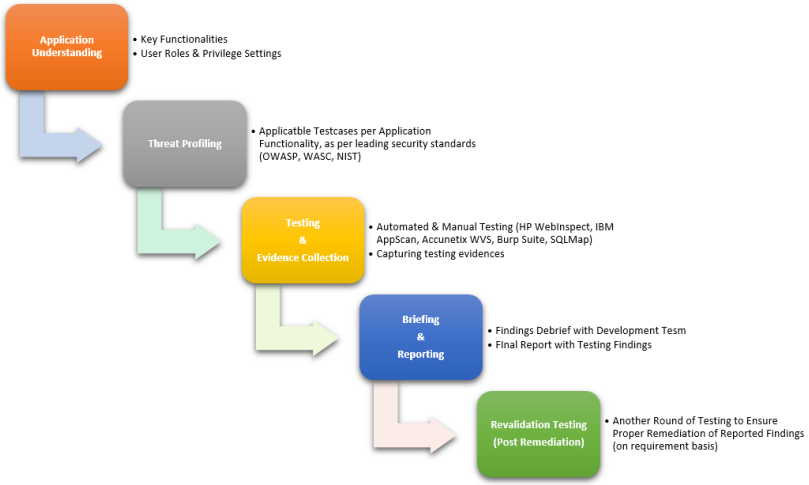
The following phases are involved in secure code review –



We perform secure code review for all programming languages including – C, C++, Objective C, Java, JSP, .Net, HTML, JavaScript, PHP, Python, Perl, COBOL

