**Byron Hayes**

•1822 Plymouth Ct. Bowie MD• (240) 424-7051• byhay1@terpmail.umd.edu

**Objective:** A cybersecurity professional looking to use educational knowledge and industry experience to assist clients with identifying, quantifying, and mitigating risks to organizational data & assets.

**Skills:**

|  |  |
| --- | --- |
| **Adept Computer Skills** | •InDesign •Illustrator •Visio •Nmap •Cain and Abel •Orphack •Snort •Metasploit •Forensic Toolkit (FTK 6.1) •Symantec Endpoint Encryption |
| **Advance Computer Skills** | •CSAM •RMPS •DreamWeaver •Microsoft Office (Excel , Word, PowerPoint) •Computer Architecture •Audacity •SharePoint •WireShark •Nessus •Tanium •Splunk •Nexpose |
| **Programming/Scripting** | •HTML •C++ •CSS •SQL •VBA •Solidity •PowerShell •Python •RegEx/rex(Regular Expressions) |

**Education:**

Graduated University of Maryland University College Cyber Security Tech., MS

Grad Spring 2018

Graduated University of Maryland – College Park, College Park, MD Studio/Graphic Art, BA

Grad Fall 2012

June 2010- West Liberty University, Wheeling, West Virginia Business, Junior

July 2010 Business Plan Competition,

September 2008- Morgan State University, Baltimore, MD Electrical Engineering, Sophomore

May 2010 Partial Academic Scholarship

**Certifications:**

Security + CE, SYO-401

Amazon AWS Solutions Architect, SAA-C01

Certified Bitcoin Professional, CBP

ITIL v4 Foundations

**Clearances:**

Active Secret Clearance supporting Department of State

Public Trust supporting the Department of Commerce

Public Trust supporting the Department of Transportation

­**Training/Bootcamps:**

2018 Ethereum Developer Bootcamp – Flatiron School/DApperNetwork

2019 WorkShop Plus – Microsoft PowerShell – Foundation Skills

**Organizations:**

2010 -2011Society of Satellite Professional International (SSPI)

2009-2010 National Society of Black Engineers

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Experience/Leadership:**

January 2019 – Present

**General Dynamics/ Client: Department of State**

**Senior Security Engineer/Blue Team**

* Identify zero-day vulnerabilities by means of research or soft pen-testing (testing, scanning, fuzzing). Also, identify solutions to help mitigate vulnerabilities and rank them based on other vulnerabilities found on the network in order to prioritize mitigation.
* Conducted ad-hoc and enterprise assessments on software, hardware, and systems at any time during the Risk Management Framework (RMF) process to discover more vulnerabilities and mitigations. Blue Team assessments on Microsoft Azure, Microsoft Intune, VMware AirWatch, mobile threat defense (MTD) solutions, End-of-Life services/software, depreciated/legacy protocols.
* Develop queries in Splunk and Tanium to assist in creating dashboards/boards/trends to get a better understanding of network health in real-time.

July 2018 – January 2019

**Diligent eSecurity/ Client: USAID OIG**

**Information System Security Officer**

* Created Technical Architecture Document (TAD), including the network topology diagram, interconnections, dataflow, and security for BlackBerry Unified Endpoint Manager (UEM) Mobile Device Management (MDM) solution.
* Lead coordination of table-top and functional exercises in support of contingency plans. The two-day exercise included a brief of the newly updated contingency plan and four scenarios with engagement from the systems stakeholders.
* Created, reviewed and updated all OIG security policy documentation (configuration management, auditing, access management, etc.)
* Developed dynamic web querying excel sheet used to pull Tenable Nessus Solutions directly from the internet. This modified sheet allowed for anyone working on system findings the ability to search a Nessus plugin if given an excel export of the scan. Only employee at OIG to take on complex VBA excel tasks to support mission.

January 2017 – July 2018

**Deloitte/ Client: U.S. Census Bureau**

**Security Engineer**

* Lead security engineer for various components, led meetings, and reviewed and approved configuration baselines. Also, adhered to the Risk Management Framework (RMF) process in accordance to NIST 800-37 rev 1.
* Uses the Risk Management Program System (RMPS) to help tailor controls for Census systems
  + Used previous assessment knowledge to further tailor controls to fit the system
  + Wrote implementation statements to prep SSP for ISSO
* Engineering four (4) major systems with over 30 components that needed separate SSPs and ATOs
* Work with the development teams during their SDLC process and recommended ways to harden the systems before they went to production.
* Create implementation descriptions for NIST 800-53 controls in order, per component, to insure accurate description of control implementation within the component.
* Write findings and recommendations for improvements and Present to CIO, CISO and Federal Leads for Pre-Assessment and Authorization to Operate (ATO).
* Created risk profiles in accordance to OMB A-123 and assessed in accordance to OMB A-123 and NIST.
* Helped secure the following components:
  + Hortonworks (most sub-components including Kafka, HDFS, Ambari, etc.)
  + Oracle (Weblogic, 12c, etc.)
  + Various web applications and their components (OAuth, Applets, Servlets-Apache Tomcat, Custom Review, etc.)
* Helped Deloitte Tiger Team with reviewing, updating, and analyzing NIST 800-53 rev 5 for the National Institute of Standards and Technology. (Knowledge of new controls sets Individual Participation-IP and Privacy Authorization)
* Help with the Trusted Internet Connection (TIC) AWS architecture solution for the Census Bureau in support of the 2020 Decennial.

October 2015 – December 2016

**Business Integra - FAA at Department of Transportation**

**Technical Support III/ Assessor Support**

* Uses SharePoint as a tool to help streamline business operations at Business Integra. Also, recommends simple updates on SharePoint that can improve contractor and client cooperation when assessing multiple FAA systems.
* Simple macro creation is used with the SSP workbook in order to calculate the FIPS 200 risk level and other repetitive tasks as each given assessment team will go through at least 12 assessments a year.
* Working with, and learning NIST SP 800.53 revision 4, NIST SP 800.37, DOT Compendium in order to assist

Assessors with their assessment package.

* Help with all aspects of the security assessment package in order to properly recommend remediation for system vulnerabilities that include:
  + System Security Plan (SSP), Plan of Action and Milestones (POA&M), Security Characterization Document (SCD), Security Assessment Report (SAR)
  + Data management and the innate ability to help manage the data of multiple systems at once.

February 2014 – October 2015

**EmeSec, Inc. & FMCSA at Department of Transportation**

**Junior Security Analyst / Project Coordinator**

* Worked directly with the ISSO and the SharePoint Administrator of FMCSA and used SDLC Agile development techniques in order to create a SharePoint site to better organize completed assessments, scans, and artifacts between contractor and the government.
* Working with, and learning NIST SP 800.53 revision 4 and NIST SP 800.37 in order to assist assessors with their assessment package.
  + Helped populate and assist with the System Security Plan (SSP) and System Assessment Report (SAR).
  + Speak to System Owners (SO) in order to close open Plan of Action Milestones (POAM)
  + Quality assurance for every deliverable.
  + Obtain Baseline, WebInspect, OS, and Database scans for the assessment.
* Assist Project Manager with scheduling (due dates, meeting dates/times) and all organizational efforts.
* Handle all graphical components of the package (presentations, charts, graphs, new templates, etc.)
* Input Plan of Action & Milestones (POA&M) into CSAM and manage all CSAM related activity**.** Created a separate workbook for extracted POAMs with macro buttons that would adjust the data in a format that the client provided.