IT Security Engineer - CONSULTANT IT Security Engineer - CONSULTANT IT Security Engineer - IT Security Analyst - Information Security - Information Technology Grove City, OH   15 years' experience in Information Technology.   Group Policy Management / Automated Application Deployment   6 years' experience in Information Security   Network Access, Resource And Permissions Management   3 years' experience Incident Response   Active Directory Management   Built Information Security paradigm BEFORE certifications   Information Security Training Sessions For Users   Certified Master Instructor (MS Office)   Identify Vulnerabilities And Potential Indicators Of Attack   Project Management And Budgeting   Threat Mitigation / Defense Strategies And Techniques   Infrastructure Support / IT Support / Help Desk   Antivirus & Antimalware Architecture   Information Security Best Practices   OS Hardening / Firewall Hardening / Desktop Hardening / Web   Computer Networking, System Security   PowerBroker Desktops / MSBSA   Vulnerability Analysis, Assessment And Identification   Intrusion Detection Monitoring And Alerting / Spiceworks / Nmap   Project, Human, and Resource Management   Firewall And Network Traffic Log Monitoring And Management   Vendor Relationship Management / Communication Skills   IT Security Policies And Procedures - Development And   Backup / Disaster Recovery Best Practices Implementation   Network And Systems Administration / Security Management   Retina CS Vulnerability Scanner / Qualys (via Web) / Tripwire Work Experience IT Security Engineer - CONSULTANT NTT Data, Inc - Powell, OH April 2018 to August 2018   Project Management - Execute Successful Deployment Of Sophos AV Across Heterogeneous Environments (Windows Server, Linux Server)   Highlights Assemble Project Team - Information Security Peers, Network Infrastructure, Expert Sophos AV Representative   Develop A Plan Of Action For Successful Deployment   Leverage Talents Of Pertinent Internal Resources   Maintain Constant Progressive Communication And Reporting With Expert Sophos AV Representative (Peter S.)   Coordinate And Guide The Project From Ohio While Peter S. Does The Same From Massachusetts   Implement Mitigation Efforts To Prevent Resource Utilization Spikes Discovered On Previous Deployments   Implement Strategy Along With Peter S. To Assure Smooth Successful Deployment Without ANY Adverse Impact   Build SVMs (Protect WIN Servers - 2000+), Build Cache Servers (Protect Linux Severs - 2000+)   Sophos Anti-Virus,

Salesforce, OKTA (SSO - POC)   Implement and supports information risk management initiatives throughout company   Works with vendors, outside partners, customers and other third parties to address information risk and security-related issues. IT Security Analyst II Battelle - Columbus, OH June 2015 to November 2017 Location: Columbus, OH   Incident Response / Incident Response Plans and Revisions / Governance & Compliance / Remediation / Threat IOC Research   Identify Indicators of Compromise (IOCs) and integrate those into sensors and SIEMs (Splunk , FireEye, Carbon Black, Palo Alto, ThreatGrid)   Conduct investigations of reported information security events and incidents (Splunk , FireEye, Carbon Black, Palo Alto, ThreatGrid)   Conduct data captures from suspect systems within the corporate network (FireEye, Palo Alto, Snipping Tool) Analyze data provided from other departments in order to determine the severity of the event and make a determination if an incident has occurred (PEAR, CB, UrlQuery, Robtex, VirusTotal, ThreatGrid, FireEye, SAS, AdwCleaner)   Coordinate investigations among the information security, information technology, and other support and research organizations.   Perform specialized analysis to support routine business functions and project/task activities (PEAR, CB, UrlQuery, Robtex, VirusTotal)   Perform security monitoring, testing and oversight activities (PEAR, Splunk, Palo Alto, McAfee ePO)   First line of defense in the detection and remediation of security violations and cyber threats (Splunk, CB, JRT, Rkill, RogueKiller, SAS, Securi, MB)   Collaborate with security and technical teams to implement, maintain, and communicate security policies and controls. Triage alerts to identify malicious actors on customer networks / Prioritize assigned tasks and projects based upon directives.   Monitor and assess security industry trends and assist various IT and cyber security teams to identify emerging threats and technologies. IT Security Analyst - CONSULTANT Battelle - Columbus, OH March 2015 to June 2015 Client: Battelle Location: Columbus, OH   Conduct investigations of reported information security events and incidents. Conduct data captures from suspect systems within the corporate network.   Analyze data provided from other departments in order to determine the severity of the event and make a determination if an incident has occurred.   Coordinate investigations among the information security, information technology, and other support and research organizations.   Perform specialized analysis to support

