

Colorado, USA

(970) 538-7205

trevor@blacktemple.io

<https://blacktemple.net>

TREVOR CASE

Hi, I'm Trevor. I enjoy solving problems and being creative. Above all else, I am a results-driven Professional Security Engineer with notable success in planning, analysis, vulnerability management, and implementation of security initiatives.

SKILLS

Amazon Web Services, PCI-DSS Compliance, Static Code Analysis, Dynamic Application Security Testing, Vulnerability Management, Firewalls (SGs) and Networking.

Tooling – Python & Bash Scripting, VS Code, GitLab, GitHub, SonarCloud, Tenable, Black Duck, Alert Logic MDR (SIEM), DataDog Monitoring, Sophos, JIRA, Confluence, Slack and various other Open Source Tooling related to Security.

CAREER HIGHLIGHTS

Revel Systems

- Led 2022/2023 PCI Audit to completion, ISO27001. Received Promotion to Lead Security Engineer April, 2023.

Monarch Mountain

- Transitioned the entire workforce to WFH during the COVID-19 Pandemic.

IntraNerve

- Helped lead Domain & Infrastructure migration to come under one unified entity, “IntraNerve Neuroscience”. A Hybrid environment consisting of On Premise, Microsoft Azure, and Denver based Colocation Infrastructure.
- Achieved CompTIA Network+ CE.

EXPERIENCE

Revel Systems – *Lead Information Security Engineer*

APRIL 2022 – CURRENT

- Provide Information Security and Threat Management for a \$100M SaaS Point of Sale Based Company with more than 10,000+ live locations.
- Incident Response Team Member – Incident Manager responsible for coordinating and directing all facets of related Incident Response Efforts.
- Established/Maintaining a secure base environment
- Driving Secure Coding initiatives across the company
- Identify gaps and opportunities to improve our overall risk posture, designing effective security controls for remediation or mitigation, and assessing potential impacts.
- Perform regular and ongoing Vulnerability Management, including identifying, evaluating, treating, and reporting on security vulnerabilities in production systems, dev/qa environments, and continuous analysis of the software that runs on them to reduce our attack surfaces.
- Conduct comprehensive vendor risk assessments to ensure supplier reliability and security compliance.
- Monitor, Manage, and perform Analysis of SIEM, IDS, EDR, and various other Security Tooling.
- Monitor Cybersecurity News, Known Threat Channels, and perform on a regular basis – Threat Hunting.
- Manage End User Threats, Insider Threats, Automated Phishing campaign efforts, and regular analysis of said results.
- Working to build better Application Security Standards and collaborate directly with Development Teams, SWE/Managers, DevOps, to help move Security left in the Software Development Life Cycle.
- Respond to complex queries and requests for product security information, also providing technical and executive reports as needed.
- Provide advice on and regularly remediate security issues and provide cost-effective solutions.

Monarch Mountain – *IT Systems Engineer*

OCTOBER 2019 – APRIL 2022

- IT Manager
- Maintaining VMware Virtualization & vCenter Management
- Perform System Level Patching & Firmware upgrades

- Run PCI-Compliance Vulnerability Assessments
- Developed 2020 IT Budget and helped plan Infrastructure revisions
- Troubleshoot Network and Server issues throughout environment
- Ubiquity (SDN) Switch & Route and Point 2 Point Dishes
- Network Segmentation (VLAN, Subnetting)
- Utilization of ScreenConnect / Connectwise
- Symantec Enterprise EPP (Anti-Virus) Solution
- Actively Troubleshoot Software and Hardware issues
- Maintain Vendor Relationships regarding New Infrastructure and Pricing
- Life-Cycle Management (ITIL) & IT Asset Management (ITAM)

IntraNerve Neuroscience – *IT System Administrator*

MARCH 2018 – OCTOBER 2019

- Windows Server Management
- Managed Barracuda (F18) Firewalls, NACLs, Maintain The Least Privileged Access
- Barracuda Control Center Management for 40+ Firewalls
- Implemented and Monitored Graylog / SIEM Business Solution
- Vulnerability Assessment Scans and Reports (OpenVAS + Kali)
- Managed Core Route & Switch Troubleshooting
- Network Segmentation (Firewall & VLAN Management)
- VMWare ESXi Cluster and vCenter Administration
- Office 365 Enterprise Administrator
- Quest KACE Ticket Management and IT Asset Management
- Managed Purchasing of IT Equipment / Workstations Repair and Rebuild Computers – DISK WIPE in compliance with HIPAA
- Deployed Web root A/V Enterprise Solution
- Attended DEFCON 2018 Security Conference in Las Vegas, NV
- Achieved CompTIA Network+ CE – (<https://tinyurl.com/networkc>)

Iron Protection Group – *IT Help Desk Support*

MARCH 2015 – MARCH 2018

- Respond to email, phone and ticketing system
- Write, edit, revise training manuals
- Patching Critical Systems
- Provided Technical Assistance for questions and problems

EDUCATION

WESTERN GOVERNORS UNIVERSITY – *BS Cybersecurity and Information Assurance, Information Technology*

APR 2022 - 2026

Attending Western Governors University

PROJECTS

- Website(s) - <https://blacktemple.net>, <https://blacktemple.io>, <https://blog.blacktemple.io>

Implemented Route 53 Service, CloudFront for CDN, AWS Certificate for SSL(HTTPS), built out in Amazon S3 Buckets, Two AWS Code Pipelines for CI/CD from my Website's GitHub repository.

- TryHackMe Cybersecurity Training - **Top 1% Platform**

- **Profile:** <https://tryhackme.com/p/lyricx>

Actively participating in CTFs & Training to better understand the needs of securing organizations from the vast array of Cybersecurity Threats. Always in pursuit of the endless knowledge that is the realm of Information Technology / CyberSecurity.