Methodology, Services and Team

Author:	PreCog Security Team office@precogsecurity.com
Version:	1.0
Date:	05/25/2021

Confidentiality information:

This document contains confidential information which is the property of:

PreCog Security, 501 1st Ave N, Suite 901 St. Petersburg, FL 33701

Information in this document is intended only for the owner or recipient and is confidential.

Unauthorized publication, duplication, possession or sharing of this document with third parties is strictly forbidden and will be prosecuted to the fullest extent of the law.

Table of Content

Introduction **4**

Implementation of Application Security and DevSecOps Practice **4**

Governance and Architecture 5

Application development 5

DevSecOps and Infrastructure 6

Secure design, architecture and threat modeling **6**

Security analysis and penetration testing **7**

Web application security training **10**

Secure integration / deployment **11**

Information security and operational security **11**

PreCog Security team **12**

PreCog Security address **13**

Introduction

Thank you for choosing PreCog Security as your trusted information security partner. Security is a complex problem, spanning from the organizational domain all the way to the technical domain and beyond. We mitigate that problem by helping you solve immediate issues you face and further on we help transform your organization so that in a short period of time, you will have the necessary expertise to run your security operation at the next level.

We analyzed your product from the client's point of view, and from the client side perspective we have found a possibility to integrate modern information security, application security and DevSecOps practices for your project. Our proposed collaboration will focus on the following areas:

Implementation of Agile Application Security and DevSecOps Practice

In order to integrate information security into every fiber of your project, PreCog Security team suggests an implementation of our roadmap which is an expanded variant of the OWASP Software Assurance Maturity Model with specific industry best practices regarding application security and DevSecOps. Our roadmap provides a high level guidance that is not organized by priority. In practice, we will always focus on implementing the biggest contribution and effect in the least amount of time.

In order to effectively integrate security in your project, security needs to become everyone's responsibility and not just the security department's responsibility. To do that, we suggest developing specific security focused individuals inside your project. This doesn't necessarily mean that FT employees will be assigned from development to security, but that we will develop their potential and skillset so they will also be more security focused in their day to day activities and will directly contribute to their specific, original field of work. This also means that ideal candidates are those who are interested to become more security focused in their craft, and not simply assigning arbitrarily that responsibility inside the organization. In order to achieve this, we are able to train your internal staff and in parallel operate as an external information application security support team and provide proof of concept implementations and expertise.

Integrating security is a complex system that requires a unique skillset, we suggest starting with three roles and three (or more if possible) candidates. The candidates can be recruited inside the current teams if specific members want to be more security focused, or we can recruit horizontally or vertically from inside the organization. The roles can be filled by employing additional team members with specific skills. This is not mandatory.

Common goal is internal expertise development, in the following specific roles that will cover the areas of:

- Governance and architecture
- Application development
- DevOps and infrastructure

Governance and Architecture

In order to design secure systems, information security needs to be a product design requirement and should be measured and tracked. In order to do that, we can support your processes and improvement of the application security process that will cover the following domains:

- Lead security design, architecture and requirements definition and reviews
- Managing the projects information security strategy
- Managing security policies and best practices
- Managing project compliance requirements
- Managing and defining design requirements
- Manage the security operations inside the project
- Defining and tracking specific security metrics
- Performing threat models and risk assessments for specific elements of the system
- Organizing training, education and guidance
- Collaborate in definition and design of secure architecture
- Collaborate in design reviews

Application development

Secure code is developed by developers who are security conscious and have the required skillset to write secure code. In order to achieve this, all developers need to be trained in secure development practices, we can support you with our expertise and skills in application security in order to cover the following domains:

- Implement specific application level mitigations
- Perform security focused code reviews and application security verification
- Define and verify application security requirements
- Collaborate in definition and design of secure architecture
- Collaborate in design reviews
- Triage specific application security vulnerabilities.

DevSecOps and Infrastructure

In order to improve the security of deployed code and automated infrastructure, integration of SAST (Static Application Security Testing) and DAST (Dynamic Application Security Testing) tools in the deployment pipeline prevents developers from shipping code that has vulnerabilities. Also, specific hardening and best practices need to be deployed from hardened templates and infrastructure provisioning methods. We can support you with our expertise in order to cover the following areas:

- Implement specific infrastructure mitigations
- Operate SAST / DAST tools inside CI/CD processes
- Deploy specific environmental and infrastructure hardening in code or templates
- Perform security reviews of the infrastructure
- Optimize DR/HA processes by deploying infrastructure as code
- Operate the security monitoring solutions inside the infrastructure
- Collaborate in definition and design of secure architecture
- Collaborate in design reviews

In addition to development of your internal practice, we can assist you as a trusted third party advisory that will perform the following services inside your organization, while we develop the same capability inside your organization:

Secure design, architecture and threat modeling

PreCog Team performs secure design, architecture and threat modeling from several perspectives: one is to analyze your internal processes and systems for vulnerabilities or potential issues with the goal of mitigating risk before it can become a problem and catching problems at the specification or design stage of the project. The second perspective is, we can design an architecture or define a specific set of controls a system needs to be secure by default, in this way, we help you design secure systems before they get developed. The third perspective is that our team serves as a third party advisory service, analysing third party solutions providing vulnerability mitigation and if they are developed according to current industry standards and best practices.

