Alen Peric

SENIOR THREAT INTELLIGENCE ANALYST @CROWDSTRIKE

Profile

Cybersecurity graduate from Fanshawe College with over three years of industry experience, working as a Senior Threat Intelligence Analyst at Crowdstrike. Specialized in intelligence derived from deep and dark web monitoring, and conducting dark web analytics. Developed internal automation tools reducing alert response time by 20% and pioneered new techniques for identifying threat actors through typo-squatting. Huge homelab and network infrastructure enthusiast.

Employment History

Senior Threat Intelligence Analyst, Crowdstrike, Remote

JANUARY 2024 — PRESENT

Responsible for a portfolio of 17 Fortune 500 companies, including the strategic oversight, consultation and operational execution of cyber threat intelligence initiatives, focusing primarily on actioning alerts derived from deep and dark web (DDW) monitoring. Built several tools for internal use, that enabled the team to save up to 20% time when actioning alerts. Supplied innovative ideas and developed new concepts to identify threat actors trough typo-squatting campaigns. Responsibilities include cyber strategy consulting, analysis and interpretation of cyber events, enabling the identification, assessment, and mitigation of potential threats to client assets.

Senior Threat Intelligence Analyst, Royal Bank of Canada, Toronto - Canada

SEPTEMBER 2021 — JANUARY 2024

Executed in-depth threat landscape assessments and trend analyses to monitor potential threats and pinpoint emerging information security risks. Conducted rigorous intelligence application on active threats, deploying defensive countermeasures, and tracking advanced persistent threats (APTs). Sustained a cutting-edge understanding of evolving risks, adhering to industry best practices in risk management, threat analysis, and response techniques. Authored meticulous reports on threat intelligence analyses, effectively articulating findings to pertinent audiences. Fostered close collaboration with partners to enhance intelligence sharing among Canadian entities, delivering timely reports on recent vulnerabilities. Led the development of third-party breach policies and phishing kit analysis, alongside deep and dark web monitoring initiatives. Undertook thorough investigations of notable breaches and ransomware group activities, successfully retrieving data compromised by hackers. Conducted astute threat actor group analysis, further fortifying organizational cybersecurity posture.

Technical Expert, Apple Retail Inc., Vienna - Austria

JANUARY 2018 — MARCH 2021

Integral member of the inaugural team that established the first Apple Store in Vienna, Austria, marked as the 501st retail establishment of Apple globally. Following a year of dedicated service in Vienna, transitioned to London, Ontario, continuing my tenure with Apple at the Masonville retail outlet whilst pursuing collegiate studies in cyber security. Demonstrated adeptness in troubleshooting under demanding circumstances, proficiently restoring customer relations and ensuring device functionality.

Education

Details

163 Professor Day Dr
Bradford, L3Z3C2
Canada
+1 (548) 588-1420
alenperic@protonmail.com

Links

Homepage: alenperic.com

LinkedIn: linkedin.com/in/alen-peric

GitHub: github.com/alenperic

HackTheBox: hackthebox.com/profile/588878

Skills

Threat Intelligence

Project Management

Troubleshooting

OSINT

Data Analysis

Policy Development

Scripting

Penetration Testing

Network Architecture

Virtualization

Large Language Models

Cryptography

Languages

English

German

Slovenian

Croatian

Spanish

Cyber Security, Fanshawe College, London - Canada

JANUARY 2019 — JANUARY 2022

Upon completing the rigorous three-year Advanced Diploma in Cyber Security, I have acquired a robust foundation in the cardinal principles of Information Security (InfoSec), bolstered by a versatile skill set indispensable for excelling within the IT security sector. The curriculum encompassed an expansive spectrum of cybersecurity domains, encompassing information security, ethical considerations, network management/analysis, programming and scripting, operating system functionalities, and database management protocols. The program furnished profound training in risk analysis, cryptographic techniques, vulnerability assessment, access control architectures, and the meticulous execution of security audits. Armed with this exhaustive educational background, I am adept at deploying proactive security protocols to mitigate potential risks, and effectively address security infringements with a responsive tact.

Courses

OffSec Wireless Professional (OSWP), Offensive Security

DECEMBER 2023

Practical Network Penetration Tester (PNPT), TCM Security

JUNE 2022

eLearn Security Junior Penetration Tester, INE Security

JULY 2021

Extra-curricular activities

Team Lead - 3.4 Validating Threat Infrastructure, GeekWeek, Toronto

APRIL 2022

Leading a group project for a Threat Intelligence feed dashboard, created trough PowerBi. Ingested several feeds and running them trough a neural language processor, in order to assigns positivity/negativity score, which sub sequentially affects the threat ratings for a given industry sector. The dashboard featured built-in asset scanning for businesses to track their attack surface. The application provides feedback and security recommendations based on the asset scanning results. Finally, the application features a SYSMON component that detects any malicious events and notifies the user. The application is supported by a no-cost model aimed at small businesses who don't have a budget for expensive licensing, but wish to gain valuable insights into threat intelligence feeds and news.

Team Supervisor, CanHack 2022, Toronto

MARCH 2022

Supported high-school students and provided mentorship with penetration testing CTF exercises in an international competition. The Canadian team came in 3rd place worldwide.