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

Employment History

¶ **Firmex** (Cloud Security Engineer)

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

¶ **Deluxe** (Cloud Administrator)

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 contributes 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.

¶ **IMS** (Systems Administrator)

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.

Code Portfolio

---

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: 2024-10-20 21:24:52.346511 (UTC).

Document UUID: 4b9ebe62-fbef-4bc6-84b9-08ddaa67a915

Generation: 107500

ContainerId: 2edc349396d0 Load: 0.44 0.47 0.45