Security analysis and penetration testing

PreCog Team can analyze any part of the infrastructure, including application source code, for vulnerabilities or issues. This scope ranges from analytical reviews that are conducted against designs, specs or architecture documents, to applied low level code reviews that include penetration tests against infrastructure and code to red teaming engagements. Our goal is to perform security analysis on any required level.

PreCog Security's penetration testing approach is focused on optimizing the conducted tests and the time that is available to uncover security vulnerabilities in the web applications. Since it is not possible to run all possible tests, nor it is possible to test for vulnerabilities that are not known and/or available at the time of testing, nor it is possible in terms of time and practical considerations to test every component of the system for all possible input/output values and scenarios that could occur to test the entire attack surface, we tailor our testing to discover vulnerabilities that could have the most potential risk and impact, regarding a possible threat scenario, optimized for the ease of discovery by a third party. This enables us to discover vulnerabilities that have the biggest possible impact on the system, but are practical and realistic according to the threat model of the testing object.

Our penetration testing methodology relies upon following industry best practice standards:

OWASP Top 10 - The Open Web Application Security Project's Top 10 document outlines the most critical web application security flaws for a specific year the document was created. According to the latest OWASP Top 10 document: *"The OWASP Top 10 - 2017 is based primarily on 40+ data submissions from firms that specialize in application security and an industry survey that was completed by over 500 individuals. This data spans vulnerabilities gathered from hundreds of organizations and over 100,000 real-world applications and APIs. The Top 10 items are selected and prioritized according to this prevalence data, in combination with consensus estimates of exploitability, detectability, and impact".* The value in using this document as a reference on the possible prevalence, exploitability, impact and detectability of a particular class of vulnerabilities, helps us focus on finding the most prevalent and detectable vulnerabilities that could have the most significant security impact. Uncovering the classes of vulnerabilities that are defined by the OWASP Top 10 set is our highest priority. To read more about the OWASP Top 10 project, please refer to:

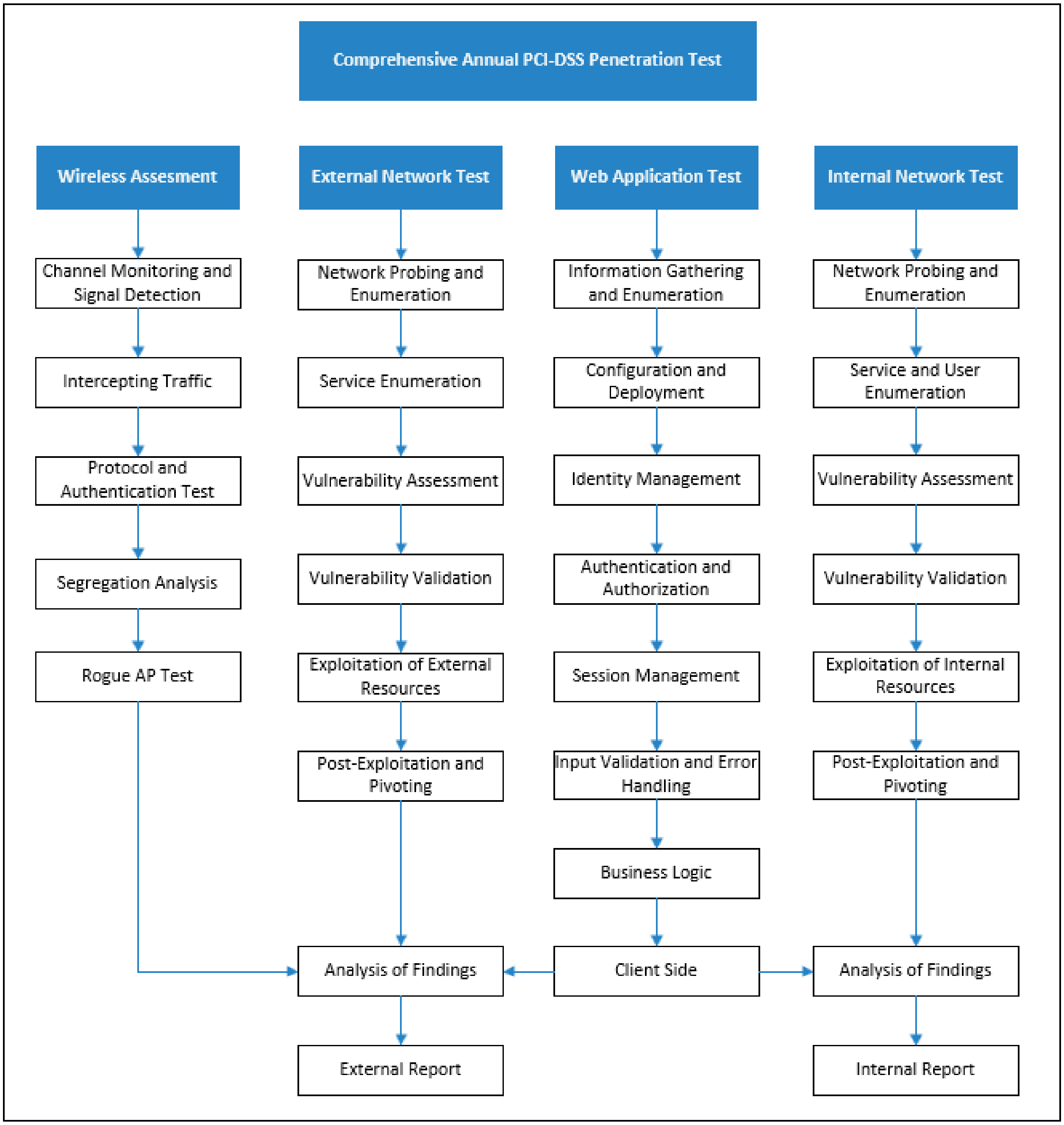
- https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

