Sanjiv Kawa

Experienced cyber security consultant specializing in threat intelligence led red teaming, enterprise network, application and cloud penetration testing, architecture review, risk management, defensive strategy, and remediation planning. Strong work ethic, well organized, attentive to detail, with exceptional leadership skills. Able to undertake simultaneous projects with enthusiasm and follow them through from initiation to closure.

Employment History

Apr 2021 - present

Senior Managing Security Consultant, Adversary Services, X-Force Red

IBM, New York, NY (Remote)

- Performed mid-to-long term adversarial simulation (red team) engagements against mature organizations in various industry verticals, such as, financial, retail, software, energy, and healthcare. Able to effectively emulate adversaries TTP's to reach target objectives.
- Led the presentation of findings to technical and executive audiences.
- Oversaw the success of various strategic initiatives, including developing a tiered sophistication service model and integrating the IBM acquisition of Randori Continuous Automated Red Teaming into the adversary services offerings.
- Identified and addressed capability gaps to mature the red team.
- Led and mentored junior and intermediate consultants. Involved in the recruitment process.

Feb 2018 - Apr 2021

Managing Principal Security Consultant and Head of US Penetration Testing

Nettitude, New York, NY

- Leadership responsibilities included overseeing key engagements, budgeting, recruitment, operations and utilization forecasting.
- Lead technical pre-sales specialist for key and strategic accounts. Strong ability to understand complex client requirements. Collaborated with leadership and account managers to build solutions for clients and create long term strategic relationships.
- Performed threat intelligence led red teaming (CBEST) for mature and capable organizations, such as, central banks, exchanges, insurance, and healthcare.
- Performed infrastructure and web application penetration testing for medium to large organizations. Conducted physical and remote social engineering campaigns.
- QA of global reports prior to delivery. Led client debrief presentations.

Jun 2015 - Feb 2018

Senior Penetration Tester

PSC (Acquired by NCC Group), San Francisco, CA (Remote)

- Conducted internal and external penetration tests for large organizations in various fields. A majority of these assessments were PCI oriented, where evaluating the security posture of the cardholder data environment (CDE) was the primary focus.
- iOS penetration testing, general ReST and SOAP API testing.
- Performed technical QA of reports prior to delivery.
- Performed technical interviews for candidates. Involved in the recruitment process.
- Developed offensive security tools to aid with penetration testing.

Jan 2013 - Feb 2015

System Administrator and Security Consultant

Graycon Group, Calgary, AB

- Primary duties involved conducting vulnerability assessments, penetration tests, security policy development and incident response for medium to large sized organizations.
- Provided remote server and client-side support for over 100 small to medium sized clients.

Jun 2012 - Dec 2012

Security Response Team Intern

Red Hat, Brisbane, QLD

- Developed a Java application that filters security-related issues in JBoss for engineers to address.

Oct 2010 - Oct 2012

Quality Assurance Engineer

Clarity, Calgary, AB

- Analyzed and tested ASP .NET web applications for security and functional issues.
- Other duties included database development, error testing, load and distribution testing, scripting, and reporting.

Academics

Bachelor of Information Technology, Security and Networking

Griffith University, Gold Coast, QLD, Australia

Diploma in Information Technology, Computer Systems

Southern Alberta Institute of Technology (SAIT), Calgary, AB, Canada

Personal Info

Email
sanjiv@popped.io

GitHub
www.github.com/skahwah

LinkedIn
www.linkedin.com/in/sanjivkawa

Website
www.popped.io

Skills

Skill	Rating
Critical Thinking and Problem Solving	●●●●●
Teamwork / Collaboration	●●●●●
Written and Verbal Communication	●●●●●
Risk Management	●●●●○
Project Management	●●●●○
Offensive Security Testing	●●●●○
Defensive Strategy	●●●●○
Tool Development (C#, Go, Python, Ruby, etc)	●●●●○
Exploit Development (C++, C, ASM, etc)	●●●○○

Certifications and Awards

CISSP

OSEP, OSCP and OSWP

CRTO and CRTO2

AWS Certified Security - Specialty

Sektor7 MDE

CVE-2018-10956

Part of the DerbyCon CTF team (spicyweasel) that finished first place in 2018 and second place in 2019.

Projects

SQLRecon
github.com/skahwah/sqlrecon

- A C# MS SQL toolkit designed for offensive reconnaissance and post-exploitation.
- Presented at Black Hat 2023, DEF CON 31, and Wild West Hackin' Fest 2022.

Wordsmith
github.com/skahwah/wordsmith

- Generate tailored geo-location based wordlists to improve password attacks.
- Presented at Wild West Hackin' Fest 2017, BSides D.C. 2017, and BSides LV 2016.