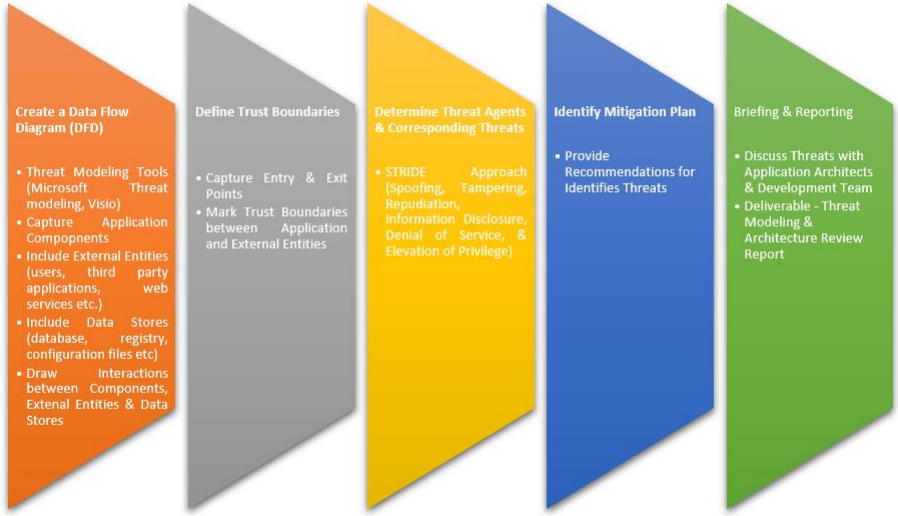
Application Penetration Testing

Our methodology for application security testing is –



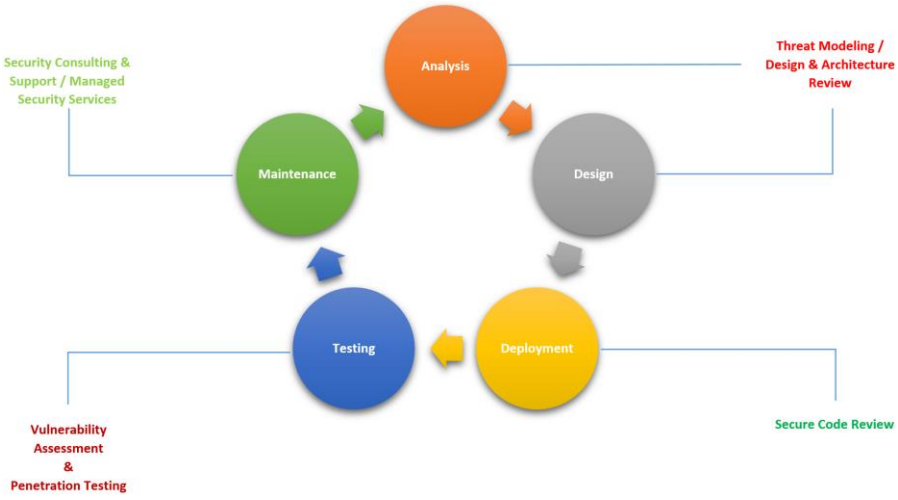
Threat Modeling & Architecture Review

An overview of our methodology –



Secure Software Enablement

Security infused in Software Development Life Cycle -



Third Party & Open Source Risk Assessment

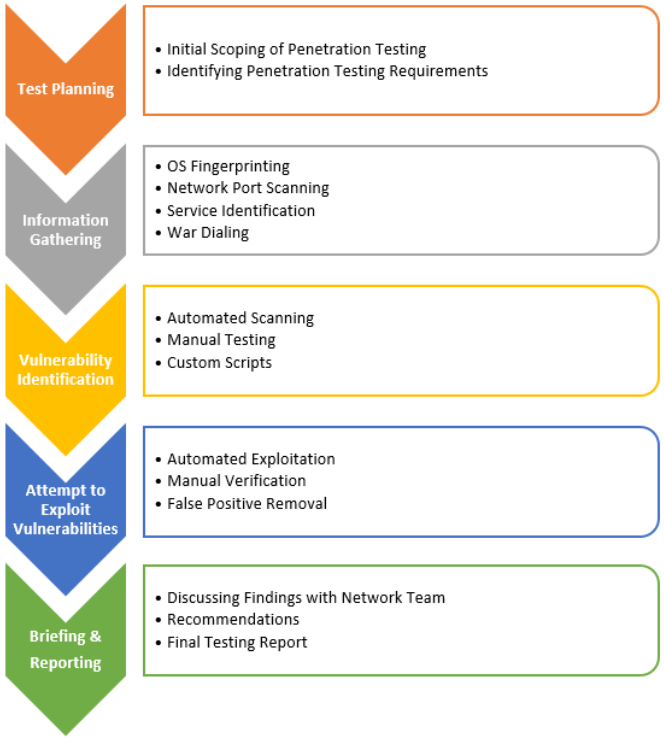
Third party and open source software components usage have exploded. Today, 90 percent of the typical enterprise application is comprised of open source or 3rd party building blocks, known as components. Recent research reveals that 71 percent of all applications contain components with known security flaws classified as severe or critical, and an alarming 76 percent of all organizations have no component management policies in place. Concerns over component vulnerabilities are now high on the priority list for standards bodies, such as the Open Web Application Security Project (OWASP), Payment Card Industry (PCI) and the Financial Services Information Sharing and Analysis (FS-ISAC) whose guidelines now mandate that open source and 3rd party components with known vulnerabilities must be avoided.

To gain deeper visibility to potential threats, we offer third party and open source component-level risk assessment.

Network Security

Network Penetration Testing

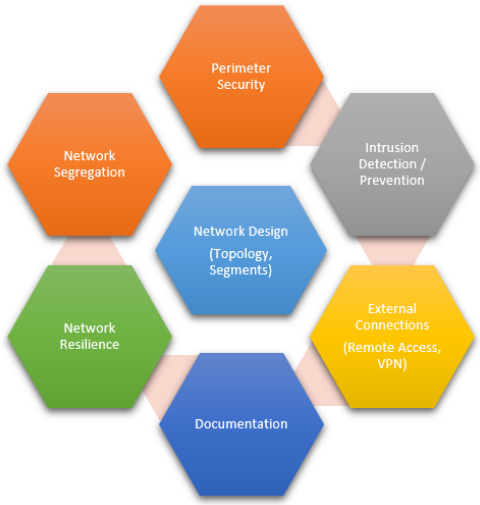
Our specialized network penetration testing approach –



We utilize automated scanning tools (Nessus, Nmap, Nikto), custom scripts and manual tests to ensure comprehensive network penetration test.

Network Security Architecture Review

The objective of network security architecture review is to determine if existing network architecture of an organization is fulfilling security requirements established by the organization. Network Security Architecture Review touches upon several aspects of network security and helps unveiling critical security threats to organization network security architecture.

