YOEL YOEL

Cybersecurity Analyst

Houston, United States

832-374-7213 **yoely282@gmail.com**

PROFILE

Aspiring Cybersecurity Analyst with foundational knowledge in Splunk, Python, and cloud security, along with hands-on experience in incident response, threat detection, and network security. Strong background in Windows and Linux systems, with skills in vulnerability assessment, risk management, and security operations. Leveraging 3+ years in security and quality control, recognized for problem-solving, teamwork, and adaptability in fast-paced environments. Seeking a full-time role or internship to apply and expand my expertise while contributing to an organization's cybersecurity initiatives.

CORE COMPETENCIES

- Vulnerability Assessment and Remediation
- Network Security
- SIEM Data Analysis
- Incident Response and Investigation
- AI-enhanced Incident Response
- Incident Handling
- Encryption Implementation
- Cloud Security
- Azure Network Security
- AWS Cloud Management
- Python & Powershell
- Window and Linux
- Network Design
- Effective Communication
- Teamwork and Cooperation
- NIST CSF, ISO/IEC 27001
- Customer Support
- Continuous Improvement Mindset
- Attention to Detail
- Adaptability to Change

EDUCATION

Texas Southern University
Aug 2021 — May 2025

Bachelor of Science in Management Information System

Houston TX

Allen Community College
Aug 2017 — Jul 2019

Associate In General Studies

Iola, Kansas

Associate in General Studies of Information Network Technology.

EMPLOYMENT HISTORY

Physical Security, UPS
Aug 2023 — Present

Houston TX

- Implemented proactive safety measures to **enhance security** and mitigate hazards. **Monitored** surveillance systems, conducted **regular patrols,** and **responded to incidents and alarms**.
- Enforced **access control procedures**, **verified credentials**, and ensured secure facility entry for staff, guests, and contractors.
- **Educated personnel** on security protocols to **promote emergency** preparedness.

Customer Service Officer, Radkin — Jun 2022 — Aug 2023
Houston TX

- Demonstrated strong organizational, **communication**, and **interpersonal skills** while assisting diverse populations.
- **Provided professional customer** service through phone, email, and in-person interactions. Managed concierge services, including tracking packages, handling administrative tasks, and **maintaining confidentiality.**
- Ensured **customer satisfaction** through follow-ups and **efficient service delivery**.

Quality Control Inspector, Prime Industry Recruiter Inc. — Jan 2020 — Jun 2021
Ada, OK

- **Operated** and maintained molding machinery to **produce high-quality** car parts while ensuring precision and accuracy.
- Conducted quality inspections, adjusted **machine settings**, and utilized **computer systems for data entry** and process tracking.
- **Collaborated with quality teams** to identify defects and resolve production issues. Performed **troubleshooting** and basic maintenance, **adhering to safety protocols** and maintaining a **clean work environment**.

CERTIFICATIONS

CompTIA Security+ — Mar 2025 — Mar 2028

IBM Cybersecurity Analyst Certification — Oct 2023 — Jan 2024
Coursera

- Completed diverse cybersecurity training, including **incident response**, **digital forensics**, penetration testing, threat hunting, and cryptography. Proficient in network security, **operating system administration**, and **compliance frameworks**. Hands-on experience with cybersecurity tools, **threat detection**, and breach response case studies, reinforced by the IBM Cybersecurity Analyst Assessment.

Microsoft Cybersecurity Analyst — Jan 2024 — Jun 2024
Coursera

- Comprehensive cybersecurity training covering networking, **cloud security,** identity management, and compliance frameworks. Hands-on experience with threat detection tools, **Microsoft Defender**, and **Azure AD identity solutions.** Skilled in OS security, endpoint protection, and real-world threat mitigation strategies, including a cybersecurity capstone project.

Google IT Support Certification — Sep 2023 — Apr 2024
Coursera

- Strong foundation in IT security, networking, and system administration with hands-on experience in threat defense, **OS management (Linux & Windows),** and IT infrastructure services. Skilled in **troubleshooting, technical support,** and virtualization, reinforcing cybersecurity and system optimization expertise.

Splunk Search Expert Certification — Apr 2024 — May 2024
Coursera

- Proficient in **searching, navigating**, and analyzing machine data within the **Splunk platform.** Skilled in creating dynamic reports, dashboards, and **data visualizations** to support decision-making. Experienced in transforming raw data into actionable insights for stakeholders.

PROJECTS

Vulnerability Assessment Lab — Nov 2024 — Present

- Set up and configured a **Windows virtual machine (VM)** on VirtualBox, creating a secure and isolated environment for testing and analysis.
- Installed and configured **Nessus vulnerability scanner on the Windows VM,** empowering comprehensive vulnerability assessment and analysis.
- Conducted comprehensive **vulnerability scans** using Nessus, including **credential scans**, to identify and assess potential security risks and weaknesses.

