

**Brian Jopling**  
3514 Lancaster Ave, Apt 116  
Philadelphia, PA 19104  
267-644-5009  
brian.r.jopling@drexel.edu  
<https://www.brianjopling.com>  
<https://www.github.com/PolyatomicBrian>

---

## Education

Drexel University  
Bachelor of Science in Computer Science  
Computer Security

Philadelphia, PA  
Anticipated Graduation: June 2020  
Cumulative GPA: 3.70, Dean's List

## Skills

- Programming Languages: Python, Bash, Java, C++, C#, HTML, CSS, JavaScript, PHP, SQL, Visual Basic.
- Frameworks: Django, Spring, jQuery, Bootstrap, Scrapy, Drupal.
- Tools & Software: Elasticsearch, Kibana, Docker, Git, Vi/Vim, Nmap, Wireshark, BurpSuite, Zed Attack Proxy (ZAP), Metasploit, Volatility, Hashcat, Nessus, VirtualBox, VMware, Eclipse, Visual Studio Code.
- Amazon Web Services: VPC, EC2, ECS/Fargate, IAM, CloudWatch, CloudTrail, Lambda, CloudFormation, DynamoDB, S3, Route 53, API Gateway, Kinesis (Firehose, Data Analytics), SageMaker, Elastic Beanstalk, Cognito, CodeBuild, CodeDeploy, CodePipeline.
- Operating Systems: GNU/Linux (Fedora, Kali Linux, Ubuntu), Windows (XP, 7, 8, 10), Mac (macOS).

## Experience

Comcast Corporation  
Security Engineer

Philadelphia, PA  
April 2018 to Present

- Performed infrastructure automation by crafting CloudFormation templates, custom Lambda functions, & shell scripts.
- Upgraded existing DynamoDB infrastructure from provisioned capacity to on-demand, saving \$160,000 annually.
- Automated & maintained infrastructure for serverless MFA API ingested by customer-facing Xfinity Authenticator app.
- Integrated CI/CD for Lambda-backed API and ECS (Fargate) through CodeBuild, CodePipeline, and CodeDeploy.
- Implemented SSO into PKI application front-end using OpenID Connect to permit access to only Comcast employees.
- Architected modular anomaly-detection engine, utilizing SageMaker, to identify evolving threats found in web traffic.
- Architected extraction, transformation, and storage of Big Data using AWS Data Pipeline, Lambda, and DynamoDB.
- Designed and developed serverless vulnerability management notifier, parsing logs from Security Monkey using Lambda and emailing account owners of the vulnerabilities using SES.

University of Pennsylvania School of Arts & Sciences  
Information Security Engineer

Philadelphia, PA  
April 2017 to March 2018

- Developed NECTOR, an open source SIEM that provides analysis of security alerts produced by Nessus.
- Performed frequent security audits on university websites and their servers.
- Discovered and patched XSS vulnerability affecting majority of existing SAS websites, preventing future attacks.
- Conducted code reviews on Drupal Core and Contributed modules to ensure SAS websites were secure.
- Assisted with vulnerability management by reviewing logs produced by Nessus and OSSEC.
- Engaged in incident response team by analyzing memory dumps of infected computers using Volatility.

Fit Results Personal Training & Cycle Studio  
Technical Officer

Skippack, PA  
May 2014 to August 2015, June to September 2016

- Designed and developed company website using HTML, CSS, JavaScript, and the Bootstrap framework.
- Migrated existing source code from local storage to GitHub repository to promote version control.
- Actively maintained website using Bootstrap, jQuery, and custom JavaScript on a weekly basis.
- Managed electronic devices (iPads, iPhones, and desktops) by monitoring usages and maintaining software updates.
- Integrated CI/CD into the workplace using git-ftp, pipelining commits to host's FTP server.

## Activities

- Co-Founder, DEF CON 215 (DC215.org), Present
- Volunteer, WOPR Summit (woprsummit.org), Present
- Participant, BSidesPhilly, BSidesNYC, 2018
- Drupal Security Tool Developer, Drop-Fuzz, 2017
- Web App Developer, Anthology, 2017
- Mobile App Developer, The Cave of Trials, 2016
- Mobile App Developer, Coin Grabber, 2015
- Member, Robotics Club, Methacton High School, 2011-15