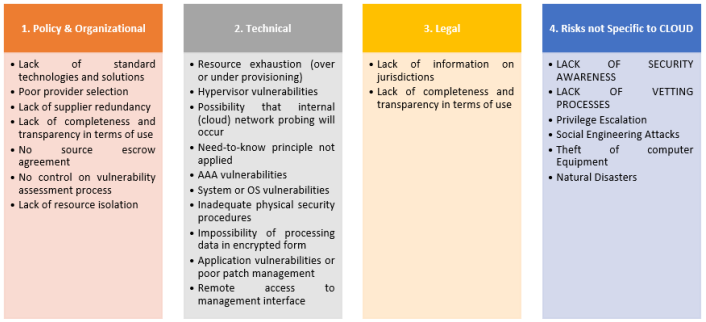


Configuration Auditing

Our approach to configuration audit ensures that IT assets including OS, database, network devices, network security devices etc. have necessary security settings enabled. We benchmark existing configurations against different security standards such as – CERT, CIS, PCI DSS, HIPAA, and OWASP etc. and identify gaps by leveraging automated tools (Nessus) and custom scripts.

Cloud Security

Our cloud security services consider risks from following categories –



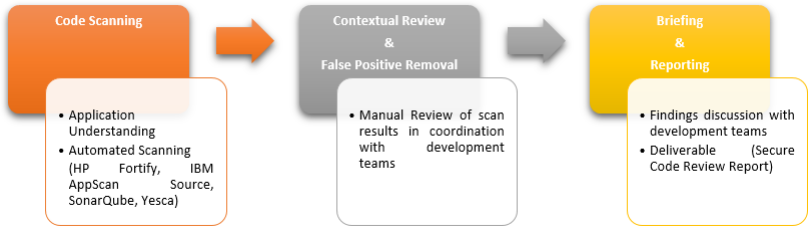
We offer a variety of cloud security services –

- ✓ ***Cloud Security Strategy and Risk Assessment*** – We help organizations assess security and risk tolerance, determine the right level of security for their cloud platform and design a comprehensive strategy and architecture to adhere to their security requirements.
- ✓ ***Application and infrastructure security*** – Our application and infrastructure security services help organizations design, develop and deploy secure cloud-based applications in a secured cloud infrastructure.

IoT Security

Secure Code Review

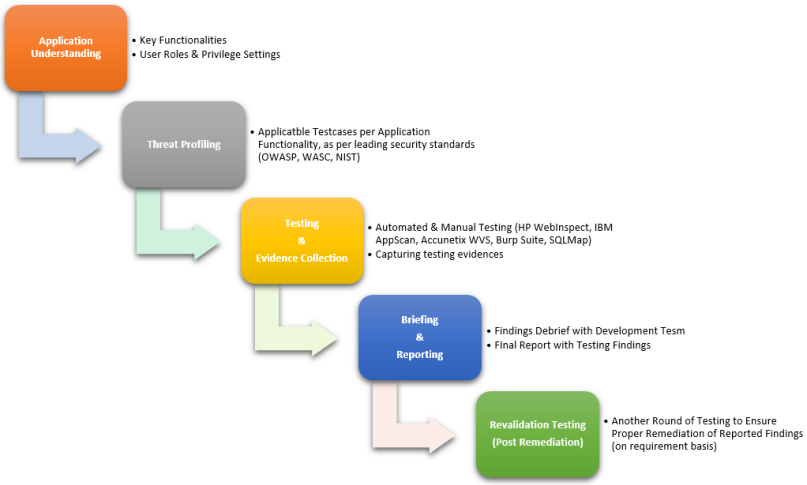
The following phases are involved in secure code review –



We perform secure code review for all programming languages including – C, C++, Objective C, Java, JSP, .Net, HTML, JavaScript, PHP, Python, Perl, COBOL

