JONATHAN DEFREEUW

redacted ⋄ defreeuw@vt.edu
https://jonathandefreeuw.com
Active DoD TS/SCI Security Clearance

WORK EXPERIENCE

U.S. Naval Research Laboratory June 2017 - Present
Computer Engineer *Washington, D.C.*

- Serve as Principal Investigator and Technical Lead for research and development portfolio spanning malware analysis, network intrusion detection systems, and cloud security.
  - Successfully align technical milestones with Department of Defense strategic modernization goals.
  - Secure and manage a ∼$1M/year research budget, authoring technical proposals and delivering executive briefings to high-level stakeholders to justify funding for critical cybersecurity research.
  - Deliver milestone and technical reviews to demonstrate capabilities.
- Architected, deployed, and administered an enterprise automated malware analysis platform using a collection of commercial, government, and open-source tooling in support of Navy network operations.
  - Engineered a containerized suite of microservices to coordinate data processing and enable simplified integration of new capabilities.
  - Administered Linux systems, maintained DevSecOps pipelines to accelerate feature deployment.
  - Spearheaded a critical migration to Kubernetes that improved system scalability, reduced infrastructure overhead, and minimized analysis turnaround times.
- Designed, built, and optimized network security monitoring platforms using Zeek and Suricata, ensuring robust telemetry collection and threat visibility across both on-premise and cloud deployments.
  - Developed Ansible roles and playbooks to support the rapid deployment and configuration of network sensors and their remote management systems.
  - Unified system architectures into an infrastructure-agnostic design that streamlined patch management and reduced system complexity for administrators.
  - Performed continuous integration and quality assurance testing using Ansible to verify the correctness of these complex, mission-critical systems in support of Navy sponsors.
- Researched the use of neural networks and unsupervised clustering in the detection of novel malware samples, including Advanced Persistent Threats (APT).
  - Developed pipelines for automated malware unpacking and clustering to detect functional relationships between known and unknown APTs.
- Actively lead cross-functional Agile teams of 3 to 5 civilians and contractors, serving as Project Lead and Scrum Master to consistently deliver research milestones.
  - Foster a collaborative, high-performing research environment by mentoring junior developers, managing sprint lifecycles, and bridging the communication gap between technical teams and senior leadership.
  - Engage and onboard summer interns, providing academic and professional mentorship through mission-essential projects.

EDUCATION

Virginia Tech August 2016 - December 2018
M.S., Computer Engineering **Overall GPA**: 3.61/4.0
Thesis: *Embedding Network Information for Machine Learning-based Intrusion Detection*

Virginia Tech August 2013 - May 2017
B.S., Computer Engineering - Magna Cum Laude **Overall GPA**: 3.60/4.0
Minors in Cybersecurity, Computer Science, and Mathematics

SKILLS & PROFICIENCIES

Python - Django, Flask, Celery, PyTorch	GitLab CI/CD, Jenkins, Ansible, Terraform
Linux - RHEL, Debian, Talos, CoreOS	Cassandra, PostgreSQL, Redis, MinIO, Elasticsearch
Docker, Podman, Kubernetes, Rancher	Cuckoo Sandbox, CAPEv2, Suricata, Zeek
Proxmox VE, VMware vSphere, AWS	Juniper Junos, Cisco IOS, OpenFlow, OpenVSwitch

PERSONAL PROJECTS

Bare Metal Kubernetes With Fedora CoreOS *in progress*

- Configure network boot environments using Fedora CoreOS as baseline image
- Use Ignition and matchbox to create a pipeline for updating a cluster of bare metal hosts
- Automate bare-metal Kubernetes cluster deployment with minimal user interaction

Cloud Resume Challenge *in progress*

- Develop a static website using Hugo to deploy in AWS using S3, CloudFront, and Route53, with a visitor counter using DynamoDB and Lambda
- Automate updates to the website using Terraform and GitHub Actions to push new files, create new AWS resources, and invalidate caching
- Progress can be viewed at *https://jonathandefreeuw.com*

Deploying Talos Linux Using Ansible

- Automate the deployment and bootstrapping of a Talos Linux cluster using Ansible
- Enable configurable-sized clusters on Proxmox VE, including updates to Talos Linux images
- Code can be found on GitHub at *https://github.com/jdefreeuw/talos-ansible*

Home Raspberry Pi Cluster

- Operated a 6-node Raspberry Pi cluster as a testbed for practicing container technologies at home
- Deployed 3-master, 3-worker Kubernetes cluster using K3s with distributed GlusterFS storage
- Enabled PXE Boot on Raspberry Pis using pfSense and TrueNAS SCALE for reliable storage and backups
- Run containers for at-home services such as Pi-hole, Omada Controller, and BookStack

Brute Force Defense Using OpenFlow on Raspberry Pi

- Prototyped a software-defined network on a cluster of Raspberry Pis and designed a threshold-based IPS
- Used a POX controller and OpenVSwitch to perform rate-limiting to protect Internet-connected camera
- Performed brute force login attempt using Hydra as a proof-of-concept attack

ADDITIONAL EXPERIENCE

Haven Church September 2020 - Present
Media Director

- Lead and train a team of volunteers in audio mixing and video presentation for weekly services using Behringer mixers and RenewedVision ProPresenter software
- Operate church website for church resources and information, performing weekly editing on sermon recordings for listening on both Spotify and Apple Podcasts
- Spearheaded the design and procurement of a mobile AV system, including training for volunteers on setup and teardown procedures