

JOHN HILTON Cyber Security Professional - CASP+

Dallas, TX

706-987-3839

Johnhilton@gmail.com

[linkedin.com/in/johnhilton1](https://www.linkedin.com/in/johnhilton1)

SUMMARY

Highly motivated and results-oriented Cybersecurity Analyst with two plus years of experience seeking to leverage expertise in threat analysis, vulnerability management, and security controls to transition into an Azure Security Engineer role. Proven ability to identify and mitigate security risks, configure security solutions, and collaborate with IT teams to ensure a secure cloud environment. Eager to learn and apply Azure security best practices to protect data and workloads in the cloud..

EXPERIENCE

Cybersecurity Analyst

Critical Start — Plano, TX

2022 – Present

- Continuously monitored security systems and logs for signs of malicious activity using SIEM and SOAR tools.
- Investigated security incidents, including malware infections, data breaches, and unauthorized access attempts, ensuring swift containment and mitigation.
- Conducted threat hunting using advanced techniques, such as behavioral analysis and threat intelligence, to identify undetected risks.
- Reduced False Positives by implementing updated security policies and refining detection rules, aligning with MITRE ATT&CK framework.
- Delivered actionable insights to management by analyzing security data and providing detailed reports on incidents and risks.

Helpdesk IT Support

DXC Technology — Irving, TX

2020 – 2022

- Participated in deployment projects for hardware and software installations, supporting over 500 users.
- Delivered seamless performance for client systems by implementing efficient troubleshooting processes.

- Installed and configured hardware components, including workstations, printers, and peripheral devices, ensuring operational readiness.

IT Support Specialist

QNET — Dallas, TX

2019 – 2020

- Supported over 500 users by deploying and configuring workstations, printers, and peripherals, ensuring a seamless user experience.
- Enhanced system readiness by ensuring 100% operational uptime during deployments of new hardware and software.
- Reduced troubleshooting times by developing streamlined processes for diagnosing and resolving system issues.

Infantry Non-Commissioned Officer

U.S. Army — Various Locations

2006 – 2014

- Ensured operational security for over 650 personnel during international missions across more than 500 patrols.
 - Secured assets valued at over \$10M by implementing stringent safety and security protocols.
 - Trained personnel in advanced safety measures, achieving 100% certification compliance.
-

SKILLS

- **Cloud Security:** Azure Security Center, Microsoft Sentinel, Azure AD Conditional Access
 - **Endpoint Protection:** Endpoint Detection and Response, Antivirus/Antimalware, Endpoint Encryption
 - **Security Operations:** SIEM, SOAR, Vulnerability Management, Incident Response, MITRE ATT&CK
 - **Compliance:** MITRE ATT&CK, NIST Cybersecurity Framework, ISO 27001
 - **Technical Tools** Cyber Operations Risk & Response, VMware Carbon Black Endpoint Standard and EDR, CrowdStrike Falcon, Sentinel One, Palo Alto Cortex XDR, Devo
-

CERTIFICATIONS

- Microsoft Certified: Azure Security Engineer Associate (AZ-500)
 - Microsoft Certified: Security Operations Analyst Associate (SC-200)
 - CompTIA Advanced Security Practitioner (CASP+)
 - CompTIA CySA+, Security+, Network+, A+, Server+, Project+
-

EDUCATION

- **I.T.-Systems Administrator Certificate Program**
MyComputerCareer — Dallas, TX
 - **A.A.S in Hospitality Management**
Collin College — Frisco, TX
-

AWARDS

- Valedictorian, MyComputerCareer
- Best Concept, Hospitality Marketing & Sales (2015)