Theodore Brucker

Objective

To secure a cybersecurity software development role leveraging my hands-on SOC experience with industry-leading security tools, practical expertise in machine learning and network intrusion detection systems, in-depth knowledge of privacy engineering and regulatory compliance, and strong foundation in software development and automation.

Projects

Network Intrusion Detection with Machine Learning (MVP)

- Developed scalable microservice for real-time anomaly detection using Python, Docker, Kafka
- Implemented Transformer-based Autoencoder with TorchServe for continuous model improvement
- Created data pipeline with MongoDB integration for storage and SQL querying
- Built React frontend and Flask backend for security professionals to manage data and investigate anomalies

Automation of SOC Business Processes

- Identified inefficiencies in manual security configuration audits at a Security Operations Center
- Developed bash script to automate configuration management of Linux event collectors
- Reduced audit time by dozens of hours per month across multiple clients
- Eliminated human error in configuration management, ensuring policy compliance
- Improved client assurance while reducing operational costs

Education

UNIVERSITY OF MAINE

B.S. Computer Science 05/04/2024

- Key Coursework: Machine Learning (developed NIDS project), Software Development, Privacy Engineering
- Relevant Project: Implemented machine learning-based anomaly detection system, precursor to post-graduation NIDS

COMPTIA

Security+ 07/15/2023

Experience

SYSTEMS ENGINEERING https://www.systemsengineering.com Portland, ME

SOC (Security Operations Center) Technician **08/28/2022 – Current**

- Detected, investigated, and triaged incidents using FortiSIEM, Adlumin, Huntress, Arctic Wolf, and Qualys
- Developed semi-supervised bash script for Linux event collector configuration management, reducing audit time and improving standardization
- Maintained security event collectors, enhancing event detection capabilities across multiple clients
- Communicated threats and recommended actions directly to clients, honing technical communication skills

Network Engineering Intern **05/23/2022 – 08/27/2022**

- Gained hands-on experience in client-facing infrastructure, network administration, and network security
- Rotated through various roles, developing a comprehensive understanding of cybersecurity operations

Research

PRIVACY ENGINEERING - REGULATORY COMPLIANCE LAB University of Maine

Student Researcher **09/01/2021–05/04/2024**

Privacy Engineering and Regulatory Compliance Lab

- Investigated privacy laws and practices in relation to the software development lifecycle
- Contributed to development of tools for maintaining privacy best practices and regulatory compliance
- Gained insights into upcoming regulatory shifts and their impact on cybersecurity software development

Research Presentations

Presented "Evaluating Privacy Questions From Stack Overflow: Can ChatGPT Compete?" at IEEE International Requirements Engineering Conference, Hannover, Germany (September 2023)

Presented "Investigating Which Privacy Topics Software Developers Most Struggle With" at UMaine Student Symposium, Orono, Maine (April 2024)