KB

Kyle Barbre

Kylebarbre7@gmail.com

508-641-0938

Oxnard, CA 93036

Professional Summary

Dedicated cybersecurity professional with a relentless drive for self-improvement and a passion for lifelong learning. Known for my commitment to mastering new technologies and methodologies, I thrive on challenges that push me to expand my knowledge and skills. With a proven track record of saving my company time and money. I am eager to leverage my expertise to better the company.

Work History

Techurion - System Administrator

03/2024 - Current

- Established and managed the entire tech stack at Techurion, including Azure Active Directory and Jira ticketing systems, leveraging expertise in automation and scripting languages such as JSON, Python, and Bash.
- Implemented Tines automations to streamline workflows, integrate systems, and enhance communication across the organization, driving efficiency and productivity.
- Led security operations as part of Techurion's Managed Security Service Provider (MSSP) offerings, conducting virus scans using tools like VirusTotal, performing network analyses, and conducting host analyses to fortify our security infrastructure.

Edx - Teaching Assistant

01/2023 - Current

- Aided in teaching 6 month long Bootcamp to cohorts of 50+ students supporting a wide range of technologies from cloud computing in Azure to VM management from vagrant.
- Course covers teaching bash, linux administration, windows administration, powershell, offensive security Metasploit, vulnerability scanning nesses, Pentesting and reporting with the DVMA and custom weak Webserver.
- Main challenges is student interaction and getting them to understand where they are going wrong without giving them the answer.

Websites, Portfolios, Profiles

- https://github.com/dobyfreejr
- https://www.linkedin.com/in/kyle-barbre-81a574239

Accomplishments

- Built Winston from Scratch.
- Migrated a biotech research facility EDR from S1 to CS of 80 end points in addition to network reconfigurations.
- Setting up Jira Ticketing System for company wide use.
- Self taught assembly and reverse engineering skills for Huntress CTF placing in 87th out of 1018 teams.

Skills

- SIEM management
- Threat Hunting
- Log Analysis
- Wireshark Usage
- IDS/IPS Knowledge
- Vulnerability Assessment
- Nmap Scanning

Personal Projects

"Winston" Malware Analysis Tool

- **Description**: Developed a comprehensive malware analysis tool aimed at empowering Security Operations Center (SOC) analysts to swiftly identify and mitigate cyber threats.
- **Key Contributions**:Integrated with VirusTotal API to enable seamless submission and analysis of suspicious files and URLs, leveraging global threat intelligence.
  Implemented WHOIS and IP lookup functionalities to facilitate in-depth investigations into malicious domains and IP addresses.
  Designed an intuitive command-line interface (CLI) for streamlined usability and efficient workflow navigation.
  Demonstrated dedication to continuous improvement by actively troubleshooting and enhancing integration with services like MalwareBazaar.
- **Technologies Used**: Python, VirusTotal API, WHOIS, IP lookup, Command-line Interface.
- **Impact**: Significantly accelerated incident response times and bolstered organizational resilience against cyber threats by providing SOC analysts with a robust toolkit for malware analysis and investigative tasks.

Home Network Monitoring with ELK Stack

- **Description**: Designed and implemented a comprehensive network monitoring solution using the ELK (Elasticsearch, Logstash, Kibana) stack to monitor activity and analyze logs on my home network.
- **Key Contributions**:Configured Elasticsearch as a scalable and distributed search and analytics engine to store and index network logs and events.
  Utilized Logstash for log ingestion, parsing, and enrichment, enabling seamless integration with various data sources within the home network.
  Developed custom Kibana dashboards to visualize network traffic, identify anomalies, and track system performance metrics in real-time.
  Leveraged Google Cloud Platform (GCP) to host and manage the ELK stack, ensuring high availability and scalability of the monitoring infrastructure.
- **Technologies Used**: Elasticsearch, Logstash, Kibana, Google Cloud Platform (GCP).
- **Impact**: Empowered proactive monitoring and troubleshooting of network issues, enhancing network security and optimizing resource utilization within the home environment.

- TCP and IP Protocols
- Python and Bash proficiency
- Malcolm
- CrowdStrike Falcon
- Reverse Engineering with Ghidra
- Incident Response

Hobbies

- Working on Winston
- **Raspberry Pi Projects,**
- Pihole
- Home Networking Speed Monitor
- Chatgpt with OpenWebui
- **Linode Projects**,
- Wazuh
- OpenVpn
- Beef