DARNELL MAIDEN

Cybersecurity Analyst

CERTIFICATIONS

- **CompTIA Security+ | [Mar. 21, 2026]**
- **Google Cybersecurity Professional Certificate | [Mar. 6, 2026]**

SKILLS

Security Operations (SOC):

- SIEM (Microsoft Sentinel, Wazuh), Log Analysis, Threat Detection, Incident Response, Honeypot Management (T-Pot).

Vulnerability Management

- Nessus, Asset Discovery, Patch Management, Remediation Validation, Risk Assessment.

Cloud & Virtualization:

- Microsoft Azure, AWS, Digital Ocean, VirtualBox, VMware.

Operating Systems:

- Linux (Ubuntu, Kali), Windows Server, Active Directory.

Query Languages & Scripting:

- Kusto Query Language (KQL), Bash, PowerShell, Python, SQL.

Frameworks/Regulations

- NIST CSF, ISO 27001, HIPAA, PCI-DSS, GDPR

Tools/Concepts

- Firewalls (NGFW), VPNs, Network Segmentation, Packet Analysis (Wireshark), Intrusion Detection/Prevention Systems (IDS/IPS).

EDUCATION

High School Diploma

Western Hills University High School

Aug. 2009 - May 2013

Cincinnati, OH

CONTACT INFO

darnellmaiden1535@gmail.com

(321) 250-0580

Decatur, GA 30002

https://www.linkedin.com/in/saintmaiden

http://saintmaiden.site

PROJECTS

Microsoft Sentinel SOC Lab In Microsoft Azure

- **SIEM Configuration:** Deployed a **Microsoft Sentinel** environment in **Azure**, centralizing security logs from cloud-hosted virtual machines into a **Log Analytics** workspace.
- **Threat Detection:** Authored custom **KQL** queries to identify and alert on live RDP brute-force attacks and unauthorized access patterns.
- **Security Visualization:** Engineered a real-time **Sentinel Workbook** map to visualize global attack vectors and transform raw logs into actionable geographic intelligence.

Vulnerability Assessment Lab Using Nessus

- **Vulnerability Scanning:** Conducted credentialed scans using **Nessus** on a Windows VM to identify high-risk misconfigurations and outdated software (CVEs).
- **Remediation & Validation:** Spearheaded end-to-end remediation by deploying security patches and performing follow-up scans to verify a **100% resolution rate**.
- **Risk Reporting:** Translated technical scan results into actionable insights, documenting the impact of potential exploits like unauthorized remote code execution to simulate real-world risk management.

Honeypot Platform Using T-Pot & Digital Ocean

- **Platform Deployment:** Deployed a **T-Pot** honeypot framework on a **Digital Ocean** cloud instance, exposing multiple emulated services (SSH, RDP, HTTP) to capture real-world attack data.
- **Threat Analysis:** Monitored live global traffic to identify and analyze common attack vectors, including brute-force attempts, automated botnets, and malicious payloads.
- **Data Intelligence:** Leveraged built-in **ELK Stack** dashboards to visualize threat actor origins and behavior patterns, translating raw logs into actionable geographic and tactical intelligence.

Password Management System Using AWS & Passbolt

- **Cloud Infrastructure Deployment:** Engineered a scalable, high-availability password management environment by provisioning an **Amazon EC2** instance on **AWS** and configuring strict network security groups for HTTP/HTTPS and SSH access.
- **Cryptographic Security:** Strengthened authentication by using **Kali Linux** to generate custom RSA key pairs, ensuring encrypted communication and secure access to the cloud host.
- **Zero Trust Credential Management:** Implemented **Passbolt** to transition from memory-based habits to a secure credential lifecycle, mitigating risks like credential stuffing and password reuse through end-to-end encryption.

WORK EXPERIENCE

Team Lead/Manager

Donatos Pizza

MAY 2023 - current Avondale Estates, GA

- Managed a team of 10 during peak hours, overseeing time-sensitive workflows to maintain 100% accuracy in procedural compliance with strict Service Level Agreements (SLAs).