OWASP Testing Guide - The Open Web Application Security Project's Testing Guide document defines the industry best practice web application penetration testing methodology. The methodology is very detailed and outlines 91 tests in a total of 11 categories:

1. Information Gathering
2. Configuration and Deployment Management Testing
3. Identity Management Testing
4. Authentication Testing
5. Authorization Testing
6. Session Management Testing
7. Input Validation Testing
8. Error Handling
9. Cryptography
10. Business Logic Testing
11. Client Side Testing

Depending on the available time for the test, we optimize to run tests that would have the most significant impact and could be discovered easily by an attacker. To read more about the OWASP Testing guide and the application penetration testing methodology, please refer to:

- https://www.owasp.org/index.php/OWASP_Testing_Project


Comprehensive Annual PCI-DSS Penetration Test
Wireless Assesment
Channel Monitoring and Signal Detection
Intercepting Traffic
Protocol and Authentication Test
Segregation Analysis
Rogue AP Test
External Network Test
Network Probing and Enumeration
Service Enumeration
Vulnerability Assessment
Vulnerability Validation
Exploitation of External Resources
Post-Exploitation and Pivoting
Analysis of Findings
External Report
Web Application Test
Information Gathering and Enumeration
Configuration and Deployment
Identity Management
Authentication and Authorization
Session Management
Input Validation and Error Handling
Business Logic
Client Side
Internal Network Test
Network Probing and Enumeration
Service and User Enumeration
Vulnerability Assessment
Vulnerability Validation
Exploitation of Internal Resources
Post-Exploitation and Pivoting
Analysis of Findings
Internal Report

Web Application Security Training

PreCog Security, Inc. offers training for various internal teams in the practices of secure development according to OWASP best practices, training them in operational security, threat modelling and security architecture and devsecops practices. Our training is formed as a workshop that combines lectures, examples and hands on work for knowledge transfer that is customized according to your infrastructure and your specific use cases and compliance requirements. Our specialists cover specific issues and entire class of common AppSec vulnerabilities:

1. Injection
2. Broken Authentication
3. Sensitive Data Exposure
4. XML External Entities (XXE)
5. Broken Access Control
6. Security Misconfiguration
7. Cross-Site Scripting (XSS)
8. Insecure Deserialization
9. Using Components with Known Vulnerabilities
10. Insufficient Logging & Monitoring
11. Application Security Verification Standards
12. Threat modelling for FinTech applications
13. Secure design for FinTech centric applications

In addition to application security our team helps cover the domain of DevSecOps when applications are built in house and specific topics are demanded by the client and environment:

1. Connecting AppSec, DevOps and Security
2. Logging and audit logging infrastructure
3. Secrets management and integration in software
4. Error tracing for security
5. Hardening systems according to benchmarks and standards
6. Infrastructure as code and its use in disaster recovery
7. Integrating security into the CI/CD process
8. DAST testing in CI/CD
9. SAST testing in CI/CD

Secure integration / deployment

PreCog Security team helps integrate static and dynamic application security tests into organizational CI / CD processes to automatically detect security vulnerabilities in your commits.

