Robert Nieto

29960 W Monterey Dr.
Buckeye, AZ 85396
robert.nieto1@gmail.com

Professional Summary

- Over 15 years' experience in IT
- Over 5 years' experience in Information Security and Compliance
- Experience with incident response, investigation, handling, engineering and management
- Experience with security practices, design, management and audits
- Skilled with development, implementation and management of security policies and procedures

Educational Summary

- Master of Network Communication Systems, emphasis on security - Keller School of Management
- Bachelor of Computer Information Systems - DeVry University
- **CISSP**
- **GWAPT** (GIAC Web Application Penetration Testing) - SANS Institute
- **GCIH** (GIAC Certified Incident Handler) - SANS Institute
- **GCFE** (GIAC Certified Forensic Examiner) - SANS Institute
- **GCED** (GIAC Certified Enterprise Defender) - SANS Institute
- **GSEC** (GIAC Certified Security Essentials) - SANS Institute

Technical Summary

- **Security:** Privilege Access Management, Risk Analysis and Mitigation, Vulnerability Testing, Disaster Recovery, Forensics, Evidence Collection/Handling, Root Cause Analysis, Perimeter Defense, Defense in Depth, 20 CIS Controls, PCI, ICS, HIPAA, System Hardening, Risk Management, Critical and Analytical Thinking, DDoS mitigation, Government Compliance, Data Loss Prevention (DLP), Web App security and pen testing, API and application vulnerability detection and management
- **Tools:** Nessus, Metasploit, Nmap, Wireshark, Tcpdump, Iptables, Sudo, Tableau Forensic Imager, dc3dd, FTK, FTK Imager, The Sleuth Kit, Caine, Exiftool, Volatility, SSH, MS Visio, MS Project, Veeam Backup
- **Technologies:** LDAP, DNS, DHCP, NTP, SIEM, IDS, LAN, WAN, Routers/Switches, DMZ, Single Sign On (SSO), Web Servers, Application Servers, Web applications and API, Mail Servers, SAN/NAS, Virtualization, Excel, Two Factor Authentication (2FA), OWASP, Voice over IP (VoIP), Data Encryption, Open Source Systems
- **Platforms:** Trend Micro Hosted Email Security, Trend Micro, Symantec Security Suite, Cisco ASA, Palo Alto FW, VMware ESXi/vSphere, Apache/IIS Servers, MS SQL, MySQL, MS Active Directory (AD), MS DNS, Bind DNS, Splunk SIEM, Snort IDS/IPS, Big Brother/Xymon, MS Office 365, Google G Suite, OKTA, FireEye, ExtraHop, F5 WAF, CloudFlare WAF, Azure Cloud, Keyfactore, ZScaler, Noname Security
- **Operating Systems:** Windows Desktop (XP, Vista, 7, 8, 10), Windows Server (2008, 2012, 2016, 2019), Linux (Arch, Debian, Ubuntu, Fedora, RedHat, Kali, SIFT, Helix), Apple (MacOS, iOS), Google (Chrome, Android)
- **Programming/Scripting Languages:** C++, HTML, PHP, JavaScript, MySQL, Python, Bash, PowerShell

Experience

BannerHealth (Healthcare) - Cybersecurity Engineer III - 04/2020 - Present

- Team lead
    - Supported all engineers with managing and deployment of projects
    - Trained and hired new team members to support different projects
    - Represented team in projects and updates to senior leadership
- Web application security

    - Performed **vulnerability assessments and remediation** plans for **web applications** and **APIs** in **Azure** cloud and on-premise using **Tenable, Noname and ServiceNow**
    - Created and implemented vulnerability remediation process and API standards
    - Deployed **WAF/DDoS** policies in **Cloudflare** and **F5 WAF** to applications
- Network Security tools management
    - Architected, deployed and managed network security tools and standards
    - Deployed and designed standards around network firewalls for **Cisco ASA** and **Palo Alto** devices
    - Deployed and managed **Extrahop**, **FireEye**, **Noname** and **Zscaler**
    - Supported PKI infrastructure using **Keyfactor**
    - Supported CIRT and CSOC teams with network intrusion detections and hardening

Arizona Power Authority (State Agency) - IT Manager - 08/2004-04/2020 (15+ years)

- IT Security Manager/Engineer, Web Developer, Project Manager, Network/System Admin

- 2019 - First responder for security breaches and incidents
    - Responsible for the monitoring and triage of security events, having to identify, analyze, contain, eradicate and recover from incidents
    - Collected and analyzed data and evidence using monitoring tools such as **SIEM, IDS/IPS and incident response tools** while collecting data in a **methodological forensic approach**
    - Presented evidence to court ordered cases and investigations to other agencies or investigation teams
- 2017 - Deployed **VPN solution** for organization
    - Created risk and cost analysis. Researched appropriate solutions and implemented the best product for our organization
    - Project was deployed successfully and it allows staff to be more mobile and efficient
    - Increased staff productivity by 15% and availability by 50%
- 2015 - Developed a **disaster recovery (DR) and continuity (DC)** plan
    - Plan included multiple storage devices and sites, being able to recover from natural disasters, malware, ransomware and staff accidental file deletions or alterations
    - Increased backup and continuity posture by 90%
- 2014 - Managed the research, risk/cost analysis and deployment of **next generation firewalls** and **perimeter defense** solutions
    - Firewall was able to perform deep packet inspection and filter traffic based on user and application
    - Deployed **email security and AV solutions** that protected users at the network perimeter and at end points, creating a defense in depth approach
    - Solutions increased security posture and reduced risk by 20%
- 2013 - Architected a full redesign of server operations
    - Used **VMWare virtualization** solution to restructure operation
    - Project greatly increased production and security by providing faster response, server mobility and deployment options
    - Achieve 100% server virtualization
- 2012 - Deployed **SIEM** and **IDS** systems
    - Conducted research and installation of **Splunk and Snort**
    - Gave the organization great visibility into network security and operations
    - Solution increased security analysis, troubleshooting and incidents by 70%
- 2012 - 2019 **Coached and trained** staff, customers and executives in current cyber security threats, defense tools and procedures
    - Training included internet safety, basic security procedures and current threats and attacks

Associations

- Arizona InfraGard (FBI/InfraGard)
- Sonoran Desert Security Users Group (SDSUG)