Mr. Hud Seidu Daannaa *CEH* | *AWS-SAA* | AZ-500| *GCHQ*| *M.Sc.* *Information Security*
Recently completed studies on: CISSP (ongoing)| **SANS 508** |**EC-Council Cybersecurity Career Mentor**
Work: *+971522510778*, **Mobile**: *+971566300943* **Email**: hdaannaa@gmail.com

Website:
www.daannaa.space

NOTE: *For most of my works, there are sample deployment in my home lab, upon request, access or demonstration can be provided*

Profile

With over a **decade of experience in IT and cybersecurity**, Hud specializes in **building cutting-edge security tools custom integrations and secured architectures**. As an experienced Security **Architect**, **engineer** and **researcher**, Hud grew, led and mentored teams, to successfully develop and implemented **state of the art top-level security clearance Next Generation SOCs and MSSPs for the private and government sectors**, ensuring robust defense mechanisms and operational excellence. His leadership extends to engaging teams in comprehensive **guest lectures**, **knowledge transfer** and **training sessions**, empowering them with the latest in cybersecurity practices. Additionally, Hud has a strong track record of over **8 years in the several open-source communities**, where he **authored influential libraries and articles**, driving innovation and knowledge sharing. Hud is also a **part-time lecturer** and a **mentor**, where he is dedicated to passing on his expertise to the next generation of IT and cybersecurity professionals.

Portforlio: https://github.com/huddaannaa/HudsPortfolio (portfolio) http://daannaa.space/ (personal website) https://www.linkedin.com/in/hud-daannaa-senior-security-engineer/ (LinkedIn profile)

Key Responsibilities:

- **Mentorship and Leadership**: Hired and mentored a team of outstanding technical security professionals, providing guidance and direction, resulting in a 30% increase in team performance and morale. https://www.linkedin.com/in/hud-daannaa-senior-security-engineer/details/recommendations/ https://www.linkedin.com/pulse/unlocking-power-brain-redefining-our-reality-through-hud-daannaa-teq3f/?trackingId=vz9af%2BjQTbSPpuJKamj%2Blg%3D%3D https://www.linkedin.com/pulse/marketplace-life-lessons-mutual-dependence-trust-hud-daannaa-st0bf/?trackingId=fP3ty1xNQzaeYIOEGeuCpQ%3D%3D *(the last two article were written to motivate, and boost the confidents of individuals I mentor)*
- **SecOps Standards and Playbooks**: Defined and enforced SecOps security standards and playbooks, leading to a 25% improvement in incident response times and a 40% reduction in security incidents. https://github.com/huddaannaa/NextGenSOC-Snippet/blob/main/SOAR/about-playbook.pdf *(leveraged, SOAR platforms)*
- **SOC Architecture and Design**: Architected and designed the Security Operations Center (SOC) from the ground up, implementing advanced logging, firewalls, network segmentation, and honeypots, which enhanced threat detection accuracy by 35%. https://github.com/huddaannaa/NextGenSOC-Snippet/tree/main/1-SOC
- **Continuous Security Improvement**: Analyzed and continuously improved the security architecture, resulting in a 20% increase in overall security posture and resilience.
- **Security Tool Evaluation and Implementation**: Evaluated, selected, and implemented cutting-edge security tools and practices, reducing manual security processes by 50% and improving threat remediation efficiency. https://github.com/huddaannaa/ASM-Transactor/blob/main/ASM-Transactor-doc.pdf *(automation)*
- **Threat Identification and Remediation**: Identified, contained, and guided the remediation of security threats and cyber-attacks, decreasing incident response time by 30%.
- **Thought Leadership in SecOps**: Enhanced the presence and thought leadership of the SecOps practice within the industry, leading to a 15% increase in industry recognition and partnership opportunities.
- **Open-Source Threat Intelligence**: Contributed to open-source threat intelligence initiatives, representing the organization in sector-specific governance bodies, which improved collaboration and threat sharing by 25%. **https://www.techsphere.biz/ https://github.com/huddaannaa/Intelligence-notes-tool** https://github.com/huddaannaa/SIFIA-TechVibe-TechSphere.md/blob/main/API-Overview.md *(develop a CTI solution, free feeds available and integration to MISP available)* https://github.com/huddaannaa https://pypi.org/project/hudutils/0.7/
- **Threat Modeling and SecOps Practices**: Drove threat modeling, tabletop exercises, and other SecOps practices across engineering, IS, and the broader organization, enhancing cross-team collaboration by 35%. https://github.com/huddaannaa/Experience/blob/main/SOC_v4.pdf
- **SecOps Learning and Development**: Developed and delivered SecOps learning and development materials, resulting in a 40% increase in internal training effectiveness and staff knowledge. https://github.com/huddaannaa/NextGenSOC-Snippet/blob/main/Training.md (training material timetable)
- **Content Creation and Public Speaking**: Published blog posts, whitepapers, and delivered conference presentations, which increased the organization's visibility and influence in the security community by 20%. https://github.com/huddaannaa/DFIR (lecture slides), https://articles-by-hud.blogspot.com/ *(blog spot)* https://github.com/huddaannaa/DFIR/blob/main/GuestLectures/Cybersecurity-month.pdf (guest lecture)
- **SecOps KPIs and Agile Practice**: Identified, implemented, and tracked SecOps KPIs, and planned and delivered SecOps work within the framework of the organization's agile engineering practice, improving project delivery timelines by 30%.
  Security Leadership Collaboration: Collaborated with Security leadership to present information and influence organizational change, leading to the implementation of 15 new security features and policies. https://github.com/huddaannaa/Experience/blob/main/SOC_v4.pdf https://www.linkedin.com/pulse/copy-critical-july-2024-crowdstrike-falcon-sensor-update-hud-daannaa-jnvqf/?trackingId=4u0giGuKTSayo128wTUNMg%3D%3D

