Over the past16 years, up to December 2016 I held different positions in the banking industry for Huntington Bank. Since than I worked as a Consultant in a Government Environment as an IT Security Specialist for 9 months. I learned that technology is always changing which presents new unique challenges every day to protect the Confidentiality, Integrity and Availability of data.

One of my positions I held at Huntington was in the Information Security Engineering department, I worked as an IT Security Analyst as well as the System Engineer and Administrator for Symantec Control Compliance Suite. Also, administrator for Qualys , and set up Compliance Policy controls for over 46,000 host assets in all of the OS platforms and IIS. This lead to implementing standardized intrusion prevention, vulnerability management, reducing the risk from $12M down to $4M.

One of my favorite parts of working in IT is the people aspect. Whether it is, teaching people how to use a complex software, or being the leader or part of a support team, I have received numerous Recognition awards and 43 Certificates of Appreciation for providing the best service to clients.

I enjoy and look forward to new working opportunities and building new relationships.

| **DEGREE** | **AREA OF STUDY** | **SCHOOL/COLLEGE/UNIVERSITY** | **LOCATION** |
| --- | --- | --- | --- |
| Master | Network & Communication Management/IT Security | Keller Graduate School / DeVry University | USA |
| **CERTIFICATION AND TRAINING** | | | |
| * **IT Security Certificate** * **Qualys Certification** * **CJIS Level 4 Security Training Certification** * **F5 Application Security Manager (ASM) – Certificate** * **Splunk** * **Aspect Security- Security Application Development** * **Symantec Control Compliance Suite** | | | |

|  |  |  |
| --- | --- | --- |
| Skill | Years Used | Last Used |
| Total years IT experience. | 21 | 2017 |
| IT Security experience | 11 | 2017 |
| Hands-on SIEM experience, and IPS (QRadar, McAfee, Splunk). | 5 | 2017 |
| Hands -on experience with Web and Email Filtering and Security (IronPort). | 5 | 2017 |
| Hands -on experience with Web Application Firewall/Database Activity Monitoring with (Imperva). | 1 | 2017 |
| Hands - on endpoint protection experience (EPO McAfee). | 7 | 2017 |
| Hands - on Vulnerability Management and Policy Compliance and Mapping network experience (Qualys). | 7 | 2017 |
| Hands-on static and dynamic application security scanning experience (AppScan). | 1 | 2017 |
| HIPS McAfee Enterprise solutions (EPO McAfee). | 6 | 2017 |
| Work with Active Directory | 7 | 2017 |
| Experience with the full range of system administration and networking tools including DHCP, DNS, Wireshark, Putty, etc. | 8 | 2017 |
| Collect, analyze big data (Splunk). | 7 | 2017 |
| Host-based Intrusion Prevention System ( IDS/IPS McAfee, QRadar) | 7 | 2017 |
| Proven contribution to continuous process improvements to increase efficiency in IT projects. | 15 | 2017 |
| Excellent communication skills both written and oral. | 20 | 2017 |
| Writing comprehensive requirement documentation showing restrictions or constraints and development for IT Security tools. | 7 | 2017 |
| Patch management, software distribution, operating system deployment, network access protection and hardware and software inventory ( SCCM) | 1 | 2017 |
| Permission management and auditing (Symmetric Control Compliance Suite (CCS), and Datadvantage. | 7 | 2017 |

**Employment History:**

**DevCare Solutions/State of Ohio Department of Public Safety, January 2017 – October 2017, Columbus, Ohio Area**

**IT Security Specialist 2/Consultant**

**Responsibilities:**

* I worked as the Qualys Unit Manager, and discovered and investigated a critical vulnerability within a Qualys scan that was found on an asset four months prior, which turned out to be a false positive.
* Setup procedures for investigating vulnerabilities daily with Qualys scans, and how to put in tickets for different IT groups to remediate found vulnerabilities. This reduced 5 vulnerabilities in the network from 75% to 30%.
* Setup weekly Qualys Map scans to discover all assets in the network, and created documentation and statistic reports for executives to show the status of vulnerabilities within the network.
* Restructured Cisco Ironport access policies so users can be put in different exemption policies that will allow access to different web sites pertaining to their job titles. Also, upgraded the appliances to the latest WSA and ESA AsyncOS as they became available on a by monthly basis.
* Monitor and investigated Cyber Security incidents using EPO McAfee, Qradar, Splunk, Ironport, Imperva and Qualys. Had some PC’s taken off the network
* Created Splunk IT Security dashboard, Data Models and pivot tables for easier search function. Set up alerts for Security Operation Group to help monitor network, firewalls, applications and users.
* Confirmed daily that SCCM permission and auditing patch management software upgrade deployments were being deployed for all operating systems to fix security issues. If they were not implement on the different systems, I put in a ticket for the department in charge of the system to do the patching.
* Ran static and dynamic Web application security AppScan scans for all the new web applications before and after recommendations were given before they go to production. I would generate reports and then meet with the development teams to go over identify security vulnerabilities, and give recommendations on how to fix the vulnerabilities.
* Documented IT Security procedures, and set up OneNote with all procedures and steps for handling security issues, for the tools that were used. Worked on setting up metrics for Executive Reports.

