Wiktor Kaczor

Mobile Number: 07936271953

Email: wiktoraleksanderkaczor@gmail.com

Website: https://wiktorkaczor.com

LinkedIn: https://www.linkedin.com/in/wiktorkaczor

Home Address:

Flat 14, 9 Muirhouse Crescent

Edinburgh

EH4 4QF

Education

Undergraduate Study at Edinburgh Napier University (2019 to 2021):

- BEng (Hons) Cybersecurity and Forensics (3rd Year Entry) with First Class Honours [2019 to 2021]

Higher Education at Edinburgh College (2016 to 2019):

- Higher National Diploma Computing: Networking - Grade A (SQCF Level 8) [2017 to 2019]
- National Certificate Computing: Technical Support - (SQCF Level 6) [2016 to 2017]

Additional Certifications:

- Splunk Core Certified Power User [Certified 2022]
  https://www.credly.com/badges/9316b645-80f6-4db7-bb0c-4fbf985d1a2d
- Splunk Core Certified User [Certified 2021]
  https://www.credly.com/badges/01d7b394-831b-42cf-8d89-f0c8eaed8abb
- MTA (Microsoft Technology Associate): Windows Operating System Fundamentals [Certified 2017]
  https://www.youracclaim.com/badges/754731c9-fdf1-461a-b0e5-b658b1839778

Work Experience

Software Developer

- Adarma, United Kingdom
- May 2022 to May 2023

Overview:

My job involves utilizing various AWS-oriented computing, storage, and observability systems with a specialization in server-less lambda and container based architecture. Utilizing infrastructure-as-code and containerization tooling such as Terraform and Docker. PyTest industry-standard testing framework usage plus in-house extensions for interfacing with server-less architecture. Finally, security event investigation enrichment tooling, both vendor provided and written in-house.

Responsibilities:

- Agile-based meetings discussing and working with cross-functional teams to implement business requirements
- Platform serviceability improvements, mainly credential asset health validation and related automated support issue creation
- Documenting service up-time conditions and failure scenario cases for determining service level agreement fulfillment
- AWS service integration and usage, particularly lambda compute, object storage, low-latency caching, document and relational databases with inclusions cloud-based logging, and metric monitoring
- Utilizing containerization technology for Python-based AWS Lambda services deployment and local testing
- In-house testing migration to industry-standard framework with test profiling and debugging features
- Troubleshooting and debugging using various monitoring platforms, mainly log search and tracing based
- New security enrichment functionality based on historical event data to reduce duplication of effort
- Security posture improvements with cross-site script stripping and user input validation
- CI/CD code quality assurance and schema update pipelines
- Minor assorted front-end improvements and fixes

SOC Analyst

- Adarma, United Kingdom
- August 2021 to May 2022

Responsibilities:

- Monitoring clients' IT infrastructures for threats
- Triage, investigate and escalate security incidents
- Conducting monitoring for new security rule development
- Hunting for the newest Indicators of Compromise (IoC) within client estates
- Assisting with response process development
- Verifying security event detection with tools and databases to confirm reputation
- Updating thresholds, whitelists and threat lists for new and existing security rules

Student

- Edinburgh Napier University, United Kingdom
- August 2019 to June 2021

Responsibilities:

- Developing a dissertation project using existing photogrammetry solutions for image tracking purposes
- Analyzing existing source code for vulnerabilities using secure software development practices
- Collaborating with a team on web technologies group project for employee rota management system
- Python scripting for network packet analysis, filtering and geographical location lookup
- Analyzing file and operating system artifacts for forensic evidence
- Executing and protecting against attacks in an IoT network simulator
- Basic network server penetration testing

References

- Adarma (Cybersecurity) - PeopleTeam@adarma.com
- Dr Sean McKeown (Edinburgh Napier University) - S.McKeown@napier.ac.uk

Personal Projects

Distributed storage, compute and database with ephemeral cluster (WIP)

Abstracted multiple-access storage with various backends, auto-discovering and bootstrapping hosts forming consensus:

- Ephemeral, master-less and distributed architecture with consensus conflict resolution
- Extensible framework for additional storage implementations and wrappers
- Multi-paradigm distributed database services and compute providers
- File-system in Userspace (FUSE) storage mounting with cluster-level multiple-access
- Network auto-discovery service configuration and bootstrapping
- No external service dependencies