Work Experience

August 2023 - **Present**
Role: Lecturer
Company: Middlesex University *(UK)* Dubai
Company website: https://www.mdx.ac.ae/
Dubai Knowledge Park Campus, Dubai, United Arab Emirates
Subjects:
Digital Incident Scene Investigation *(A practical module, which involves the creation and simulation of an incident scene).*
Sample lecture notes: https://github.com/huddaannaa/DFIR
Computer security and Ethical hacking

Achievements:

- **Fostered Security-First Mindset**: Fostered a security-first mindset among over 200 students annually by integrating practical threat modeling, secure code review, and solutions architecture exercises into the curriculum, resulting in a 50% increase in students' ability to identify and mitigate security risks.
- **Developed Comprehensive Cybersecurity Courses**: Developed and delivered comprehensive cybersecurity courses covering the latest industry trends and technologies, enhancing students' understanding of strategic and technical aspects of cybersecurity products and services, leading to better real-world application.
- **Recognized Security Thought Leader**: Recognized as a subject matter expert in cybersecurity, regularly invited to speak at industry conferences and workshops, sharing best practices and innovative security solutions, contributing to a 30% increase in the adoption of these practices within the community.
- **Led Real-Time Incident Response Simulations**: Led real-time incident response simulations and labs for students, enhancing their ability to identify, quantify, and manage security issues swiftly and effectively, resulting in a 40% improvement in student performance in handling cybersecurity incidents.
- **Collaborated on Curriculum Development**: Collaborated with industry professionals and academic colleagues to develop and update the cybersecurity curriculum, ensuring it reflects current industry standards and practices, which led to increased program accreditation and industry recognition.

April 2023 - **Present**
Role: Founder and *(CTO)The Inventor*
Company: Techvibe, INC. *(Techsphere)*
Company website *(visit website to get documentations and slides):* https://www.techsphere.biz/ Preview demo at: https://fs-ui.trendsetterfarm.com/
Middletown, Delaware
Solution: [A cybersecurity solution] Generative Pretrained Transformer (GPT) powered - Security Intelligence Feed and Indicator Analytics *(SIFIA),* with advanced analytics and visualizations and a robust API, to enhance integration with other systems *(The platform started as a hobby in my home lab)*
The solution also has an API: https://github.com/huddaannaa/SIFIA-TechVibe-TechSphere.md/blob/main/API-Overview.md

I founded **Techsphere** as a startup with a focus on innovative cybersecurity solutions. One of our flagship products is Security Intelligence Feed and Indicator Analytics (SIFIA), which originated from my home lab and is now undergoing Proof of Concept (POC) evaluations with several clients in production environments.
SIFIA is a **SaaS multi-cloud and hybrid platform designed to operate within a zero-trust** environment. **I personally designed, developed, and implemented this solution from the ground up**. SIFIA collects and ingests OSINT data, dark web content, security news articles, and other threat-related feeds from verified, credible, and paid sources globally. Utilizing large language models (LLMs) and advanced data processing techniques, the data undergoes extensive preparation, processing, and filtration. This process extracts vital information in the form of Indicators of Compromise (IOCs) through data correlation and enrichment methodologies. **Documentation**:
https://onedrive.live.com/?authkey=%21AE027I%2DxzTWctZE&id=BC6C1638DFED86AA%217319&cid=BC6C1638DFED86AA&parId=root&parQt=sharedby&o=OneUp

Nov 2018 - **Present**

Role: Senior Manager Cyber Security Architecture and Engineering

Company: Maguire Software Trading **LLC**
Company **website**: https://www.maguire.ae/
Dubai, United Arab Emirates
List of projects:

Project 7 – currently in progress-
April 2024 – **Present**
Government Sector *(Ministry of presidential Affairs - UAE)*
Sas-al-Nakhl, Abu Dubai, United Arab Emirates
Project type: (Project lead and SOC Architect) To improve an existing Security Operations Center (SOC) by integrating large language models (LLMs) powered by both local and public Generative Pre-training Transformer (GPT) technologies.