This means every commit will be vulnerability scanned before being deployed. In addition, we can integrate dependency checking and software composition analysis tools so if a third party component has a security vulnerability such code won't get pushed to production and will get identified as vulnerable immediately. Also we help with secrets management and secrets decoupling which will prevent hardcoded passwords and access tokens from ending up in your code or scripts, which will prevent leakage or loss. This also includes:

1. Improving the CI process inside your project with:
    a. Integration of static code analysis solutions into the CI process
    b. Integration of and dynamic security analysis solution in the CI process
    c. Integration of dependency checking & tracking inside the CI process.
2. Development of hardened images / hardened configurations
3. Improvement of DR procedures with automated deployments.
4. Monitoring, Error tracking, Log analysis and tracking.
5. Specific security assurance and security review for your infrastructure

Information security and operational security

Your company is a software development company, PreCog's job is to highlight information security and operational security best practices. Our goal is to assist you run an information security management system (ISMS) according to ISO 27001 / ISO 27002 and align to other compliance requirements such as GLBA, FINRA, SOX and GDPR. This includes defining and writing procedures, best practices and help with implementing organizational and technical controls that are mandated by ISO 27002 or NIST 800 series. We provide the fully tailored service according to your threat model, risk profile and specific organizational issues.

Web application security and development of information security practices inside an organization is a continuous and never ending project. Pricing is developed as a plan where the client has access to PreCog Security's engineers and staff of advisors, testers, reviewers and implementers.

PreCog Security Team

Security Risk Lead: David O’Berry - Chief Security Innovation Officer
(david.oberry@precogsecurity.com)

Chief Security Innovation Officer and Co-Founder. David is a visionary, cyber scientist and security technology executive often quoted and referenced by local and global news agencies. David has unique experience as a strategic enterprise security architect with Fortune 100 companies such as Intel, McAfee and VMWare. Prior to executive experience, David spent 19+ years as a network manager and core architect in both the private and public sector. David earned the title of the youngest CIO and CISO in the state of South Carolina from 1997-2011 working for its Department of Probation, Parole and Pardon Services .
David holds CISSP-ISSAP, ISSMP, CSSLP, CRISC, and MCNE certifications, among numerous others.

Security Testing and Architecture Lead: doc.dr.sc. Tonimir Kisasondi
(tony.kisasondi@precogsecurity.com)

Tonimir Kisasondi is the lead security architect at PreCog Security. He finished his PhD at the University of Zagreb. From his industrial cooperation side, for the last 10 years he specialized in helping software, IoT and distributed systems companies from the EU and US build secure products from the design to the production stage. In his spare time, he’s involved with the OWASP project where he leads the Croatia chapter, contributes to various open source tools and organizes some of the largest information security gatherings in the region. His professional and research area of interest is security architecture, application security, security testing & analysis and applied cryptography.

Infrastructure security and DevSecOps lead: Igor Vuk
(igor.vuk@precogsecurity.com)

Igor Vuk is the lead infrastructure security specialist at PreCog Security. He has been working as a system administrator for 10+ years, his work includes most available and security critical deployments and systems in the EU. He holds several technical certifications in the area of system administration, such as Red Hat Certified Engineer and Red Hat Certified Specialist in Server Security and Hardening. As an infrastructure specialist, his personal interests are in the area of implementation of DevSecOps principles, with a strong focus on infrastructure security.

Penetration Tester: Zoran Jovic (zoran.jovic@precogsecurity.com)

Zoran is currently serving as a Consultant and penetration tester at PreCog Security. Zoran has led the development of security controls, network assessments/deployments, and penetration testing engagements with both small businesses and Fortune 10 organizations. Zoran specializes in conducting HIPAA and PCI-DSS mandated assessments. Zoran currently holds CompTIA Security+, Cisco CCNA and GIAC Penetration Tester (GPEN #14542) certifications.

Project Operational Lead: Alex Paunic - CEO
(alex.paunic@precogsecurity.com)

CEO and Co-Founder - 15 years of experience in cybersecurity channel and distribution management with MX Logic, Intel and McAfee. Alex managed a $100 million + dollar distribution channel with Florida based global distributor Tech Data and built enterprise security practice for national and SMB Value Added Resellers (VARs). During this time Alex worked with Fortune 100 executives to develop software, cloud and software-as -a-service platforms with sell through infrastructure. During this time he met and collaborated with David O'Berry while both working at McAfee and Intel.
Alex is an avid supporter of not for profit causes earning recognition from Boys and Girls Club of Pinellas County in Tampa Bay, FL for digital safety for children programs. He is also a member of the New Gen Tech mentorship program “Connect-IT 360” with Pinellas Education Foundation in Tampa Bay, FL.

Contact PreCog Security

PreCog Security, Inc.
E-mail: office@precogsecurity.com
Phone: 813-616-2868
Address: 501 1st Ave N, Suite 901
St. Petersburg, FL 33701