Anthony Tam

SECURITY RESEARCH, SOFTWARE DEVELOPMENT

☎ +1 (647) 786 8248 | ✉ hello@anthonyt.ca | ⌂ www.anthonytam.dev | anthonytwh

Skills

Programming	Python, SQL, Javascript, Typescript, HTML5, CSS, LaTeX
Frameworks	Tensorflow, Keras, Scikit-learn, Pandas, Flask, NodeJS, ReactJS, AngularJS
Tools/Infra	AWS, Docker, Gitlab, Redis, PostgreSQL, Linux, Wireshark, Powershell, Kali Linux

Experience

Darktrace

Toronto, Canada/Remote

LEAD SECURITY DEVELOPER, THREAT DETECTION — *May. 2020 - Present*

- Research and develop machine learning models to detect adversary activity in the network, cloud and SaaS environments.
- Maintain 900+ threat models, improving accuracy and fidelity of detections by ~25% using test-driven development and CI/CD.
- Develop and maintain analytical tools (fullstack) used to identify statistical trends and malicious activity in global breach data.
- Research classification methods to improve detections of malicious activity such as DNS Tunneling communications.
- Simulate cloud and network attack tools, and tested malware against our detection systems to improve capabilities.
- Lead development of Cloud and SaaS threat detection models in AWS, Azure, GCP, M365, GSuite, Salesforce, Okta, etc.
- Train internal teams and supported key strategic customers with model optimization, development, and training.

CYBER SECURITY ANALYST — *Nov. 2018 - Apr. 2020*

- Lead analyst in Canada and security Subject Matter Expert, supporting strategic technical client engagements in North America.
- Performed threat hunting exercises on client environments, writing weekly/monthly threat reports with detailed technical analysis.
- Investigated active compromises and live pen-tests in customer environments, compiling incident reports for clients/executives.
- Maintainer of the Darktrace Python library, a light-weight wrapper library for simple implementation of the Darktrace API.
- Identified 50+ new IOCs for Darktrace's internal threat intel database from threat hunting exercises and research activities.

CYBER SECURITY ENGINEER — *Sep. 2017 - Oct. 2018*

- Architect deployments and integrations of Darktrace products for network, virtual, and cloud environments.
- Traveled weekly to lead onsite technical integrations with security engineers, managers and executives.
- Developed internal SSH CLI tool to improve workflow, speed and security of accessing internal resources.
- Contributed to over 30% growth of the Canadian customer base from proof-of-value customer trials.

Zebra Technologies

Mississauga, Canada

CATEGORY MANAGEMENT ANALYST — *May. 2016 - Aug. 2016*

- Developed a dynamic Excel (VBA) dashboard to automate monthly analysis reporting of vendor operational and financial risk.
- Led RFQ/RFP exercise with key vendors to reduce cost on tail-spend of global semiconductor component procurement.

Education

McMaster University

Hamilton, Canada

B.ENG.MGT - BACHELOR OF MECHANICAL ENGINEERING AND MANAGEMENT — *Sept. 2012 - Apr. 2017*

- Five-year program incorporating engineering major, business management minor and multi-disciplinary projects.

Nanyang Technological University

Singapore, Singapore

INTERNATIONAL EXCHANGE PROGRAM — *Aug. 2014 - May. 2015*

- Study abroad for one year, exploring the local and neighboring cultures across South East Asia.