ANDREW YODER

avirtualyoder@gmail.com
ayodernm.github.io

SKILLS

Excellent Communication Skills
Network Security
Project Management
Risk Management
System Hardening
Threat Analysis
Threat Intelligence
Vulnerability Management

SOFTWARE

Aqua
ExtraHop
Git
Linux
LogRhythm
Microsoft 365 Defender
Microsoft Power BI
Microsoft Sentinel
Nexpose/InsightVM
PowerShell
Qualys
SQL
Tenable.io/sc/ot
Windows Server / IIS

CERTIFICATIONS

Azure Fundamentals
CISSP
GIAC-GCSA (Cloud Security Automation)

PROFILE

Strategic security leader with experience working in small and large IT organizations. My interest is to lead a cross functional team responsible for information security threats and vulnerabilities.

EXPERIENCE

Manager, Vulnerability Management Engineering, First Republic Bank — 2022-Present

Leader of the first line risk team for threat intelligence and vulnerability management. Accountable for threat & vulnerability management for workstation, server, infrastructure, network, cloud, and application security initiatives. Responsible for analyzing and remediating technology and cyber risk. Determined criteria for prioritization efforts based on risk factors. Developed key performance indicator (KPI), key risk indicator (KRI), and service level agreements (SLA) to measure program effectiveness and drive continual risk reduction efforts. Researched compensating and mitigating controls. Seek and monitor threat intelligence sources to identify evolving threats to the organization. Implemented enterprise vulnerability management solution Tenable.io. Resolved escalated technical issues associated with remediation activities. Operationalized data from Aqua product suite to prioritize findings based on risk factors for containers and custom developed software.

Threat & Vulnerability Lead, Becton Dickinson — 2021-2022

Brief leadership on threats and advances in the cyber threat landscape for all regions of the global organization with 74,000 associates through written and oral briefings. Manage communications, processes, timelines, resources, and remediation progress for enterprise, manufacturing (OT/ICS), and product security areas. Support incident response, threat hunting, and analysis efforts. Conduct research on emerging threats. Develop written analysis of identified risks and their potential impact. Identify gaps in security program and controls with IT architecture and operations teams to reduce risk and improve the organizations security posture. Provide strategic oversight for vulnerability management operations including the prioritization of remediation efforts. Responsible for Attack Surface Management and reducing risk for public facing systems including on premise and cloud infrastructure. Train resources on how to identify and remediate vulnerabilities and build partnerships to integrate risk management into departmental initiatives. Leverage reporting sources including CMDB to support prioritization efforts. Foster relationships with federal government partners.

Lead ECM Architect, Princeton University — 2017-2021

Technical lead for packaged applications. Responsible for security and management of packaged solutions. Modernized integration strategy between

applications by implementing and securing new REST API processes. Develop strategy for migrating applications to public cloud infrastructure. Troubleshoot network and application issues. Business analysis of existing university processes to develop secure technical solutions. Member of project team to implement CMDB, EDR, updated SIEM, NGFW, and network security monitoring platforms. Member of Problem Review Board which reviewed high priority/high impact incidents and provided guidance on resolving complex technical issues.

Systems Analyst 2, University of New Mexico — 2015-2017
Administered a variety of applications and infrastructure including physical servers, virtual server infrastructure, databases, and network appliances. Developed vulnerability management program for student information systems.

Technical Analyst 1, University of New Mexico — 2013-2015
Enterprise client systems analyst. Built hardened images and managed enterprise antivirus deployment. Member of Network Security Advisory board which reviewed network changes to reduce impact on service delivery.

Information Systems Technician, U.S. Probation Office — 2010-2013
Troubleshoot network and workstation issues. Managed Linux file and web servers.

EDUCATION

University of New Mexico - M.S. Information Systems and Assurance, 2017
University of New Mexico - B.B.A. Management of Information Systems, 2014

REFERENCES

References available upon request.