**Huntington National Bank, October 2013 – December 31st 2016, Columbus, Ohio Area**

**IT Security Analyst**

**Responsibilities:**

* Ran Qualys VM and PC scans, helped to decrease threat risks on our company’s official score cards from “medium” to “low” status, developed and implemented security controls, standards, and guidelines for policy compliance. Along with implementing standardized intrusion prevention, vulnerability management, for over 46,000 host assets reducing the risk from $12M down to $4M.
* Integrated vulnerability management SQL queries with the CMDB to create reports that showed the direct flow of ownership for the vulnerabilities to the respectful owners. Created SQL queries from CCS imported data, which allowed the data to be parsed into readable reports.
* Provided technical guidance to the security operations center and or the lines of businesses during investigating a cyber-attack. Using Splunk log management security data platform, set up alerts which helped SOC team rapidly identify, prioritize, and respond to various security events, compliance violations, policy braches, cyber security attacks, and insider threats.
* Restructured the Symantec Control Compliance Suite as the System Engineer and Administrator, to scan both Windows and UNIX servers, did all the updates, troubleshooting and validations for the system.
* Worked closely with Risk and Audit departments, delivering Risk assessment intelligence-driven reports. Assisted in helping Risk in creating ISO 270001 controls. Ran reports to make sure that the different business departments were using Segregation of duties for setting up employees.
* Administrator for Qualys Vulnerability Management and Scanning infrastructure and processes. Performed internal and external vulnerability scanning with Qualys, than sent vulnerability reports to business departments and management. Set up and ran the Policy compliance scans, based on the CIS Security Bendmarks for Window, Unix servers and IIS.
* Maintained, support and diagnose Intrusion Detection/Protection solutions. Troubleshooting IDS/IPS hardware and software issues Produce and distribute weekly reports to identify the state of the environment Configure and maintain IDS/IPS policies and signature management
* Evaluated and implemented through QA Testing as Administrator for a new application that technology would be used for auditing, analyzing and reporting across the enterprise. This application was put into production to replace another application that saved the bank a little over $200,000.
* Performed Security event monitoring of heterogeneous network architecture solutions using McAfee Enterprise Security Manager, McAfee Security Suite of Products such as McAfee Endpoint Encryption, McAfee EPO Management, McAfee Antivirus and Anti-Malware.

**Huntington National Bank,** **October 2012 – October 2013** **Columbus, Ohio Area**

**Enterprise Fraud Specialist 2**

**Responsibilities:**

* Monitored custom snort signature alerts for Cyber security attacks in McAfee Network Security Manager. Rapidly identify and respond to the various cyber security attacks, using WireShark network protocol analyzer and Splunk to get more detail that helped the investigation of the attack, which stopped thousands of attacks before money was lost.
* Investigated fraud detection and stopped fraud transactions using multiple channels of electronic money movement including, but not limited to using FiServe/Cashedge for bank-to-bank transfers, Bill Pay, ACH, and wire transfers.
* Worked with MTS (ACI Money Transfer System) to investigate and stopped suspected fraudulent domestic and international wires from being sent.
* Used Actimize and Early Warning System to investigate Fraud and Cybercrime to properly discern between fraudulent and valid activity, reacting to potential fraud losses. Saved the Bank and their retail (business/consumer) online organizations well over $1,000,000.

**Huntington National Bank, September 2007 – September 2011 Youngstown, Ohio Area -- September 2011 – October 2012 (1 year and 1 month) Columbus, Ohio Area**

**Technical Business Analyst**

**Responsibilities:**

* Worked as the liaison between IT and the Corporate /or Business Banking customers, with documenting process improvements. Created training manuals and did training for Treasury Management products and services. I have received numerous Recognition awards and 43 Certificates of Appreciation for providing the best service to clients.
* Evaluated and implemented in QA, the Remote Deposit System. I engineered the process for companies to deposit their checks into their bank accounts as while as their accounting software and other back office systems. This lead to the automated processing and posting of payments in a single pass – i.e. straight through processing.

**Sky Bank,**

**January 2000 – September 2007 New Castle, Pa. - Level 2 Technical Support Help Desk**

**July 2000 – January 2002 (2 years and 6 months) Canfield, Ohio - Customer Service Representative**

--------------------------------------------------  
**Education**

# DeVry University - Keller Graduate School – (Graduated with Distinction)

# Master’s Degree: Network & Communication Management/IT Security Certificate

# 

# Youngstown State University, Ohio – (Graduated Magna Cum Laude)

# Bachelor’s Degree: Fine Arts (Photography) Minor: Computer Science

# 

# Training

# Qualys Certified Specialist Certification

# Criminal justice Information System Level 4 Security Training – Certification

# F5 Application Security Manager (ASM) – Certificate

# Splunk

# Aspect Security- Secure Application Development

# Symantec Control Compliance Suite

**Professional Affiliations**

Splunk - User Group Columbus / Pelotonia Photographer / Association of Certified Fraud

ISACA / InfraGuard Central Ohio