Ivan Obrien

Vice President, Penetration Testing and Security Assurance

(973) 555-1842 ivan.obrien@protonmail.com
linkedin.com/example/ivanobrien Morristown, NJ 07960

STRENGTHS

Risk-based testing
Focused manual testing on highest-consequence attack paths, giving leaders clearer risk decisions and stronger assessment value.

Executive communication
Turned sensitive findings into plain-language remediation choices; senior stakeholders gained confidence during difficult risk discussions.

Team coaching
Guided consultants through threat modeling, code review, and negotiations; peers frequently sought advice on complex assessments.

Assessment quality
Introduced evidence reviews and retest checkpoints, creating smoother delivery and more consistent assurance across regional teams.

Threat research
Tracked emerging vulnerabilities and exploit activity, then converted useful intelligence into practical testing procedures and advisories.

SKILLS

Penetration Testing | Code Reviews | Threat Modeling | Risk Management | Manual Exploitation | Security Assurance | Remediation Validation | Executive Reporting | Team Leadership | Web Security | Mobile Security | Cloud Security | Infrastructure Security

SUMMARY

Vice President-level **penetration testing** and security assurance leader with 15 years across banking, payments, and regulated technology environments. Leads web, mobile, API, **infrastructure**, cloud, network, and **secure code review** engagements from scope through executive reporting and remediation validation. Combines manual exploitation, threat modeling, automated assessment, source-code review, and control analysis to expose material risk without disrupting operations. Partners with developers, architects, infrastructure teams, risk leaders, auditors, global specialists, and external firms to turn sensitive findings into practical remediation decisions. Builds testing methodologies, service request workflows, reporting standards, peer review checkpoints, and retest programs that improve delivery quality. Coaches distributed consultants and advises senior stakeholders on emerging threats, exploit techniques, compensating controls, governance, and operational risk. Ready to help strengthen **security assurance services** through clear analysis, collaborative execution, and accountable risk reduction.

EXPERIENCE

Vice President, Penetration Testing and Security Assurance

Granite Harbor Bank March 2021 - Present New York, NY

Leads distributed security assurance teams across banking applications, mobile services, APIs, cloud workloads, infrastructure, and secure development pipelines. Owns assessment quality, executive communication, service workflows, coaching, hiring input, and remediation validation.

- Directed web, mobile, API, cloud, and infrastructure assessments across customer-facing banking services.
- Established risk-based scoping using criticality, **threat intelligence**, data sensitivity, and prior findings.
- Validated automated results through **manual exploitation** with **Burp Suite**, Nmap, Metasploit, and Nessus.
- Standardized evidence, **peer review**, quality checks, and retests through ServiceNow and Jira.
- Coached senior consultants on threat modeling, **source-code review**, **cloud attack-surface analysis**, and negotiations.

Senior Manager, Offensive Security

Redwood Payments Group July 2017 - February 2021 Jersey City, NJ

Managed offensive security delivery for payment platforms, merchant portals, mobile applications, APIs, and hybrid infrastructure. Guided playbook development, external testing coordination, stakeholder remediation, board reporting, and cloud security analysis.

- Managed testing for payment processing, merchant portals, mobile applications, APIs, and hybrid infrastructure.
- Built playbooks covering OAuth, SAML, **REST APIs**, containers, AWS identity, and **Azure configurations**.
- Combined OWASP methods, Burp Suite, Nessus, Nmap, **Metasploit**, and manual business-logic testing.
- Traced findings with engineering teams, defined **compensating controls**, and verified targeted fixes.
- Produced board-ready reports linking **vulnerabilities** with payment flows, customer impact, and **regulatory exposure**.

Penetration Testing Manager

Crescent Ridge Technology Services January 2014 - June 2017 Philadelphia, PA

Led concurrent assessments for financial, insurance, healthcare, and SaaS clients under defined statements of work. Directed planning, testing ethics, client communication, consultant mentoring, reporting, workflow migration, and remediation follow-up.

