Nathan Ndefo Hristov

+447538646397 | Nathanndefo@gmail.com | LinkedIn

Summary

Aspiring cyber security professional with a CompTIA Security+ & BLT1 certification, eager to leverage skills from IT Field Engineer experience and self-study to contribute effectively to a dynamic SOC or cyber security team.

- Hands-on experience with **SIEMs**, specifically **Splunk**, through Security Blue Team Level 1.
- Experience in monitoring using **EDR** (Sophos Intercept X) systems during my time as an IT Field Engineer
- Familiar with **MITRE ATT&CK** and **NIST** frameworks from **Security+** certification and university
- Proficient managing and overseeing **Microsoft Windows Defender, AD, Azure AD and 365 Administration** from IT Field Engineer experience
- Knowledge in vulnerability management from using tools such as **Nessus** from Security Blue Team labs.

Experience

Sept 2022 – Apr 2024 **IT Field Engineer** **Inspire ICT Ltd**

During my time as a field engineer, I was responsible for providing on-site technical support for 7 different sites on a weekly rota, each site utilised a wide range technologies, giving me a broad and comprehensive experience across various systems and environments. My responsibilities included administering Active Directory, managing Azure cloud services, configuring and maintaining Windows Server environments, managing security monitoring tools and orchestrating intricate network setups.

- **Sophos Intercept X (EDR)** to monitor, oversee and respond to threats ensuring the security and integrity of IT systems.
- **Sophos Phish Threat** to create phishing templates and run phishing awareness campaigns.
- Managed mobile devices using **Cisco Meraki MDM**, configured profiles and ensured compliance with security policies.
- Experience with **Active Director**y architecture and administration, including user account management and security principals
- Maintained **Windows Server** environments, including configuration, monitoring, and troubleshooting to ensure optimal system functionality and uptime.
- Proficiency in networking, installation and configuration of network devices such as switches, firewalls and access points.
- Implemented and managed **Group Policies** to enforce security and configuration settings, manage user rights, utilising **GPOs** and **GPPs**.
- Strong interpersonal and communication skills, working with end-users to provide technical support and resolve end user issues in a **help desk** setting in a timely manner.

Aug 2017 – Sept 2018 **Web Developer Internship** **Fable Bureau**

At Fable Bureau, I shadowed a senior full-stack web developer and assisted in implementing a multimedia gallery for showcasing event photos and videos along with several other content pages.

- Used **JavaScript** and **CSS** to create and style web pages
- Liaised with graphic designers to retrieve appropriate web elements and ensured they were of quality
- Gained hands-on experience with **Git** to manage and track code changes.
- Developed and executed comprehensive test plans for **React** components and **JavaScript** code using testing frameworks such as **Jest** and React Testing Library

Certifications

August 2024	**Blue Team Level 1**	**Security Blue Team**
May 2024	**CompTIA Security+ (SY0-701)**	**CompTIA**

Education

Sept 2019 - Jun 2022, BSc (Hons) Computer Science, Brunel University, London

Specialisation: Cyber security

Sept 2015 to July 2017, A Levels, City and Islington College, London

Level 3 Extended Diploma in IT Practitioners: D*D*D*

Technical Projects

Security Blue Team Level 1:

SIEM and Log analysis – Completed hands-on SIEM labs as part of the Security Blue Team Level 1 certification, focusing on leveraging **Splunk** for comprehensive security monitoring and incident response.

- Collected, normalised and analysed logs from diverse sources, including firewalls, IDS/IPS, and endpoint protection systems.
- Developed custom **dashboards** and visualisations in **Splunk** to effectively communicate security metrics and incident trends.
- Employed Splunk's **search query language (SPL)** to investigate security incidents, create queries, and extract actionable insights from data.

Phishing Analysis – Completed labs consisting of categorising phishing emails based on key indicators, retrieving email, web and file artifacts from emails and creating **reports** based on an email's malicious intent.

- Used **PhishTool** to analyse phishing emails and collect email artifacts such as file hashes and header details
- Visualisation tools such as **URL2PNG** and **URLScan** to safely asses potentially malicious URLs
- Analysed IP addresses, URLs, domains and file hashes using **VirusTotal**

Digital Forensics – Hands on labs covering digital evidence collection, Windows and Linux investigations.

- Forensic tool **Autopsy** for in-depth forensic analysis, including file recovery, timeline creation, and identifying artifacts on digital storage devices
- **FTK Imager** to create forensic images of digital storage devices and ensure data integrity through hashing
- Employed **KABE** for comprehensive memory analysis and investigation of volatile data in live systems
- **Scalpel** in Linux for carving files from disk images based on file headers and footers, recovering deleted data for forensic examination
- **Volatility 3** to analyse memory dumps from systems

Networking/Linux Project - A project using **Ubuntu** to capture and investigate network packets using **Wireshark**

- Confident in navigating and using commands on Linux based OS such as **Ubuntu**
- Set up a **virtual network** to study network protocols using **Oracle VM VirtualBox**
- Experience in using Wireshark **packet sniffer** tool and **protocol analyser** to examine network traffic
- A firm understanding of network concepts including TCP/IP protocols

Interests

Technology

- Regularly watch podcasts on cyber security and cybercrime, such as Darknet Diaries exploring incidents and trends.
- Eager to expand knowledge in cyber security through certifications, self-study and hands-on experience.

Other

- Enjoy the outdoors, regularly find the time to hike, camp and fish.
- Small business in photography focusing on portraits and cars.