**Michael Venturella**

Personal Email: michael.venturella@outlook.com

Website: <https://www.michaelventurella.com/>

LinkedIn: [https://www.linkedin.com/in/michael-venturella-189102195/](https://www.linkedin.com/in/michael-venturella-189102195/%20)

**Publications**

<https://cybersecurity.att.com/blogs/security-essentials/business-email-compromise-bec-tracking-a-threat-actors-funny-business>

<https://cybersecurity.att.com/blogs/security-essentials/stories-from-the-soc-something-smells-phishy>

**EDUCATION**

Bachelor’s Information Technology Western Governors University

Masters in Cybersecurity & Information Assurance Western Governors University

**CERTIFICATIONS**

* CompTIA CASP+
* CompTIA Pentest+
* CompTIA CySA+
* CompTIA Security+
* CompTIA Network+
* CompTIA Project+
* Cisco CCNA
* CompTIA A+
* ITIL Foundations
* Microsoft Certified: Security, Compliance, and Identity Fundamentals (SC-900)
* Microsoft365: Fundamentals (MS-900)
* AlienVault Security Engineer (AVSE)
* AWS Cloud Practitioner

**Projects**

**Project:** Automated Asset Discovery Script

* Developed bash/Python scripts leveraging Nmap and Linux command-line tools for network asset discovery, facilitating early identification of new devices for security design reviews and vulnerability assessments.

**Project**: Building AD Domain with Integrated SIEM for Log Ingestion

* Engineered and deployed an Active Directory domain from the ground up, integrating workstations and users, and implemented a SIEM solution (Wazuh) for comprehensive event collection from Domain Controllers and Workstations.

**Project**: Vulnerability Management

* Utilized the Nessus Vulnerability Scanner within a dedicated home lab environment to detect and evaluate vulnerabilities in an unpatched Windows OS, driving security mitigations and hardening efforts.

**Project**: Coded Personal Website using AWS services and HTML, CSS, and JavaScript

* Developed and maintained a robust personal website utilizing HTML, CSS, and JavaScript, hosted on AWS. This project not only demonstrated my technical prowess in web development but also showcased my ability to integrate and manage cloud-based hosting solutions, further emphasizing my versatile skill set in both cybersecurity and software development.

**EXPERIENCE**

**Company: AT&T Cybersecurity**

**Title: Senior SOC (Security Operation Center) Analyst 4/1/2022-Present**

* Triage customer alarms from the SIEM. Customer industries include (FinTech, Health, Education, Government, Infrastructure, Retail)
* Contextualizing and prioritizing findings for threats customers face via custom investigations to piece together cohesive incident timeline
* Pioneered the use of external tools for Open-Source Intelligence (OSINT) and Cyber Threat Intelligence (CTI) to analyze and mitigate suspicious activities.
* Developed and refined custom dashboards, reports, and automated suppression rules in SIEM.
* Using OSQuery language, built custom alarm rules to detect anomalies and/or threats
* Applied the MITRE ATT&CK framework to perform identify on threat actor tactics, techniques, and procedures (TTPs)
* Securing cloud environments for customers (AWS, Azure, GCP)
* Providing recommendations to customers to eradicate threats using the EDR platform Sentinel One response actions
* Apart of the threat research team that gives presentations to other members of the current threats in cyber space.

**Company: Daytona State College**

**Title: Lead Cyber Security Analyst 8/1/2021-4/1/2022**

Under supervision of CISO, performed tasks such as:

* Led the monitoring of Microsoft Cloud App Security to proactively detect compromised accounts and suspicious activities.
* Generated detailed vulnerability assessments using Rapid7, playing a pivotal role in the security testing processes.
* Ensured strict adherence to the Center for Internet Security (CIS) controls, continuously evaluating and fortifying security policies. My leadership in this area led to the implementation of cutting-edge security standards throughout the organization, significantly reducing security risks.
* Utilized LogRhythm SIEM for effective log monitoring, demonstrating my ability to participate in threat model reviews and enhancing the organization's resilience to attacks through meticulous security analysis.
* Performed critical account management and security operations using Microsoft Active Directory, ensuring secure user access and effective response plans that minimized organizational exposure to potential security breaches.
* Authored innovative Nmap scripts using Linux BASH to uncover and secure new network assets, reflecting my proactive approach in identifying and neutralizing potential vulnerabilities before exploitation.
* Applied industry-leading practices in managing Azure cloud environments, including meticulous management of user and application access, Resource Groups, and Key Vault. My contributions have been crucial in enhancing the security of Azure-hosted products and services, reinforcing my reputation as an authority in cloud infrastructure security.

**Company: Flagler County Schools 5/1/2021-8/1/2021**

**Title: IT Support Intern**

* Aid in asset tagging and inventory of new MacBook’s for the 2021-2022 school year.
* Image over 2,000 new MacBook’s to the latest OS “bigsur”
* Engage with the local community to help deliver laptops to students.