This document is generated by a Kubernetes sidecar running Pandoc.

This is all self hosted and the full stack is maintained and run myself.

Colin Tufts

E-Mail: colin@colintufts.com

Website: https://colintufts.com/

LinkedIn: https://linkedin.com/in/colintufts/

Keybase Proof: https://keybase.io/colintufts

Professional Summary

Seasoned security engineering leader interested in protecting critical infrastructure and defense systems. Combining deep expertise in threat intelligence, incident response, and security automation with a strong foundation in cloud architecture and DevSecOps. Passionate about implementing robust security frameworks and advancing canadian national security interests through technology. Current OSCP and CPTS Candidate with extensive experience in both offensive and defensive security operations. Working towards completing my CISSP.

Employment History

¶ **Senior DevSecOps Engineer** (Peoples Group)

February 2025 - Current

- Architect and implement CI/CD pipelines from the ground up to support secure software delivery.
- Integrate AWS and Azure environments into Microsoft Sentinel for centralized security monitoring.
- Leading the Security Centre of Excellence, ensuring security is a focus of our SDLC.
- Reevaluate and enhance AWS configurations, supporting a seamless migration to Azure cloud.
- Develop and enforce infrastructure as code practices using Terraform and GitHub Actions.

- Implement Azure Blueprints to ensure consistent policy enforcement across resources.
- Conduct regular threat modeling and risk assessment sessions to mitigate security vulnerabilities.
- Integrate and tune SAST/DAST tools for continuous security scanning.
- Collaborate with development teams to embed security processes in the SDLC.

¶ **Cloud Security Engineer** (Firmex)

July 2023 - Current

- Actively monitor and research cyber threats impacting business operations or technology infrastructure
- Handle Incident Management and Incident Response, leading the organization in cyber threat management.
- Conduct Vulnerability Management and Penetration Testing, and ensure compliance with PCI, HIPAA, GDPR, SOC
- Work collaboratively within a team of security professionals across the organization on security best practices and product support
- Collaborate with engineering, infrastructure services, and application development to integrate technology solutions
- Develop subject matter expertise on assigned security technologies for efficient delivery of security services
- Implement custom software solutions using python and applicable scripting languages, including writing scripts in PowerShell/Bash
- Configure, automate and actively monitor threats within AWS using SecurityHub and GuardDuty
- Develop standards in partnership with other teams
- Create, Implement, advance security posture and status via CI/CD pipelines
- Make use of Kali linux and security tools such as Burpsuite, Wireshark to find and test vulnerabilities in our applications
- Make use of the Microsoft Azure suite of tooling, including Microsoft Sentinel, Defender Security Platform, to analyze the environment for threats as well as triage incidents
- Contribute to the Development of Standards, Technical Security Specifications, and Operating Procedures

- Provide support to various IT, IT Security, and Business projects with insights on security technologies
- Manage and configure AWS services, including writing Cloudformation templates
- Work extensively with Windows, Linux infrastructure, and SaaS/PaaS environments in a 24x7 production environment across multiple data centers and Public Cloud providers

¶ **Industrious** (DevSecOps Engineer)

March 2022 - February 2023

- Working with Github actions and other build tools such as CircleCI in a CI/CD process to build and deploy to AWS cloud environment
- Maintain, update ACLs, VPC environments, to keep all systems secure.
- Containerize and upgrade legacy applications to provide better adaptability and provide continuous delivery of the applications.
- Deploying/implementing Grafana, Prometheus, and other monitoring tools for observability of traditional services and micro-services.
- Monitoring all environments (via tools like Elastic Beanstalk, EC2, S3, Cloudwatch, Cloudtrail) acting preemptively to prevent system failures and outages
- Implement systems architecture and data strategy projects while minimizing impact on internal teams and members
- Architect, implement and build deployment solutions for downstream consumption.
- Increase reliability, maintainability, scalability of existing and future stacks

¶ **Cloud Administrator** (Deluxe)

November 2020 - March 2022

- Member of the production SRE team during incidents and outages with investigation of stack / node / container failures.
- Grafana dashboard and Observability SME.
- Container triage and management SME.
- Turbonomic (Application Performance Management) SME.
- Incident responder, including threat and vulnerability management.
- Built dashboards for both executive management and production support consumption for insight into deeper environmental stability.