- Leveraged GPT models to enhance the SOC's alert investigation process, providing contextual insights and automating routine tasks, to help facilitate faster and more accurate incident response, reducing the time to mitigate security threats.
- Ensured the SOC architecture is scalable to handle increasing data volumes and evolving threat landscape to help optimize the use of vector databases for efficient data retrieval and processing, supporting the SOC's operational efficiency.
- Integrating LLMs, including Llama 2, 3, and ChatGPT API capabilities, with existing SIEM tools, enhancing the SOC's ability to correlate and analyze data from multiple sources. You can find a same usage of Llama2 here: https://ai-38ac61289cc9431d9335733b776afcfa.mentispotestas.com
- Developing, GPT powered advanced threat and behavioral analytics to help analyze data to identify complex threat patterns and anomalies in user/system behavior, improving threat detection and response.

Project 6
April 2022 – June 2024
Government Sector *(National Supreme Council - UAE)*
Al Bustan, Abu Dubai, United Arab Emirates
Project type: (Project lead and SOC Architect) **Designing**, **developing**, and **managing** a private MSSP for multi-tenants powered on multi and private cloud environment- G42 *(Security Cleared)*

- Designed and led a team of security engineers to develop a high-availability, 6-node Kubernetes micro-service architecture for a threat intelligence platform on a multi-cloud environment. Aligned with OWASP Top 10 security best practices and created pipelines for ingesting, parsing, enriching, and correlating intelligence sources
- Ensured robust security by integrating necessary security implementations, including firewalls, intrusion detection/prevention systems (IDS/IPS), and endpoint protection solutions.
- Designed and deployed secure, scalable architectures *(custom built SIEM)* in G42 cloud for monitoring and logging.
- Developed and enforced IAM policies, ensuring granular access controls and secure authentication mechanisms across cloud and on-premises resources.
- Utilized SIEM tools to collect, analyze, and correlate logs from AWS, VMware, and on-premises systems, identifying and responding to security incidents in real-time.
- Conducted regular security audits and penetration tests to identify and remediate vulnerabilities in hybrid cloud infrastructure.
- Deployed advanced threat detection solutions, including machine learning-based anomaly detection and threat intelligence feeds, to enhance the platform's security posture.
- Provided continuous monitoring and incident response capabilities, swiftly containing and mitigating security threats in hybrid environments.
- Collaborated with cross-functional teams to integrate security best practices into the development lifecycle and ensure secure application deployment.
- Delivered training and knowledge transfer sessions on security policies, procedures, and best practices for cloud and hybrid environments
- Created an API to integrate the threat intelligence platform with an Apache Spark processing pipeline for indexing into Elasticsearch, enhancing data processing and search capabilities.
- *Threat Modeling and Research*: Conducted research on attack matrices and mapped indexed intelligence against threat modeling frameworks such as MITRE ATT&CK (APTs, intrusion sets, mitigations) and Cyber Kill Chain.
- Designed, developed, and documented SOAR automation playbooks integrated with the intelligence platform. These playbooks empowered SOC operations by validating incidents via alert triage and connecting to security controls to act based on alert criticality from the SIEM.
- *Incident Response and Forensics*: Performed threat hunting, digital forensics, and incident response; managed incidents effectively and maintained clear communication with stakeholders.
- Mentored team members, suggested security improvements, and managed security projects from inception to completion.

Project 5
Feb 2020 – **Present**
Raptorx – MSSP – Injazat data systems https://www.raptorx.com/
Client: *Cleveland Clinic, STRATA, SANAD, Mubadala, BMS etc.*
Role

- **Threat Detection Enhancement**: Improved threat detection capabilities by integrating advanced SIEM tools and machine learning algorithms, resulting in a 30% increase in early threat identification for client environments.
- **Incident Response Leadership**: Led a team of analysts in orchestrating incident response processes, successfully mitigating 95% of cybersecurity incidents within SLA-defined timeframes.
- **DFIR Operations**: Spearheaded Digital Forensics and Incident Response (DFIR) efforts, conducting in-depth forensic analysis on breached systems, leading to a 40% reduction in investigation time.
- **Risk Management Framework**: Developed and implemented comprehensive risk management frameworks, aligning with industry standards, which improved clients' risk assessment accuracy by 50%.
- **Mentorship and Training**: Mentored junior security staff, providing guidance and training on best practices and advanced security techniques, enhancing team efficiency and skill levels by 25%.
- **Secured Design Implementation**: Architected secure infrastructure designs for client projects, incorporating zero-trust principles and robust encryption methods, leading to a 35% improvement in system security posture.