routine business functions and project/task activities.   Multi-Task / Task Prioritization   Quick Utilization Of Multiple Systems   Proactive Incident Triage & Response   FireEye - WebMPS 7000, MAS 4310 , HX 4000, MIR   Nitro / McAfee Enterprise Security , ePO   ServiceNow IT Specialist II Delaware County Health District - Delaware, OH April 2006 to March 2015   NEW Migration of local host email to Google Apps Enterprise - Complete with Postini (Email Spam Filter) and Web Office Apps (i.e. MS Office)   NEW Help Desk Software (Spiceworks), Wireless Internet Access And Vulnerability Scanning Projects - Developed, Managed, Implemented   Developed Information Security Paradigm From The Ground Up (Network Assessment / Checklists / Info Sec Policies, Procedures, Training)   NEW (PBX To) VOIP Phones Project (Shoretel) AND MalwareBytes Console Project - Developed, Managed, Implemented, Maintained   Vendor Relationship Management   Use of Group Policy to strengthen security of Domain and Domain Workstations (Group Policy Management)   Project, Human and Resource Management, Coordination, Implementation, and After Action Analysis   Develop and execute schedules for testing & agency wide installation of software   Review and evaluate systems and systems documentation , test results and security impact on network infrastructure   Work with agency managers & supervisors to provide hardware, software & other needed technical resources   Security advisor to managers on all workplace matters of software, hardware and network   Develop hardware & software requests & project proposals   Research, evaluate, document , recommend software, applications, utilities, hardware, peripherals, tablets, mobile devices for possible   implementation within current infrastructure   Develop agency wide information security policies and network user policies (adopted and implemented)   Develop agency wide information security awareness training (annual presentation) complete with QUIZ   Engage weekly vulnerability assessment scans, reporting and remediation   Engage weekly intrusion detection scans, reporting and remediation   Engage daily network inventory, health, and bandwidth scans, reporting and remediation   Engage daily aggregation of Security Information Event Management software for prioritized reporting and remediation   Contemplate potential threats, known and unknown, and strategize threat defense paradigms   Project management - manage multiple projects simultaneously and manage multiple

vendors simultaneously   Develop disaster recovery policies, procedures and standards.   Develop and execute disaster recovery exercises, analyze results and improve relevant policies, standards and procedures   Develop and execute vulnerability and hacking exercises, analyze results and improve relevant policies, standards and procedures   Develop and execute exercises of intrusions and security compromises caused by users, analyze results and improve procedures   Research, document, execute and revise best practices of intrusion detection, network administration, active directory management   Assist in providing technical security advice in decision making processes   Secure network infrastructure from advanced persistent threats (APT), most notably CryptoLocker and its variants, as well as potential zero-day threats.   Consult with fiscal director on special projects (VPN, Security Enhancements, Document Digitization, etc.)   Submission of Security Bulletins / Emails / HealthENews Articles educating users on security and proactive workplace computer protection.   Majority Contributor to HealthENews MIS Articles. Serve as Information Security Specialist / Information Security Advisor   Implement wireless internet backup failover protection should primary internet access fail.   Spiceworks - Help Desk / Hardware Inventory / Software Inventory / Network Scanning / Intrusion Detection   Membership in various SpiceCorps Groups (OH, IN, TX) and related forums (Networking/ Security / Best Practices / Remote Access / MS   Windows/MS   Office /   Windows   Server   2008,   2012   R2,   Server   2010 / Spiceworks/MalwareBytes/VMware   Fiscal Budgeting Via AccuFund - Spreadsheets: Importing and Formula Validation, Generate Reports   Note - Much automation exists via my custom reports users can execute without assistance. Total Infrastructure Computer Replacement Project (NEW Policy Inspiration - Developed, Adopted, And Implemented)   Manage the project from its inception, purchased the necessary hardware (computer workstation package including mouse, keyboard and speakers, and widescreen monitor), enlisted vendor services to assist with installing new computers throughout infrastructure , used a staggered method of transition, one unit at a time, providing advanced 3 day notice with instructions taped on the monitor on what the user can successfully complete prior to new workstation replacement. Developed (and proposed) NEW asset identification model. ALSO, skills to repair computers, laptops, printers, install/configure software, MS Office ,

Anti-virus, Anti-malware installs, maintain wireless network.   The Architect   Adaptability Consulting Results Orientation Business Process Knowledge Analytical Thinking   Decisiveness Strategic Thinking Knowledge of Emerging Technology Building Relationships   Change Advocate Business Enterprise Knowledge Information Systems Knowledge Developing Others   Strategic Technology Planning Group Session Model Continue Until Successful Lead, Mentor, Guide Instructor, Applied Business & Computer Applications Southwestern College of Business - Dayton, OH April 2001 to July 2005 Dayton, OH Apr 2001 - July 2005   Instructor, Applied Business & Computer Applications   Develop new training and certification methodologies and new curriculum development.   Operate, update, maintain and manage computer labs.   Provide classroom instruction, grading, exams assessment, and motivation to 50 students (minimum) per quarter. Analyzed, reviewed and implemented various textbooks for professional review and curriculum development. Education M.S. in Information Security Western Governors University - Salt Lake, UT May 2017 Master in Information Security Western Governors Univ - Salt Lake City, UT May 2017 Info. Technology South University - Savannah, GA December 2013 B.S. in Information Technology Security South University - Savannah, GA March 1997 Wilberforce University - Wilberforce, OH August 1985 to May 1989 Skills Information Security (6 years), It Security (6 years), Certified Ethical Hacker (4 years), CEH (4 years), CompTIA CSA+ (3 years), CompTIA CySA+ (3 years), CompTIA Certified Security Analyst (3 years), Cyber Security, Siem, Nist, Information Assurance Links http://www.beyond.com/Terrell-Bowden

Name: Nicholas Grimes

Email: michaelconrad@example.com

Phone: 8997728293