

CHRIS EHOLER

Kelseyville, CA | 530-228-6244 | chris@eheler.tech
eheler.tech | linkedin.com/in/chris-eheler-639480144 | github.com/ceheler

SECURITY ENGINEERING | INFRASTRUCTURE SECURITY | SECURITY AUTOMATION

PROFESSIONAL SUMMARY

Systems, software, and security professional with six years of technical experience supporting production environments across application development, systems administration, networking, and security operations. Professional security experience includes FortiGate firewall administration, Wazuh SIEM deployment and detection tuning, network segmentation and VPNs, security-event investigation, and PCI DSS remediation. Strong software-development background in C#, with current security automation and cloud engineering work using Python, PowerShell, AWS, Terraform, IAM, and CloudTrail.

TECHNICAL SKILLS

Security: Wazuh SIEM, FortiGate, Security Monitoring, Detection Engineering, Windows Security Events, Firewall Policy, Network Segmentation, PCI DSS Remediation

Infrastructure: Windows Server, Active Directory, Hyper-V, DNS, DHCP, Linux

Cloud & IaC: AWS, Terraform, IAM, VPC, CloudTrail, Systems Manager

Software & Automation: C#, Python, PowerShell, SQL, LINQ, Git, JSON

Networking: TCP/IP, Cisco Switching, VLANs, VPNs

PROFESSIONAL EXPERIENCE

Deputy Sheriff | Lake County Sheriff's Office

July 2023 - Present

- Conduct complex investigations and serve as a technical resource for digital evidence, mobile-device forensic extraction data, computers, storage media, body-worn camera systems, and field-computer troubleshooting; produce detailed investigative documentation and courtroom testimony.

Jr. Systems Administrator / Software Developer | Transfer Flow Inc.

April 2020 - July 2023

- Deployed and administered Wazuh SIEM across approximately 100 workstations and machine controllers, managed agents through Group Policy, created detection rules and alerts, and investigated security events and unauthorized access attempts against public-facing infrastructure.
- Selected, installed, and configured FortiGate firewalls, including VLAN segmentation, firewall policies, site-to-site VPN connectivity, and ongoing security administration.
- Partnered with an external PCI DSS auditor to remediate infrastructure findings and reduced exposure from vulnerable legacy systems through network isolation when upgrades were not feasible.
- Designed and implemented a Cisco switching refresh and 10 Gb server backbone while administering five Hyper-V hosts supporting approximately 15-35 virtual machines and AD, DNS, DHCP, and SQL Server services for more than 100 users.
- Developed and maintained production C# applications supporting reporting, inventory management, engineering file versioning, and internal business processes using C#, LINQ, and Microsoft SQL Server.

Technical Support Specialist | Transfer Flow Inc.

August 2017 - April 2020

- Resolved workstation, application, account, and infrastructure issues through Jira; documented technical processes and communicated technical recommendations to technical and nontechnical stakeholders.

Corporal, Motor Transport | United States Marine Corps Reserve

September 2013 - July 2019

- Selected for a Maintenance and Supply Quality Control Chief billet normally assigned to a Sergeant; provided technical quality control and instruction for automotive and electrical systems and previously held a U.S. government Secret security clearance.

SELECTED SECURITY ENGINEERING PROJECTS

Security Automation & Detection Lab

C# | PowerShell | Python | Windows Security Events | Linux Security Logs

github.com/ceheler/SecurityEventAnalyzer | github.com/ceheler/SecurityAutomationLab

- Built a cross-platform security automation workflow that collects and normalizes Windows and Linux security telemetry into structured events for modular analysis and detection.
- Implemented detections for brute-force activity, account creation, privileged-group membership changes, and network port scanning, including time-window correlation and standardized findings.
- Developed Python and PowerShell tooling for collection, normalization, filtering, and analysis of Windows Security Events, Linux SSH authentication activity, and UFW firewall telemetry.

CloudTrail Security Monitor

Python | AWS CloudTrail | Detection Engineering

github.com/ceheler/cloudtrail-security-monitor

- Built a Python CloudTrail parser and modular detection engine that identifies selected security-relevant AWS API activity and generates standardized findings with identity, source, affected-resource, and execution-result context.
- Validated detections against controlled Terraform-generated activity using benign, successful, failed, multi-resource, missing-field, and malformed-data test scenarios.

Terraform Security Lab

Terraform | AWS | IAM | VPC | Systems Manager

github.com/ceheler/terraform-security-lab

- Built a reusable AWS environment through Terraform using VPC networking, public and private subnets, security groups, EC2, IAM roles, and AWS Systems Manager access without exposing SSH.
- Separated administrative and Terraform execution permissions through IAM roles and used the environment as a controlled telemetry source for CloudTrail detection validation.

EDUCATION & CREDENTIALS

Associate Degree, Computer Programming - Butte College

Fortinet Network Security Expert (NSE) Level 4 - Legacy credential