YAMANOORSTANI
Manassas Park,VA |
ynoorstani@gmail.com

CYBERSECURITY | INFORMATION SECURITY | SYSTEM ENGINEERING | CLOUD | ACCESS MANAGEMENT | AWS

Resourceful, highly analytical information security and IT professional with extensive experience identifying system vulnerabilities and security threats within enterprise-level environments. Demonstrated leader with team-oriented interpersonal skills and the ability to interface effectively with a broad range of people and roles, including upper management, IT leaders, and technology vendors. Excellent ability in identifying system vulnerabilities and possible threats, and then apply technical and administrative safeguards to mitigate the probability of potential attacks. Possesses strong knowledge of HIPAA and NIST frameworks.

- **Interim Secret Clearance & Public Trust**
- Strong analytical skills, including collecting, extracting, synthesizing, and summarizing relevant data, perform root cause analysis and implement recommended scalable solutions.
- Proven ability to quickly assess issues and challenges, utilize relevant data and innovative methodologies, and develop solutions in the best interest of long-term gain for the client/customer.
- Proven track record of building deep technical relationships with senior IT executives in large or highly strategic accounts. Experience in managing various stakeholder relationships to get consensus on solution/projects.
- Knowledge of risk assessment procedures, authentication technologies, policy formation, and security attack pathologies.
- Possesses expertise with SCCM, Certificate Management and SSH credentials management, Agile methodologies, Software Security Architecture, Application Security, Threat Modeling, and AWS.

TECHNICAL SKILLS

SSCM, JIRA, SharePoint, Cloud services, Sophos Central, Containers, Docker, Microservices, Serverless, APIs, IaaS, Immutable infrastructure, and micro-segmentation, MS Office (Word, Excel, PowerPoint), Mac OS, Linux Power User,VMWare Configuration, Hardware, Network, OS Troubleshooting, OS Reimaging, OS Hardening, MS Active Directory, MS Office 365, SOX Compliance, Vulnerability Scans, Okta Application integration, SDLC, Tech Writing

CERTIFICATIONS

A+ Certified, CCNA Certified and Cisco IT Essentials certified

PROFESSIONAL EXPERIENCE

SYSTEMS ENGINEER
DEPARTMENT OF TREASURY **2020-PRESENT**

Work closely with the cloud platform team for design and implementation of MS Cloud applications. Coordinate with architects and other system engineers to build migration plans encompassing infrastructure baseline, plans and roadmaps. Install, configure and maintain Active Directory and third-party software utilities for hardware systems within company operational guidelines. Provide Handle system access and maintain user accounts, passwords, data integrity & security. Assist the SOC team with initiating vulnerability scans, applying cyber security industry best practices.

IT Security Consulting

- Giving advice, recommendations, guidance to program management, and insight into the overall management and evaluation of the system security posture, including migration of systems to the cloud, leads to the establishment and management of executive steering committees and requirement management boards.
- Works with business and technical stakeholders to solicit and gather requirements.
- Ensure all solutions exhibit high levels of performance, security, scalability, maintainability, and appropriate reusability and reliability upon deployment.

Risk Management/ Security

- Establishes and maintains a framework to ensure that information security policies, technologies, and processes are aligned with the organization's business regulations.
- Ensures that risk identification, mitigation controls, and analysis are integrated into the application life cycle and change management processes.
- Establishes and implements certification and accreditation procedures for various information systems and platforms.
- Conducts regularly review of Global Security Incidents and reports and updates the same to the internal teams.
- Ensures that the operation, design, and management of information systems are in accordance with the organization's standards.

Identity & Access Management

- Utilizes Okta to integrate Client applications for MFA, SSO, and Provisioning needs. Implements Okta for Group and Role-Based Access Control implementation across Clients IT infrastructure.
- Coordinate and execute proactive Information Security consulting to the business and technology teams covering Infrastructure Security, Resiliency, Data Security, Network Architecture and Design, and User Access Management.
- Oversaw certificate management and SSH credentials management. Participate in the installation, integration, deployment, and support of IAM tools and products. Deliver process improvements utilizing Identity and Access Management platforms.
- Communicates aspects of both the product and the implementation at the technical and functional level appropriate for the solution.

IT ENGINEER

CUSTOM INK **Mar 2019 - May 2020**

Oversaw security of the cloud infrastructure, serving as the main point of contact for investigating and resolving security-related issues. Developed threat and vulnerability management policies and manage SEM (security event management) system. Performed focused risk assessments of existing or new services and technologies to ensure the organization's information assets and customer information.

- Partnered with infrastructure, application development, and business intelligence areas to develop and maintain recovery procedures for key business applications.
- Performed information security risk assessments on all systems and vulnerability assessments and testing of all infrastructure (routers, firewalls, servers) and applications.
- Coordinated security testing procedures to verify the security of systems, networks, and applications and manage the remediation of identified risks.
- Supported all facets of operations to include physical security, product production, communications security, personnel security, software upgrades, etc.

DevOps(Contractor)

ASCO **May 2018- Dec 2018**

- Managed the development for key system-wide customizations within JIRA and analyzed potential impact of new threats and exploits. Communicated risks to the Privacy Security Team
- Identified, troubleshot, and resolved performance issues in Amazon's workspace service and assisted with creating customized dashboards for teams and developed confluence pages.
- Performed hands on technical design, configuration and troubleshooting of the OKTA service. Conducted Evident.io checks to monitor the cloud security posture of our AWS infrastructure.

Associate IT Engineer

APPIAN

- Migrated over 800 laptops from Sophos Enterprise Console to Sophos Central
- Setup Pen-Testing Laptops for our Security Team and Auditors
- Ran full system scans on vulnerable machines using Sophos Central and managed PUA alerts and threat notifications.
- Assisted in the maintenance of Appian's IT network and server infrastructure

IT Support Associate

Chemonics International **Apr 2015- Apr 2016**

- Provided IT support for Chemonics and USAID's Middle East offices
- Supported and collaborated with team members, software vendors and other technical staff on project efforts to achieve implementation plans and timelines.
- Evaluated IT procedures and made appropriate changes as needed to better serve employees and customers

IT Intern

Opower **May 2014- Nov 2014**

- Created an online dashboard maker which tracked Opower's Wi-Fi speed and IT incident responses
- Setup new hire accounts and configured laptops and installed IP phones
- Monitored user information on Active Directory and coordinated with Opower's network team in infrastructure project planning and deployment

EDUCATION

University of Arizona

BS-Cybersecurity

NOVA Community College

AS- Information Technology

AREAS OF EXPERTISE

System Engineering, Cloud Security, Security Architect, Database Security, Source Control, Monitoring Tools, IT Virtualization Methodologies, Ticket System, Database Administration, FedRamp, Threat Intelligence, IT Support, Network Engineering, Intrusion Detection and Prevention, Incident Management, Risk Assessment, AWS, Encryption, IT Project and Program Management, Change & Release Management, Enterprise IT Systems, Technical Recruiting, Training & Development, Strategic Growth & Planning, Data Analytics, Quality Engineering, Quality Assurance, Agile, Scrum, Cybersecurity, Information Security, Requirements Management, DevOps, HIPAA, Risk Management, Security Governance, Security Operations, Incident Response, Technical Research