**Alex Tran Thach**

Philadelphia, Pennsylvania

856-412-9487

[alex.thach3@gmail.com](mailto:alex.thach3@gmail.com)

<https://www.linkedin.com/in/alex-thach-297190120/>

**PROFESSIONAL SUMMARY**

Cyber security expert and military veteran with a Top-Secret security clearance and over 10 years of proven experience in the United StatesAir Force and Temple Health. Accomplished measurable results while leading teams in a dynamic, fast - paced environment. Possesses a comprehensive background in network and virtual systems engineering from conducting domestic and global operations in Germany, Poland, Iraq, Korea, and Japan. Managed risk upon multiple lines to protect assets, property, and equipment valued over fifty million dollars while meeting the expectations of senior leadership. Possess extensive knowledge in cyber forensics investigation and reverse engineering IT systems.Recipient of multiple awards for outstanding performance and professionalism. Career supported by an Information Technology associate degree and numerous certifications.

* Project team leader
* Risk manager
* Red team
* Network engineer
* Cloud System administrator
* Cyber security engineer
* Digital forensics analyst
* Cyber threat analyst
* Linux administrator

**PROFESSIONAL EXPERIENCE**

**Naval Information Warfare Center – Full-time Present**

**Defensive Cyber Operations Engineer – Philadelphia, Pennsylvania**

Lead technical engineer in charge of tooling software and hardware packages for cyber protection teams across United States Navy and USCYBERCOM personnel. Engineered software solutions for breach and attack simulation for military IT systems.

**Temple Health University Systems – Full-time Sep 2022 – November 2023**

**Security Engineer II – Philadelphia, Pennsylvania**

Lead purple teamer that analyzed, improved, implemented, and executed security controls proactively to prevent external threat actors from infiltrating company information or systems. Research more advanced and complex attempts/efforts to compromise security protocols through breach and attack simulation. Maintained security systems, assesses security policies that control access to systems, and provides regular status updates to the management team. As well as support in vulnerability research and assist in high impact incident response engagements. Coordinated red/purple team exercises with AttackIQ and penetration testing engagements with different IT teams.

* Identified high priority intelligence on weekly reports to coordinate and mitigate risk on business objectives.
* Utilized Microsoft O365 Defender suite for endpoint detection and response. Built advanced hunting KQL queries and rules for targeted threat hunting on more advanced exploits and threat actors known IOCs and TTPs. Lead team members for specific incident response tasks.
* Tested key threat scenarios against TUHS's business operations using adversarial attack tools, tactics and techniques based on MITRE framework. Results from attack scenarios were then automated into Azure Sentinel SIEM for incident response playbooks, threat intelligence ingestion with industry ISAC, and anomaly detection.
* Coordinates patch management utilizing Rapid7 IVM and Medigate with IT Teams to ensure timely remediation on discovered vulnerabilities. Conducted periodic compliance audits based on NIST and PCI frameworks.

**United States Air Force – Various Locations 2014 – 2022**

**Cyber Systems Operations Supervisor – Yokota Airbase, Japan: Aug 2021 – Feb 2022 – Full-time**

Developed open source no cost DCO and threat simulation network. Orchestrated numerous red vs blue simulated exercises within lab environment. Mentored and qualified over 30 personnel on cyber forensics skills, threat hunting, and defensive network tools.

* Personnel were trained on how to operate open-source virtualization software such as Xen Cloud Platform – next generation (XCP-NG) to utilize tools such as Security Onion, pfSense firewall, Open Vulnerability Assessment Scanner (OpenVAS), and Graphical Network Simulator 3 (GNS3) to simulate network traffic.
* Threat and simulation scenarios based on real world tactics, techniques, and procedures from numerous cyber threat actors. Open source nginx web servers deployed within Wazuh EDR solution against Metasploit, Cobalt Strike and Atomic Red Team tools used in red vs blue team exercises.

**Cyber Security and Defense Specialist – Yokota Airbase, Japan: Feb 2019 – Aug 2021– Full-time**

Accountable for the defense and risk assessment of aircraft and other industrial control systems (ICS). In charge of risk mitigation of open vulnerabilities and policy guidance enforcement for aircraft IT and network systems.

