RAFAEL GUEVARA HERNÁNDEZ

ABOUT ME

Specialist in intrusions, working in Purple Team activities. My main responsibilities include malware analysis, threat monitoring in incident response, and threat simulation through pentesting activities. I am passionate about continuous learning and exploring diverse topics in cybersecurity. I stand out for my organization and curiosity, which allow me to approach each project with meticulousness and an innovative approach.

EXPERIENCE

Scitum, S.A. de C.V.

- **Junior Monitoring Engineer (January - March 2023)**
  - Monitoring firewall security services (Checkpoint, Fortinet, Panorama).
  - Reporting of suspicious activities.
  - Analyzing user behavior to detect suspicious activities and prevent potential security breaches.
  - Analyzing suspicious artifacts through packet inspection (Wireshark, tcpdump).

- **Cybersecurity Intrusion Specialist** (April 2023 - March 2024)
  - Continuous monitoring of endpoints, SIEM, and Firewalls using advanced platforms (Palo Alto Cortex XDR, Trend Micro Deep Security Manager, Trend Micro Apex One, Trend Micro DDI, Splunk, Radware).
  - Use of Threat Intelligence platforms to obtain updated threat information and adjust defense strategies accordingly.
  - Developing scripts in Python, Powershell, and Bash to automate tasks and improve security operations efficiency.

- Sr Cyber**security Analytics Engineer (April 2024 - Present)**
  - Managing security incidents from initial detection to resolution, ensuring effective and timely response.
  - Continuous monitoring during incident response, using advanced platforms to identify and mitigate threats in real-time.
  - Performing static and dynamic malware analysis to understand its functionality and develop effective countermeasures.
  - Using advanced threat detection tools such as Palo Alto Cortex XDR, Trend Micro Deep Security Manager, Trend Micro Apex One, and Crowdstrike Falcon to protect company assets.
  - Threat simulation through pentesting techniques and using malware samples to identify and remediate potential vulnerabilities.
  - Vulnerability assessment and testing to identify weaknesses and vulnerabilities in the security infrastructure

SKILLS

Tools and Programming Languages

- XDR: Cortex Palo Alto Networks, Crowdstrike Falcon, Trend Micro Vision One
- SIEM: Splunk, FortiSIEM
- Cloud WAF: Radware
- Firewall: Panorama Palo Alto Networks, Fortinet, Checkpoint
- Python, Powershell, Bash

Languages

- Spanish (Native)
- English (IELTS certification: 7 out of 9)
- Italian (Basic)

Malware Analysis

- Hypervisors: Virtual Box, Vmware
- Operating Systems: FlareVM, REMnux
- Yara Rules
- Microsoft Sysinternals
- Debuggers: X64dbg, IDA (Basic)

Cybersecurity Frameworks

- OWASP
- Cyberkill Chain
- MITRE-ATT&CK

EDUCATION

Instituto Tecnológico Autónomo de México

B.Sc. in Applied Mathematics (2018-2023)

London School of Economics

International Political Economics Summer course

CERTIFICATIONS

Palo Alto Networks Micro-Credentials

- Cortex XDR Support Engineer (PMXdS)
  - Credential ID: 253565242
- Cortex XDR Consultant (PMXdC)
  - Credential ID: 253372301

Fortinet Training Institute

- Fortinet NSE Level 1 (Valid: January 2023 - January 2025)
- Fortinet NSE Level 2 (Valid: January 2023 - January 2025)
- Fortinet NSE Level 3 (Valid: January 2023 - January 2025)

EC-Council

- CEH (Currently pursuing)

Tryhackme - Cybersecurity training platform

- TryHackMe SOC Level 1
  - Credential ID: THM-EYPGESBQ7I
- TryHackMe SOC Level 2
  - Credential ID: THM-QAU2CG4CKG
- TryHackMe Red Teaming
  - Credential ID: THM-IWKXYTWARL
- TryHackMe Offensive Pentesting
  - Credential ID: THM-KAJRMKH1Z8
- TryHackMe Jr.Pentester
  - Credential ID:THM-BHXHQSSDNL
- TryHackMe CompTIA Pentest+ learning path
  - Credential ID: THM-MLNR5FYKJ6+
- TryHackme Web Fundamentals
  - Credential ID:THM-NILKNEOS2S
- TryHackMe Cyber Defense
  - Credential ID:THM-QZBASOUXTQ
- TryHackme Security Engineer
  - Credential ID:THM-6WDLKFE90Z

OTHER PROJECTS

Rankings on Tryhackme Cybersecurity Platform

https://tryhackme.com/leaderboards
User: alephNaN

- Global Rank reached: #122 (Top 1%)
- Rango in Mexico: #1

CONTACT INFO

Cellphone: (+52) 442 2876755

mail: rafagh00@hotmail.com

LinkedIn: https://www.linkedin.com/in/rafael-g-17236b221