Kiel Vaughn

https://www.kielvaughn.com – https://linkedin.com/in/kiel-vaughn

Clinton Township, MI

CISSP/CCSP certified engineer with a SANS-published whitepaper and two discovered CVEs, specializing in safeguarding cloud infrastructure and applications. Expert at integrating security into CI/CD pipelines and scaling enterprise vulnerability and posture management through tools like SonarQube, TruffleHog, Qualys, and Orca Security.

SECURITY RESEARCH AND VULNERABILITY DISCLOSURE

CVE-2021-38602 (Stored XSS - PluXML 5.8.7): Identified a critical vulnerability where unsanitized input in "Headline" fields allowed persistent script execution and administrative session compromise.

CVE-2021-38603 (Stored XSS - PluXML 5.8.7): Discovered a persistent XSS flaw in user profiles that allowed for widespread delivery of malicious payloads to site visitors.

Research Publication: Published SANS Whitepaper: "Is Your Cloud Environment Secure? How Do You Know?"

EXPERIENCE

CREDIT ACCEPTANCE Remote
Senior Application Security Analyst March 2023 – May 2026

- Automated quality checks by integrating SonarQube Cloud into the CI/CD pipeline, improving the overall enterprise code grade from a D to a B within six months.
- Integrated TruffleHog for automated secret detection, successfully identifying and remediating 100% of verified live credentials in production.
- Established the organization's first formal GitHub Security Standard and Application Security Policy, providing a governance framework for all development teams.
- Strengthened Kubernetes security by deploying Falco for runtime threat detection and Trivy for image scanning, providing deep visibility into 100% of production containerized workloads.
- Engineered and scaled a customized application security maturity model, driving security improvements across several development teams.
- Utilized STRIDE threat modeling to analyze core system architecture, identifying and mitigating over 50 high-impact design flaws throughout various phases of development.
- Streamlined multi-account security by deploying Orca Security across 200+ AWS accounts, ensuring continuous monitoring and a 20% increase in alignment with CIS Benchmarks.

CREDIT ACCEPTANCE Remote
Cloud Security Engineer August 2021 – March 2023

- Standardized security controls across AWS, Azure, and OCI for 3,000+ resources, reducing misconfigurations by 30%.
- Created a library of 25+ incident response playbooks, which formalized recovery procedures and significantly reduced response times for cloud-native security events.
- Conducted mandatory security reviews for all cloud-based projects, preventing over 100 misconfigurations and ensuring "Secure-by-Design" principles.
- Served as the lead investigator for cloud security incidents, driving end-to-end remediation and conducting post-mortem analyses to prevent future occurrences.

CREDIT ACCEPTANCE Remote
Application Security Analyst November 2020 - August 2021

- Conducted deep-dive security assessments on 25+ applications, identifying and remediating 50+ high-severity vulnerabilities prior to production release.
- Deployed SAST scanning to 15 development teams by embedding security tools directly into the development workflow, enabling earlier vulnerability detection.
- Developed a streamlined assessment framework, successfully reducing security assessment turnaround time by 20%.

MICHIGAN SCHOOLS AND GOVERNMENT CREDIT UNION Clinton Township, MI
Systems Administrator / Cybersecurity Engineer April 2015 – November 2020

- Deployed Rapid7 InsightVM/IDR across 1,500+ assets, establishing the organization's first enterprise SIEM and vulnerability management programs.
- Maintained banking systems with 99.999% availability through proactive monitoring; orchestrated monthly patching cycles for core production servers with zero unplanned downtime.
- Developed 250+ PowerShell and Bash scripts to automate administration tasks, reducing daily manual overhead by 75% and ensuring 100% consistency across server configurations.
- Architected the recovery strategy for core banking systems and ancillary connections, reducing the Recovery Time Objective (RTO) by 30% and ensuring zero data loss during annual failover testing.

SELECTED PROJECTS AND TRAINING

Security Research Lab: Designed a VMWare-based environment to simulate and mitigate OWASP Top 10 vulnerabilities, API abuse scenarios, and cross-platform privilege escalation.

Advanced Training: Completed specialized curricula in Cloud Penetration Testing (Black Hills), API Security, and Red Team Operations.

EDUCATION

M.S. Information Security Engineering | SANS Technology Institute | 2022
M.S. Information Technology Management | Western Governors University | 2019
B.S. Cybersecurity and Information Assurance | Western Governors University | 2018

CERTIFICATIONS

Featured: CISSP, CCSP, CKA (Kubernetes)

GIAC Offensive: GXPN (Exploit Researcher), GPEN, GCPN (Cloud Penetration Testing)

GIAC Architecture/Operations: GDSA, GCIH, GCIA, GPCS, GSTRT, GCPM, GSEC

Full Portfolio: 15+ additional certifications detailed at kielvaughn.com/certifications

Advisory: Active Member, GIAC Advisory Board

ADDITIONAL TECHNICAL COMPETENCIES

Application Security: SAST/DAST (SonarQube, Burp Suite, ZAP), Threat Modeling (STRIDE), OWASP Top 10, TruffleHog

Cloud & Infrastructure: AWS, Azure, OCI, Kubernetes, Docker, CSPM (Wiz, Orca)

Security Operations: Incident Response, Vulnerability Management (InsightVM, Qualys, Nessus), MITRE ATT&CK

Offensive Security: Metasploit, Nmap, SQLMap, Impacket, Hashcat, Gobuster

Scripting & Admin: PowerShell, Bash, Python, System Hardening (Linux/Windows), Active Directory