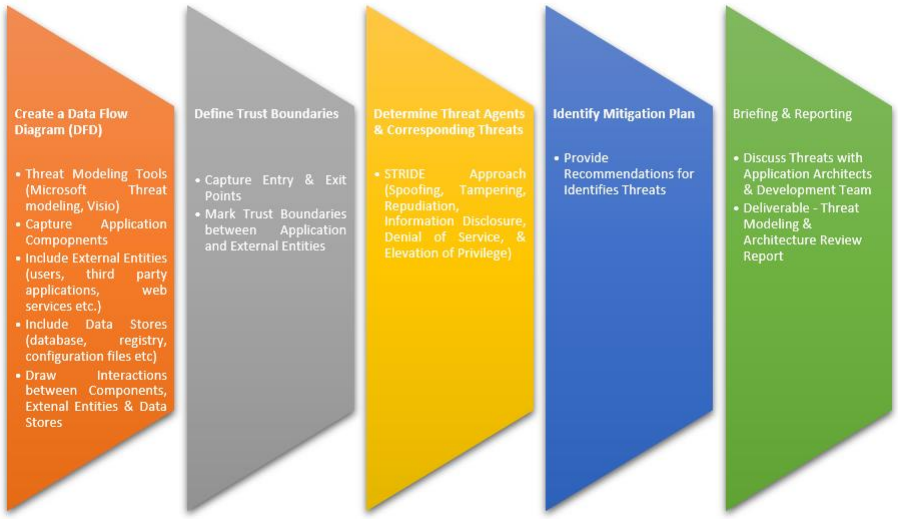
IoT Penetration Testing

Our methodology for application security testing is –



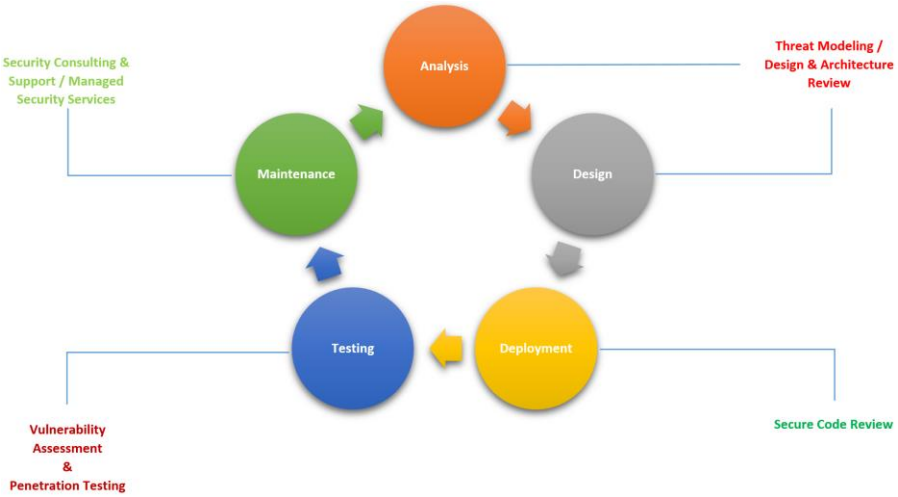
Threat Modeling & Architecture Review

An overview of our methodology –



Secure Software Enablement

Security infused in Software Development Life Cycle -



Third Party & Open Source Risk Assessment

Third party and open source software components usage has exploded. Today, 90 percent of the typical enterprise application is comprised of open source or 3rd party building blocks, known as components. Recent research reveals that 71 percent of all applications contain components with known security flaws classified as severe or critical, and an alarming 76 percent of all organizations have no component management policies in place. Concerns over component vulnerabilities are now high on the priority list for standards bodies, such as the Open Web Application Security Project (OWASP), Payment Card Industry (PCI) and the Financial Services Information Sharing and Analysis (FS-ISAC) whose guidelines now mandate that open source and 3rd party components with known vulnerabilities must be avoided.

To gain deeper visibility to potential threats, we offer third party and open source component-level risk assessment.

Hardware Testing

We review the physical security and internal components architecture of the device to determine the physical attack surface. Key areas of testing are –

- ✓ Firmware extraction
- ✓ Device Memory Extraction
- ✓ Authentication bypass by reconfiguring device
- ✓ Physical Access to Device Hardware Ports

IoT Protocol Testing

We test IoT protocols to assess communication security – ability to capture and modify data transmission, fuzzing of communication protocol etc. This includes interception and capturing of data to and from the device.

Firmware Analysis

We attempt to extract and examine the content of the firmware in order to discover backdoors, injection flaws, buffer overflows and other vulnerabilities. We will also assess the device firmware upgrade process for vulnerabilities and perform a secure boot review process.