Vulnerability Management

Service Delivery

LANGUAGES

English — Native

French — Intermediate

MY CAREER

- Vice President, Penetration Testing and Security Assurance at Granite Harbor Bank (5.5 Years)
- Senior Manager, Offensive Security at Redwood Payments Group (3.6 Years)
- Penetration Testing Manager at Crescent Ridge Technology Services (3.4 Years)
- Senior Security Consultant at BluePeak Cyber Advisory (1.3 Years)
- Security Analyst at HarborPoint Security Labs (1.1 Years)

- Led concurrent assessments for banks, insurers, healthcare providers, and enterprise SaaS applications.
- Designed plans covering discovery, **threat modeling**, validation, exploitation boundaries, evidence, reporting, and **retesting**.
- Performed web, mobile, network, wireless, and infrastructure testing with **Kali Linux** and Wireshark.
- Reviewed source code and deployment settings for **authentication**, **authorization**, secrets, and input weaknesses.
- Migrated requests and findings into **ServiceNow**, improving assignment visibility and overdue-action escalation.

Senior Security Consultant

BluePeak Cyber Advisory | August 2012 - December 2013 | Baltimore, MD

Executed penetration tests and threat modeling engagements for regulated clients across public applications, corporate networks, remote access systems, and administrative services. Delivered evidence-based reporting, **remediation** guidance, research, and focused retesting.

- Executed tests for public applications, corporate networks, remote access, and administrative services.
- Validated scanner results through enumeration, **privilege escalation**, **session analysis**, and controlled exploitation.
- Developed threat models linking trust boundaries, sensitive data paths, and adversary techniques.
- Translated evidence into **reports** with severity rationale, reproduction steps, and mitigation guidance.
- Researched **emerging vulnerabilities** and **exploit techniques**, updating internal procedures and client advisories.

Security Analyst

HarborPoint Security Labs | June 2011 - July 2012 | Washington, DC

Supported supervised penetration tests and vulnerability assessments within approved testing windows. Prepared assessment materials, investigated exposed services, documented evidence, tracked threats, assisted reporting, and participated in remediation retests.

- Supported supervised tests for **web applications**, network services, and server environments.
- Prepared asset inventories, test accounts, **rules of engagement**, and **evidence repositories**.
- Used **Nmap**, **Nessus**, Burp Suite, Wireshark, and Kali Linux during approved assessments.
- Reproduced validated findings safely and documented evidence for senior consultants and clients.
- Tracked disclosed vulnerabilities, proof-of-concept activity, affected technologies, and available **defensive controls**.

PROJECTS

Global Security Assurance Service Modernization | 2024

Improved assessment consistency through standardized evidence, peer review, ServiceNow intake, Jira tracking, and remediation retests across distributed teams.

Cloud Attack Surface Assessment Program | 2022

Established repeatable testing for AWS and Azure workloads, linking identity controls, configuration risk, exploit paths, and executive remediation decisions.

LEADERSHIP & AWARDS

- North American Financial Services Security Leadership Award, 2024
- Enterprise Risk Partnership Recognition, 2022
- Security Assurance Innovation Award, 2020

EDUCATION

Bachelor's Degree in Information Technology

University of Maryland Global Campus | GPA: 3.5 | 2011 | Adelphi, MD

Coursework: *Cybersecurity, Network Security, Database Management, Systems Analysis*

CERTIFICATIONS

- Certified Information Systems Security Professional (CISSP) 2018
- Offensive Security Certified Professional (OSCP) 2016
- AWS Certified Security - Specialty 2022
- GIAC Web Application Penetration Tester (GWAPT) 2019

TECHNICAL SKILLS

- **Web Application Security:** Burp Suite, OWASP, REST APIs
- **Mobile Security:** Android, iOS, Mobile APIs
- **Network Assessment:** Nmap, Wireshark, Network Services
- **Exploitation Platforms:** Metasploit, Kali Linux, Python
- **Vulnerability Scanning:** Nessus, Authenticated Scans, Scanner Validation
- **Cloud Security:** AWS, Azure, Cloud Workloads
- **Identity Security:** OAuth, SAML, AWS IAM
- **Secure Development:** Source Code Review, Input Validation, Secrets Management
- **Governance Workflow:** ServiceNow, Jira, Request Management
- **Assessment Methods:** Threat Modeling, OWASP Testing, Risk-Based Testing
- **Reporting Practices:** Executive Reporting, Evidence Capture, Remediation Guidance

PROFESSIONAL AFFILIATIONS

- OWASP New Jersey Chapter, Volunteer Speaker and Workshop Mentor, 2018 - Present
- Financial Services Information Sharing and Analysis Center, Contributor, 2019 - Present
- Internal Offensive Security Coaching Circle, Program Lead, 2021 - Present

ADDITIONAL INFORMATION

Work Status : Authorized to work in United States. No sponsorship required.

REFERENCES

AVAILABLE ON REQUEST