Preston Crowe

www.prestoncrowe.com

Email : prestonjcrowe@gmail.com
Mobile : (415) 265 - 3937
Github: prestonjcrowe

Passionate about privacy.
Security Engineer immersed in researching emerging threats with a focus on internal tools. Interested in network security research, service development, and automation.

Education

- **University of Washington** — Seattle, WA
  Computer Science [Dean's List, 3.71 GPA] — *Sep. 2016 – June. 2020*

  Relevant Coursework: Security, Cryptography, Networks, Hardware/Software Interface, Data Management, OS

Experience

- **Extrahop** — Seattle, WA
  Security Engineer — *December 2020 - Present*
  - **Security Engineer II**: Shifted focus from detector development to purely research and internal tooling. Built a system to visualize and query anonymized customer data to aid the detector team in building software and cloud service classifiers. Lead the effort to validate detections with the Mandiant Security Validation platform by developing a suite of tools to automate simulations and collect performance data.
  - **Security Engineer I**: Reproduced exploits in a lab environment, produced research documents and implemented rule based detectors. Built and maintained automated systems for collecting vulnerability data and exploits. Developed chat bots to interact with our vulnerability ticketing system and publish daily summaries of the most discussed CVEs on Twitter. Worked closely with the technical writing team to provide background details and guidance for detection annotations.
- **Baffin Bay Networks** — Seattle, WA
  Internship — *June 2019 - September 2019*
  - **Data Collection and Full Stack Development**: Customized logging solutions in open source software, improved proprietary data collection services built with Golang, and developed an API for Baffin Bay's Threat Insight platform. Prototyped an internal dashboard for monitoring the state of a complex sensor network in React.
- **F5 Networks** — Seattle, WA
  Internship — *June 2018 - September 2018*
  - **F5 Labs**: Worked with a team of security researchers at F5 Labs to develop a serverless vulnerability data pipeline and API. Visualized attack data including a live threat map and contributions to Black Hat talk. Automated CVE data collection, parsing, and metrics.
- **NASA AMES Research Center** — Mountain View, CA
  Internship — *June 2017 - September 2017*
  - **OpenMCT**: Implemented JSON import and export functionality for workspaces and folder hierarchies in OpenMCT, an open source mission control application. Worked on a large team in an enterprise environment; wrote extensive tests for each piece of code I contributed.

Skills

- **Programming Languages**: Python, Javascript, Golang, Java, C
- **Vulnerability Research**: PCAP analysis, exploit reproduction
- **Automation**: Web scraping, CI/CD, data collection
- **AWS**: Lambda, S3, EC2, Elasticsearch, Opensearch

Publications

- **Extrahop**: PetitPotam: Expanding NTLM Relay Attacks
- **F5 Networks**: Breaking Down the Door to Emergency Services through Cellular IoT Gateways