* Implemented scanning polices using Assured Compliance Assessment Solution (ACAS) for out-of-date software and created virtualized copies of end-of-life IT systems for forensics and reverse analysis on system function and design.
* Worked as a risk evaluations officer to report status of vulnerabilities to higher headquarters. Risk assessments were based on National Institute of Standards and Technology (NIST) guidelines for information systems security controls SP 800-53 Rev. 5.
* Utilized tools such as Ghidra, FTK imager, volatility, and Kibana for in-depth intrusion and malware analysis. Reverse engineered mission related programs and developed working threat and logical models.

**Tier 3 Helpdesk Manager and Software Compliance Auditor – Yokota Airbase, Japan: March 2018 – Feb 2019– Full-time**

Provided elevated level of IT support by consistently improving and resolving issues within large scale enterprise network using Active Directory. Performed remote troubleshooting through diagnostic techniques and pertinent questions. Discovered and innovated IT solutions using PowerShell, JavaScript, and C++.

* Managed user issues coming in by phone, remedy ticketing system, email, and in person with a staff of 300 personnel.
* Regularly performed vulnerability assessment and software compliance auditing for Microsoft 2016 servers, Linux systems and Cisco network devices using ACAS and Security Technical Implementation Guide (STIG).
* Supervised network defense personnel and functioned as scripting and software modification expert for complex device issues such as software incompatibility, maintenance automation, and networked system adjustments. Most common scripts were written in either PowerShell or Bash and most programs were written in JavaScript or C.

**Linux/Unix System Engineer – Osan Airbase, South Korea: Jan 2017 – Feb 2018– Full-time**

Lead engineer responsible for the maintenance and installation of Solaris database servers and Red Hat Linux (RHEL) Nessus scanners for secured network. Local administrator for Citrix XenApp servers that managed a virtualized desktop environment for users. Also managed Structured Query Language (SQL) database servers for thirty-million-dollar weapon system.

* Planned, scheduled, and upgraded Red Hat Linux servers that were used as ACAS scanners for secured network. Deployed scan policies for virtual desktop systems and managed 3000 user accounts in enterprise network.
* Managed daily maintenance of Microsoft SQL 2012 server database and user account data. Gained proficiency in SQL language and SQL data manipulation.
* Administered large-scale Citrix XenApp servers hosting virtual desktop environment for 1200 thin clients. Streamlined update and maintenance process for the VDI thin clients by applying a wide area network update policy.

**Projects: Strix Interceptor DEFCON31 Demo Labs**

The Strix Interceptor Drone is an open-source, multi-functional UAV designed to intercept other drones and defend against anti-drone RF systems. Features Pixhawk autonomous flight, matrix motor config, and multi-RF spoofing capabilities. Demonstrated and presented at DEFCON31 conference.

**Publications:** IAC-2023 Developing an AI-Enabled Cybersecurity Model to Protect Satellite Systems from Cyber Threats 80363

**EDUCATION**

Associate of Information Technology, Community College of the Air Force - 2017

Bachelor of Computer Science, University of Maryland Global Campus- Projected 2024 graduation

**CERTIFICATIONS**

CompTIA A+ COMP001021489491

EXP DATE: 07/29/2024

CompTIA Security+ COMP001020809919

EXP DATE: 02/02/2024

CompTIA Network+ COMP001021489491

EXP DATE: 08/25/2024

CompTIA Cloud Essentials COMP001021489491

LPI Linux Essentials

CompTIA CIOS COMP001021489491

CompTIA CSIS COMP001021489491

**NOTABLE AWARDS**

Meritorious Honor Award

Commendation Service Medal

Global War on Terror Combat Citation

**TECHNICAL SKILLS**

**Software:** Microsoft Office, SharePoint, JIRA, Confluence, GitHub,

Visual Studio Code, NMAP, Volatility, FTK Imager, Elasticsearch, Wireshark, AzureDevOps, Rapid7, ExtraHop, AttackIQ, O365

**Operating Systems:** Mac, Microsoft Windows, Red Hat Linux, Ubuntu

**Programming:** JavaScript, Bootstrap, Python, HTML5, PowerShell, C++, React