



PreCog Security, Inc - Company Services Overview

"The cost of removing an application security vulnerability during the design phase ranges from 30-60 times less than if removed during production" NIST, Gartner and IBM.

PreCog Security helps organizations in three major areas: security assessment (penetration testing), security by design (DevSecOps) and third party vendor :

1. Security Assessment (penetration testing): We analyze existing products, software, network and connected systems for vulnerabilities or potential issues with the goal of mitigating risk. Our goal is identifying and fixing security problems at the specification or design stage of the project.

Simple explanation: PreCog Team finds security gaps in your system, network or software and helps you fix them before you get hacked by cyber criminals.

2. Security by Design (DevSecOps): We design an architecture or define a specific set of DevSecOps controls within a system, product or software needs to be secure by default, in this way, we help you design secure systems before they get developed and enter production stage.

Simple explanation: PreCog Team helps you develop and build secure software early in the design phase which improves the quality and satisfies compliance needs.

3. Third party vendor testing (third party security risk mitigation): PreCog team serves a third party advisory service, analyzing suggested solutions from other parties (your suppliers, vendors, distributors etc...). We align with your internal legal, governance and security mandates to satisfy third party vendor vulnerability risk threshold.

Simple explanation: PreCog team helps you determine which third party products have high and low risk when used internally in your organization.

Areas of Expertise

1. Application security:

1. Architecture, Design, Implementing controls and creating secure applications from the design to implementation stage (Full stack - Frontend / Backend API) - Focus on Python, Java, Go etc.
2. Fully integrating an appsec practice in a company

2. Penetration testing:

1. Web Applications (Frontend / Backend API)
2. IoT devices and systems (including ICS/SCADA)
3. Network
4. Mobile applications

3. Security architecture and product security:

1. Analyzing specs/docs for potential security defects or what needs to be done to make a product / system more secure
2. Architecting and developing secure systems and networks
3. Architecting and developing secure products

4. Operational Security:

1. How to improve the security inside an organization
2. Full operational security guidance for the required threat Profile (ex. running a highly secure team, general business guidance, compliance)

5. Security Trainings:

1. AppSec
2. Operational Security
3. DevSecOps
4. Embedded / IoT Security
5. Email Phishing

6. DevSecOps:

1. Emphasis on SEC part, through DevOps / SysOps platforms that are security centric. Implementation of the following:
 - Jenkins and the Linux based CI/CD toolchain, from static analysis, dependency checking / dependency tracing, dynamic analysis
 - Creating an DevSecOps culture at an organization
 - Error tracking / Tracing - Jaeger / Sentry
 - Monitoring - ElasticCloud, Prometheus, Grafana
 - Kubernetes / Docker deployments and architecting whole kubernetes/docker clusters.
 - HashiCorp portfolio - Terraform, Vault etc.
 - Provisioning / Configuration management: Salt, Ansible and Puppet
 - Specific hardening for images, containers or systems.
2. For platforms: Amazon and Google Clouds, technology stack provided is Linux (Ubuntu, CentOS, Red Hat)

7. Compliance:

1. Emphasis on GDPR, ISO 27001, SOC2, HIPAA and PCI-DSS
2. Provide guidance and checklists for compliance needs (including strategy on protecting stored customer's data, data encryption, access control, develop secure systems and applications, test security systems and processes, develop and enforce security policies)

PreCog Security portfolio of partners and customers

- Software development companies
- Startups and corporations with in-house software and applications
- IoT product development company
- Fintech companies developing software
- Enterprise companies developing software

Process

Depending on the scope of the project, PreCog Security experts will define approach, methodology and pricing in coordination with the customer. Contact PreCog Security team for free consultation at office@precogsecurity.com

Pricing

1. Security Assessment with Vulnerability Scan (small to medium size business) - SAV

MSRP- \$1,900

The scope of work is a vulnerability scan and focused risk assessment against compliance needs. Timeframe: up to 2 days.

2. Security Assessment with Penetration Testing and Vulnerability Assessment (small to medium size business) - SAP

MSRP - \$4,900

The scope of work is a vulnerability scan and initial scope penetration test for the following testing, non-production systems containing test data. Timeframe: 2-5 days.

3. Security Assessment with Penetration Testing and Vulnerability Assessment (large and enterprise business) - SAE

MSRP - TBD

The scope of work and pricing will be determined after completion of Pre-Engagement Questionnaire and discovery call with the company and end user. Timeframe: 5+ days.

David O'Berry

***Security and Compliance Risk Lead
Chief Security Innovation Officer***
(david.oberry@precogsecurity.com)

Technology executive, strategic enterprise security architect with Fortune 100 companies: Intel, McAfee, VM Ware. Holds certs in CISSP-ISSAP, ISSMP, CSSLP, CRISC, MCNE.

doc.dr.sc.Tonimir Kišasondi

Security Testing and Architecture Lead
(toni.kisasondi@precogsecurity.com)

Tonimir Kišasondi 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 specializes 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.

Igor Vuk

Infrastructure security and DevSecOps Lead
(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 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.

Zoran Jovic

Security Assessment and Penetration Tester Business Development Director

(zoran.jovic@precogsecurity.com)

Zoran is a U.S. Army veteran, currently serving as a Cybersecurity Risk Consultant and Penetration Tester at Precog Security. Zoran performs security assessments, helping clients mitigate risk by drawing from his unique blend of technical know-how and understanding of business impact. With over 10 years of experience conducting risk assessments and consulting in the cybersecurity field, for both small businesses and Fortune 100 organizations. Zoran has led the development of security controls, network assessment, and penetration testing engagements, and managed multiple connected device and network solution deployments. Zoran currently holds CompTIA Security+ and GIAC Network Penetration Tester (GPEN) certifications.

Alex Paunic

Project Operational Lead: Alex Paunic - CEO

(alex.paunic@precogsecurity.com)

12+ years experience in cybersecurity channel and distribution management with MX Logic, Intel and McAfee. Alex worked with Fortune 100 executives to develop software, cloud and software-as-a-service platform and sell through infrastructure. At the same time Alex managed multimillion dollar distribution channel with national distributor Tech Data and assisted in creating enterprise security practice. Alex is an avid supporter for not for profit causes earning recognition from Boys and Girls Club of Pinellas County in Tampa Bay, FL for digital safety for children program.

“Make Security Simple and Affordable”

Contact Information

PreCog Security, Inc.
E-mail: office@precogsecurity.com
Phone: 813-616-2868

US office address: 501 1st Ave N, Suite 901
St. Petersburg, FL 33701