Taylor Ramble

917-412-8900
taylorramble@outlook.com
Portfolio/Website: github.com/tmramble

Cybersecurity Experience

IT Architect Specialist (Cybersecurity)
Atlanta Public Schools | 2024

- Supported SOC operations by triaging alerts, developing KQL queries in Microsoft Defender for Endpoint (Azure), and enforcing endpoint security best practices to enhance organizational resilience.
- Collaborated on the APS incident response plan, identifying and remediating control gaps and creating playbooks.
- Successfully identified over 600+ IOCs and tuned detection rules to improve Cloud Security at the District.
- Delivered quarterly Disaster and Continuity meetings and revised APS's current plans for Disaster Recovery and Business Continuity.
- Created and maintained district-wide security policies including AI governance for student devices.

Information Technology Experience

IT Architect Specialist (Information Technology)
Atlanta Public Schools | 2024

- Created real-time dashboards in Grafana using PromQL to monitor switches, closets, and surveillance systems via Prometheus.
- Leveraged MOVEit FTP servers to automate Aruba switch firmware updates, reducing manual overhead.
- Successfully followed monitoring process for outages across school locations, devices and instructional technology applications.
- Served as secondary change management lead spearheading weekly meetings and identifying gaps in changes.
- Successfully identified the root cause of multiple layer 2 outages by collaborating with multiple APS teams.

Projects

Project: Geo-Data to Azure Storage with Data Lakes
Source: https://github.com/tmramble/SentinelGeoIP
Platforms and Technology Used: Azure Storage, Azure Sentinel, Log Analytics Workspace (LAW), Azure Portal

Project: Cryptography Lab Report: Exploring Encryption Techniques and Data Security
Source: https://github.com/tmramble/cryptography
Platforms and Technology Used: OpenSSL, Wireshark, Linux Terminal, Apache Web Server

Project: Merged Whisper Security – Network Design & Security Integration
Source: https://github.com/tmramble/ Merged-Whisper-Security-Network-Topology
Platforms and Technology Used: Visio, Excel, Microsoft Defender and Excel, Cisco

Security Initiatives

Initiative: Mitigated Widespread Student Account Compromises through IOC Automation & Policy Fixes

- Automated IOC bulk upload templates, reducing response time for blocking malicious IPs by ~90%.
- Identified root cause: student passwords tied to lunch numbers; escalated to leadership with recommended policy changes.
- Discovered failure in district-wide Conditional Access for non-US IPs, leading to cross-team resolution and improved geo-blocking.

Initiative: Business Continuity & Risk Management Leadership

- Led quarterly Business Continuity and Disaster Recovery meetings; updated district-wide plans to align with evolving cybersecurity policies
- Reviewed and leveraged cybersecurity policies to guide comprehensive third-party risk assessments
- Played a key role in vendor risk mitigation by identifying a major third party's inadequate SOC 2 compliance, preventing potential security exposure.

Initiative: Microsoft Purview Implementation and Compliance Alignment

- Spearheaded the integration of Microsoft Purview in Atlanta Public Schools to protect sensitive student and employee data.
- Created and deployed customized sensitivity labels and Data Loss Prevention (DLP) policies to classify and protect confidential information.
- Delivered comprehensive guides and support for faculty and staff on how to apply sensitivity labels and adhere to DLP policies

Skills and Technologies: Azure. Machine Learning, OSI Model, Senior IT Support, Generative AI, Git, Microsoft Defender XDR, Entra ID. CTI, Linux (Ubuntu), Ansible, Prometheus, Security Controls, Business Continuity and Disaster Recovery, Sentinel Automation, Endpoint Protection, Microsoft Purview

Education

Masters in Machine Learning and Artificial Intelligence West Governers University, Current

Certifications

Azure AI-900 Fundamentals Certification (August 2025) Microsoft
Certified in Cybersecurity (Currently Certified) ISC(2)