CHRIS MEIKLE

Email: cmeik88@me.com
Website: *www.linkedin.com/in/cmeik*

Senior information security professional with 9+ years of experience, including 3+ years managing, developing, and mentoring a team of security engineering professionals. Subject matter expert in vulnerability and threat management. Creative strategist with a proven capability of developing innovative solutions to strengthen security posture, automate operations, and streamline workflows. Well-communicated technical and business leader, continually aligning project goals and metrics with organizational objectives.

EDUCATION

- **Master's Degree, Information Technology Management - M.B.A.**
Western Governors University - October 2023
- Bachelor's Degree, Computer and Information Systems Security - B.S.
Western Governors University - April 2022

CERTIFICATIONS

- CISSP - Certified Information Systems Security Professional, ISC2
- CISM - Certified Information Security Manager, ISACA
- CCSP - Certified Cloud Security Professional, ISC2
- PenTest+ | CySA+ | Security+ | Network+ | A+ | Project+, CompTIA

SKILLS

- Information Security Leadership
- Software Development (Python, SDLC, DevOps)
- Cloud Security Architecture (IaaS, PaaS, SaaS)
- Security Frameworks (ISO, NIST, HITRUST, PCI-DSS, FedRAMP)
- Networking Fundamentals (OSI, TCP/IP)
- Application Security (SAST, DAST, Developer Tools, Burp Suite)
- Computer Security Incident Response
- Cryptography and Public Key Infrastructure
- Presenting and Public Speaking
- Project and Program Management
- Ethical Hacking and Penetration Testing

HONORS & AWARDS

- Excellence Award - Received for submitting an exemplary paper on "Managing Organizations and Leading People"
Western Governors University - October 2022

WORK EXPERIENCE

Manager, Senior Vulnerability and Threat Analyst
Oracle Cerner - February 2021 to Present

- Led a team of engineers managing vulnerability scanning, analysis, and reporting for over 160k systems, both on-premises and in the cloud (AWS/Azure)
- Developed, deployed, and maintained software to automate over 4,000 hours' worth of manual security operations per year
- Designed and implemented a process to centralize and correlate system and vulnerability data, improving incident triage and response times by 30%
- Engineered methods to discover and track critical flaws in the environment ahead of detection signature releases, accelerating the mitigation of emerging threats by up to 50%
- Authored and published 25+ policies, standards, procedures, wikis, and architecture diagrams, spanning numerous security controls and complex tasks, and frequently referenced by over 25,000 employees
- Directed artifact collection and provided attestations of security controls in SOC, PCI-DSS, ISO, and HITRUST audits with a 100% passing rate
- Strategized the imperatives, goals, projects, and deliverables of five direct reports
- Trained and mentored team members to develop information technology and cybersecurity core competencies

System Security Engineer
Oracle Cerner - April 2018 to February 2021

- Architected and built an enterprise vulnerability management suite capable of assessing 160k systems around the globe daily
- Conducted configuration changes, upgrades, and patching for over 200 Windows and Linux systems
- Reported daily on critical flaws in the environment, including Log4Shell, PrintNightmare, PetitPotam, Spring4Shell, and CISA's Known Exploited Vulnerabilities Catalog, contributing to a monthly organization-wide remediation rate of 90%
- Published company-wide security bulletins and briefed senior leadership on emerging threats and vulnerabilities
- Created and managed large data sets (XML, CSV, JSON) containing over 7 million entries utilizing scripting languages and data analytics tools (Python, Excel, SQL)

Cyber Security Analyst
Oracle Cerner - June 2014 to April 2018

- Developed an executable script to collect an investigation package from compromised systems, reducing incident detection time by 70% across the entire SOC team
- Automated steps of phishing email investigations, improving compromised account recovery time by 25%
- Analyzed data from over 10 different security controls, including SIEM, IDS/IPS, endpoint protection, firewall, packet capture, Active Directory, and network logs, to identify and mitigate threats in the environment