Kyle Trantham, CISSP | GCFA | GNFA

450 Sherwood Drive #309 • Sausalito, CA 94965 • (810) 348-0368 • kyle.trantham@gmail.com

INFORMATION SECURITY ENGINEER (REMOTE)

Incident Response Lead

A well-rounded, driven, and collaborative professional that values teamwork. Five years of experience in digital forensics and incident response. Excited to continue to learn and further develop my skills.

Key skills include:

- Digital Forensics Expert Witness
- Network Security Monitoring Expert
- Web Application Security Expert
- SIEM Management (Splunk, ELK, Data Analytic)
- Full-Stack Web Development (JS, Python, Bash)
- Linux/Unix and AWS Security/API Experience

PROFESSIONAL EXPERIENCE

Diplomat Pharmacy, Inc. *Flint, MI*
Information Security Engineer (February 2013 – Present)
Improved enterprise by containing breaches, creating efficient alerting, and delivering comprehensive reporting to management. Improved efficiency of operations by delivering automated solutions.

Notable accomplishments:

- Served as expert witness in civil litigation, reporting on critical forensic evidence and findings.
- Lead forensic analyst during several major incidents and malware attack campaigns.
- Traveled to many remote potential acquisitions to identify risks and possible breaches.

Baker College, Flint MI
System Administrator (November 2011 – April 2013)
Designed, deployed, and maintained independent network of student servers and workstations.

Notable Accomplishments:

- Collegiate Cyber Defense Competition (CCDC) - Team Captain 2012 - 2013
- Developed virtualized Collegiate Cyber Defense Competition lab infrastructure and web portal

EDUCATION & CREDENTIALS

University of California, Berkeley CA
Certification, Full-Stack Web Development

Baker College, Flint, MI
Bachelor of Information Technology and Security (Cumulative GPA: 3.55) April 2013

Certifications and Organizations
(ISC)² CISSP, GIAC GCFA, GIAC GNFA, ITIL V3 Foundations, CompTIA Security+

TECHNICAL EXPERIENCE

I maintain the equivalent of an Enterprise Windows/Linux Systems Administrators level of expertise. Using these skills, I am able to efficiently interface with operations staff to complete tasks, enabling high productivity.

Windows Server:

- Active Directory (DHCP, DNS, CA, DFS)
- IIS (Security Hardening, Management)
- SCCM (Package Deployment, reporting)
- PowerShell (Automation, API Orchestration)
- MS SQL (Security Hardening, Key Rotation)
- Hyper-V (Deployment, Management)

Linux/Unix:

- Debian AppArmor
- Iptables (UFW, Firewalld)
- RedHat/CentOS SELinux
- Proficient BASH scripting

Virtualization:

- VMWare (vSwitch NSM, Guest Forensics)
- Citrix
- Hyper-V
- KVM

Cloud:

- AWS (Security Hardening, API)
- O365 (API, InTune, CASB, IAM, MFA)
- Azure (Web App Deployment)
- API (VirusTotal, OTX, Threatstream)

Full-Stack Development:

- JavaScript (Node, React, Express, jquery)
- MySQL
- Python (Pandas, Django, Scapy)
- MongoDB and Firebase

Networking:

- Palo Alto (EDU-210, User-ID)
- Fortinet
- Cisco
- AWS VPC

Security Assessments:

- Android and IOS Applications
- Web Application
- Vulnerability Scanning (Nessus, Qualys)
- Static Testing (JS, .NET, Java)
- Dynamic Testing (Burp Suite)
- Network Security Monitoring (Bro, Snort, etc.)

Digital Forensics and Incident Response:

- Memory Forensics (Volatility, Rekall)
- Network Forensics (Bro, ELK)
- Disk Forensics (SleuthKit, Plaso)
- Cloud Forensics (AWS, Azure)