Digital Profiling

Digital Footprint Identification

Social networking sites, job portals, search engines, internet registry and other public information platforms provide considerable information on organization – the digital footprint of organization. Digital footprint enables attackers to gather information and use in social engineering attacks such as – web spoofing, identity theft, phishing, whishing etc. against the organization. Most organizations don't have necessary policies and processes in place to prevent against such type of threats.

Our digital footprint identification services help organization in determining publically available information about organization, apply safeguards against posting of such information and removal of unwanted information. We utilized customized tools and scripts to automate identification with an extensive search database.

Social Engineering Attack Simulation

Social Engineering Risk Assessment

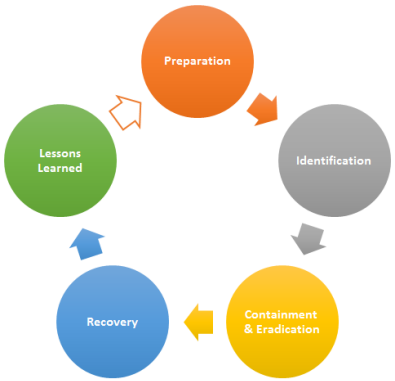
The human element is considered to be the weakest link in the security system. Even the strongest security system can be compromised by a single person acting in unauthorized manner. Social Engineering attacks utilize end user's lack of knowledge of proper security procedures.

The purpose of Social Engineering Risk Assessment is to determine how successful a social engineering attack would be, and the level of risk incurred by a social engineering attack to the organization. Based on information gathered during other phases of the assessment, we will craft and attempt one of the following social engineering attacks, customized to fit your organization environment –

- ✓ ***Impersonation Attack*** – The zero-knowledge attacker may use publicly available information to impersonate a trusted individual such as a new hire, vendor, IT support, trusted third party or fellow employee to obtain physical access to a designated facility.
- ✓ ***Spear Phishing*** – The attacker will craft a phishing email designed to for an employee to perform an action, usually clicking a website link or opening an email attachment that will cause a loss of some kind (usually credential exposure or remote control of the user's system).
- ✓ ***Media Drop*** – The attacker will prepare and distribute some type of disposable media (usually USB flash drive) in calculated locations and in a strategic manner to entice employees to view the contents of the media, triggering a notification or compromise of some kind.

Incident Response

Organization are surviving in world of attacks and eventually get hacked. The threat landscape is rapidly changing every moment. In today's era organizations can't stop being target of attacks but can prepare effective defense mechanisms to avoid the breach and in case of breach respond in a better way.



Incident response life-cycle

The question organizations should consider is "Are we aware of every anomaly in our digital space". Afflux Consulting can help you in becoming cyber Security Champion by improving response preparedness in both situations: i.e. Pre-incident and Post-incident. Our services help our clients to avoid being a next breach story.

Our Incident response services are intended for driving Incident Response and Digital Forensics program in various phases. Engage us:

- ✓ *If you are bootstrapping incident response program.*
- ✓ *If you observe any anomaly.*
- ✓ *Need help in investigating and recovering from breach.*
- ✓ *Designing defense strategies for what matters you the most.*
- ✓ *Enhancing the ability to prevent, detect and respond recent threats*
- ✓ *Executing tabletop exercises and incident response drills.*

Training & Awareness

Technical Training

Technical module of our training and awareness services is intended for development teams, application & network architects and security analysts. Key topics covered in this module are –

- ✓ Secure Development Practices
- ✓ Secure SDLC & DevSecOps
- ✓ Network Security Principles & Practices
- ✓ Security Testing Basics & Techniques

Information Security Management

Our Information Security Management training module focuses on management and leadership tier of the organization. We cover governance aspects of information security, through following key topics –

- ✓ Information Security Policy and Procedure
- ✓ Establishing and Running Information Security programs such as – secure application development, security testing, incident response, infrastructure security etc.
- ✓ Third Party / Vendor Security Policy and Procedure

We initially understand roles & responsibilities of target audiences and deliver a customized training program as per organization's security requirement.

General Awareness Sessions for End Users

We also conduct security awareness sessions for employees, students and general public to spread awareness about cyber-attacks and security measures against such attacks.