Kutay KOCA

Cyber Security Analyst

My Contact

info@kutaykoca.com

www.kutaykoca.com

Istanbul, Turkey

linkedin.com/in/kutaykoca

Summary

CompTIA Security+ certified, highly motivated Cyber Security Analyst with 3 years of experience in IT, with 1 year dedicated to Cyber Security. Background in hands-on projects involving monitoring and analysis of potential and active threats using SIEM solutions and EDR tools such as Splunk, IBM QRadar and CrowdSrike. Specialized in Network Analysis using Wireshark and Ticketing and Reporting via TheHive. As a fast learner and versatile team member, looking forward to opportunities to apply my transferable skills in the field of Cyber Security.

Soft Skill

- Analytical Thinking
- Problem-Solving
- Well-motivated and Quick Learner
- Time Management
- Adaptability
- Stress Management
- Collaboration & Teamwork
- Creativity
- Curiosity

Education

- Bandırma Onyedi Eylul University
  Bachelor's Degree, Computer Engineering
  2019-2023
- Sinop Science High School
  2014-2018

Technical Skill

SIEM & EDR: Splunk Enterprise Security, IBM QRadar, Crowdstrike, Logsign, Graylog
TICKETING: TheHive
KALI LINUX TOOLS: Burp Suite, Metasploit, Nmap
VULNERABILITY ANALYSIS: Nessus, Qualys, OpenVAS
VIRTUALIZATION: VMware, VirtualBox, UTM
FIREWALL: FortiGate, Eve-NG
NETWORKING: Wireshark, TCP/IP & OSI Layers, LAN, DNS, TCP/UDP protocols, VPN, Whois, URLVoid, MX Toolbox, Phishing Analysis, Authentication
OSINT: OSINT Framework, Google Dork, Exploit-dB, TheHarvester, Shodan.io, Hybrid Analysis, VirusTotal, Any.Run
SECURITY FRAMEWORKS/STANDARDS: NIST-800, OWASP 10, Cyber Kill Chain, MITRE ATT&CK, Framework, Information Security Playbook
SOC EXPERIENCE: Log Analysis, Detection Packet Analysis, Malware Analysis, Online Sandbox (FlareVM)
PROGRAMMING LANGUAGE: Python, Java, C, C++, C#, JavaScript, SQL

Professional Experience

Clarusway IT School, Virginia/USA

May 2023 – Oct 2023

Cyber Security Analyst Trainee

- Utilized **Splunk**'s query language (SPL) and designed custom **IBM QRadar** rules and dashboards for advanced searches, complex data models, real-time visibility, and improved security posture.
- Effectively used the **Crowdstrike** platform and **TheHive** for detecting, responding to potential security threats, managing incidents, and ensuring timely communication and resolution.
- Conducted in-depth packet-level analysis and network security assessments using **Wireshark**, **NMAP**, and **Nessus** to identify malicious activities, open ports, unauthorized access, and vulnerabilities.
- Applied **Metasploit** and **Burp Suite** frameworks to simulate and assess security risks, conduct penetration tests, evaluate network robustness, identify web vulnerabilities, and propose remedies.

Onat Digital , Samsun/Turkey

Aug 2021 - Apr 2024

Software Developer

- Utilized a wide range of tools including WordPress, HTML, CSS, and JavaScript to create engaging and visually appealing websites.
- Proved the SEO of websites using Google tools such as Google Analytics, Google Tag Manager and Google Ads
- Applied security tests and patches to detect and fix vulnerabilities.
- Employed responsive design techniques to develop mobile compatible websites.
- Created backend services with Node.js

CyberForce Security Operations Center , Istanbul/Turkey

Apr 2024 - Present

Cyber Security Analyst (L1)

- Monitored and analyzed security events using SIEM tools to detect potential threats and anomalies, ensuring timely identification and response.
- Engaged in incident response and management by performing initial triage and escalation, following predefined protocols to minimize impact and expedite resolution.
- Applied threat intelligence data to recognize and mitigate potential threats, enhancing overall security posture.
- Analyzed network traffic and identified unauthorized activities or vulnerabilities using tools such as Wireshark and Nmap.
- Collaborated with cross-functional teams to report and resolve security issues, ensuring comprehensive documentation of incidents and actions taken.

Certification

- CompTIA Security+ , *2023*
- Ethical Hacker, Cisco , *2024*
- Cyber Threat Management, Cisco , *2024*
- Clarusway IT School, Cybersecurity Certificate , *2023*
- Becoming an Ethical Hacker Course by Udemy , *2023*

Languages

- Turkish : Native
- English : Advanced
- German : Beginner