- Regularly contributed to our internal tooling to manage administrative operations across the environment.
- Heavy usage of scripting (ansible, bash, powershell, powercli) to automate and create tooling to increases operation effectiveness.
- Responsible for the overall support, maintenance, and deployment of Private and Public cloud infrastructure.
- Instructing junior staff with incident management tasks, operational tasks, and administrative tasks some examples are server level restorations, tool development, application deployment, vulnerability remediation.
- Provisioning, configuring, operating, maintaining, patching, and backing up all infrastructure through manual and automated processes.
- Responsible for Bare metal through all levels of virtualization and containerization.
- Senior escalation point for incident response.

¶ **Systems Administrator** (IMS)

August 2019 - November 2020

- Created and Implemented auditing system, reducing auditing timeline from 3 weeks to 30 minutes.
- Configured Nagios and Centreon monitoring scripts for production systems.
- Liason to executive leadership team for monitoring and observability.
- Worked with management and external customers to establish and evaluate SLAs and SLOs
- AWS SME for multi-cloud environment.
- Lead VMware cluster upgrade, requiring the management and distribution of work to multiple departments and resources.
- Lead Stakeholder in Data-Center Infrastructure & Maintenance
- Cassandra SME, lead all efforts related to maintenance and integration with Cassandra
- Trained and evaluated new-hires and upskilling employees for the Operations Team
- Implemented changes following ITIL best practices and encouraged others to do so.
- VMware SME, lead for all things virtual.

DevOps Tools

Terraform/HCL - 4

AWS Cloudwatch - 4

Docker-Compose - 4

Turbonomic - 5

Vagrant - 2

Puppet - 3

Grafana - 3

Prometheus - 3

Chef - 3

CI/CD Tools

Jenkins - 3

CircleCI - 3

Github Actions - 3

Gitlab - 4

General Skills

Python - 5

Ansible - 5

Kubernetes - 4

REST Frameworks - 2

HTML(5) - 3

CSS(3) - 2

Observium - 2

MongoDB - 4

MySQL - 5

Postgres - 3

AWS DynamoDB - 2

Docker - 5

Linux - 5

Nginx - 5

Apache - 5

JSON - 5

XML - 4

Bootstrap Framework - 2

SMTP - 3

DNS - 4

Wordpress - 5

Git (SCM) - 4

Postfix - 3

Nagios - 4

ChatGPT - 3

LLM - 3

Prompt Engineering - 3

Tomcat - 2

ElasticSearch - 3

Redis - 4

Networking - 4

Ruby - 2

Perl - 2

PHP - 3

JQuery - 1

C/C++ - 2

Java - 1

Golang - 2

Oracle - 2

Javascript - 4

Typescript - 4

Cassandra - 3

Splunk - 3

Kibana - 3

GuardDuty - 3

SecurityHub - 3

Microsoft Sentinel - 3

jira - 3

Wazuh - 3

Pentesting Skills

Enumeration - 3

BurpSuite - 3

nmap - 4

Metasploit - 4

Forensics - 4

Vulnerability Research - 4

Reverse Engineering - 3

PoC Development - 3

Interesting Projects

---

python_resume A showcase of Python/Flask/Jinja2/HTML(5)/Bootstrap/JQuery used to both generate colintufts.com and my hardcopy resume.

Document generation time: 2025-10-24 18:14:45.419211 (UTC).

Document UUID: 48f549ef-190d-4e05-bbf3-4012a2de98b1

Generation: 335918

ContainerId: 158ffa3fb4bf Load: 0.40 0.47 0.52