- Identified and **analyzed vulnerabilities in the system** and deliberately installed vulnerable software for testing purposes, simulating real-world scenarios to evaluate security defenses
- Developed and implemented **effective remediation strategies** to address identified vulnerabilities, minimizing potential risks and strengthening system resilience.

Password Management System in AWS — Nov 2024 — Present

- Created Passbolt, a self-**hosted password manager,** enabling secure storage and management of complex passwords for enhanced data protection.
- Utilized **AWS cloud services** to host Passbolt, ensuring scalable, available, and reliable access to the password manager.
- Implemente**d HTTPS encryption to safeguard sensitive** data transmitted to and from the password manager, strengthening the overall security posture
- Configured and maintained the domain hosting for the password manager, ensuring secure and accessible user experience
- Provided functionality within **Passbolt for secure storage** of complex passwords, enhancing data protection and user convenience.

Enterprise Network Design Projects - Cisco Packet Tracer — 2025 — Present

- Designed and implemented multiple enterprise network infrastructures using **Cisco Packet Tracer,** based on real-world case studies.
- Projects included small office/home office setups, hotel and campus networks, bank infrastructure, and a trading floor support center.
- Applied hierarchical models, VLANs, inter-VLAN routing, DHCP, wireless networking, OSPF routing, NAT, port security, and ISP redundancy to build scalable and secure networks tailored to organizational needs

Multi Honeypot Platform — Nov 2024 — Present

- **Deployed T-Pot** on Azure Cloud, bolstering security measures and enabling advanced threat detection and analysis
- Configured **virtual machine** and network infrastructure to support seamless installation and operation of T-Pot, ensuring optimal performance and security.
- **Monitored and analyzed honeypot** data generated by T-Pot, enabling early detection and response to potential cyber threats

SIEM Implementation in Azure Cloud — Nov 2024 — Present

- Successfully deployed **Microsoft Sentinel** a SIEM solution in Azure Cloud, fortifying cloud's cybersecurity capabilities and enabling proactive threat detection and response.
- Implemented advanced techniques and configurations, significantly enhancing the SIEM solution's **threat detection** capabilities and optimizing the identification of potential security risks.
- Enhanced threat detection with custom **KQL analytics rules**, enabling swift incident response to safeguard assets.
- Conducted incident investigations using **SIEM tools and techniques** to analyze cybersecurity incidents.
- Implemented **remediation actions to mitigate** and resolve identified cybersecurity incidents, minimizing the impact on critical assets and preventing recurrence.

AI Enabled Incident Response Automation — Nov 2024 — Present

- **Developed a ChatGPT solution** on the Azure Cloud platform designed to enhance cybersecurity incident management.
- Implemented strict access controls and permissions ensuring a secure environment for handling sensitive incident data and response actions.
- Conducted necessary fine-tuning and optimizations to **maximize AI performance,** ensuring its ability to deliver valuable insights and recommendations.
- **Created an automation within the SIEM system** to seamlessly integrate AI and streamline overall cybersecurity operations.

EXTRA-CURRICULAR TRAININGS

JPMorgan Chase Cybersecurity Job Simulation — Feb 2024 — Apr 2024

Forage — Virtual Intern

- Analyzed large dataset of fraud in financial payment services, resulting in more fraudulent identification.
- Increased security posture of personal website through implementation of fundamental application
- security techniques.
- Built an email classifier to distinguish spam from ham, achieving accuracy rate.
- Designed and developed a system for enhancing the security of sensitive data access
- Provided technical support for investigations into cyber incidents such as data loss prevention.

Wireshark for Beginners: TCP IP Protocol Fundamentals Project — Sep 2024 — Sep 2024

Coursera

- Capture and save packets on a physical wired network using Wireshark.
- Use Wireshark to observe the Internet Level of TCP/IP.
- Use Wireshark to observe the Transport Level of TCP/IP.
- Use Wireshark to observe HTTP Application of TCP/IP protocol.
- Use Wireshark to observe HTTPS Application of TCP/IP protocol.

Vulnerability Scanning with Nmap Project — Jul 2024 — Jul 2024

Coursera — Virtual

Nmap Network Scanning: Executed various Nmap commands in the terminal to perform network scans, identifying potential vulnerabilities to improve network security through hands-on practice

Metasploit for Beginners: Ethical Penetration Testing Project — Aug 2024 — Aug 2024

Coursera — Virtual

- Perform a Vulnerability Scan Analysis to enable effective vulnerability reporting
- Utilize an exploit using Metasploit to gain access to a vulnerable system
- Author comprehensive penetration testing reports with results that will enable a company to fix their vulnerabilities

Encryption with Python Project — Jun 2024 — Jun 2024

Coursera — Virtual

Encrypt data with key pairs: In this Project I Developed skills in Python-based encryption, creating public and private key pairs to encrypt and decrypt files via command-line inputs.

LINKS

- **https://www.linkedin.com/in/yoelyoel/**
- **https://github.com/yoely282**