Project 4
Feb 2020 – April 2024
Government Sector *(Ministry of presidential Affairs - UAE)*
Sadiyat island, Abu Dubai, United Arab Emirates
Project type: (Project lead and SOC Architect) **Designed**, **built**, and **managed** a Next Generation SOC in a restricted (offline) environment *(Security Cleared)*

- Designed security architectures, developed integration components for a big data platform (security data-lake). The platform was implemented based on Elastic Stack and Elastic SIEM, customized with other big data tools like spark, Kafka etc. on a 16node cluster. Extended integrations to the system included system included vulnerability and pen-test tools, SOAR, EDR and threat intelligence solutions.
- Researching and enhancing the efficiency of the systems, by creating custom modules and connectors. Developing parsers to integrate and create data pipelines for other security solutions to fetch logs from data sources like proxy, firewall, DNS, antivirus etc.
- Managing the security data-lake cluster, creating detection use-cases on security the data-lake, designing incident response playbooks on the SOAR platform, policies and rules on EDR, dashboards, as well as maintaining and fine-tuning data pipelines in the cluster: https://drive.google.com/file/d/1YrsZmrKB0jcxA9jTj4dGkVtiPaTOKl5U/view
- Performing manual and automated penetration tests (SAST/DAST) to determine an environment's security posture and validation detection use-cases in on the SIEM, to evaluate their effectiveness and robustness. Developing custom exploits, auxiliary modules, and resource scripts in python and Metasploit pro (ruby). Some example of custom resource scripts for Metasploit: https://github.com/HudKSD/Pentest-custom-modules-metaploit-by-hud

Project 3
Aug 2020 – Dec 2020
Private Sector *(G42 | Artificial Intelligence & Cloud)*
Albustan, Abu Dubai, United Arab Emirates
Project type: (Project lead and SOC Architect) To **design**, **develop**, and **implement** a comprehensive security data-lake solution within a security-cleared, air-gapped private cloud environment

- Spearheaded the engineering and architectural design of the security data-lake platform.
- Led a multidisciplinary team of engineers, fostering collaboration and ensuring project milestones were met efficiently.
- Developed the security data-lake on a highly secure, containerized cluster environment, ensuring scalability, flexibility, and robustness.
- Designed and implemented vulnerability management use-case automations, enhancing the proactive identification and remediation of security vulnerabilities.
- Ensured interoperability and streamlined communication between different security solutions to create a unified defense mechanism.
- Delivered a state-of-the-art security data-lake solution capable of comprehensive network monitoring and deep packet analysis. Enhanced the organization's ability to perform forensic investigations and respond to security incidents with greater precision and speed.

Project 2
Aug 2020 – Dec 2020
Private Sector *(Khazna Data Center)*
Khalifa City, Abu Dubai, United Arab Emirates
Project type: (Project lead and SOC Architect) Endpoint Detection and Response (EDR) management System into an existing environment *(Security Cleared)*

- Implementing and managing endpoint management solutions and ensuring all endpoints are correctly configured, up-to-date, and compliant with company policies.
- Developing and enforcing endpoint management and security policies, also configured endpoints comply with organizational standards and regulatory requirements.
- Providing support to end-users for endpoint-related issues, including troubleshooting hardware and software problems. Educating users on best practices for endpoint security and compliance.
- Maintaining an inventory of all endpoint devices within the organization and tracking the usage, location, and status of endpoints to ensure efficient asset management.

Project 1
Nov 2018 – Nov 2020
Private Sector *(Mubadala Investment Company and Injazat Data Systems.) including offices in UAE and Russia - Moscow*
Abu Dubai, United Arab Emirates
Project type: Built Attack surface management *(ASM)* components for vulnerability **management** and Penetration testing in a GSOC *(Security Cleared).*

- The lead engineer managing the attack surface (cyber exposure) aspect of the GSOC. Deployed, configured, and designed policies and best practices for security tools such as App spider, Metasploit Pro Tenable Security Center.
- Designed and developed a system, which handles the *ASM* section of in a GSOC and fits in as a vulnerability solution to aid in the reduction of the attack surface. It performs scans and enrichment to support a given number of tenants *(Assets)* and provides vulnerability validation. It is basically an integration between two solutions, namely Tenable SC, Metasploit Pro and mongo DB. https://drive.google.com/file/d/12VEs0cC_MmotC7NQAh3O-UJx12cnGhaP/view?usp=sharing

Nov 2017- Nov 2018
Role: Cyber Security Consultant & Penetration Tester. *(AWS SysOps Admin - Cloud security specialist)*
Company: www.business.daannaa.space *(Contractor/Freelance), United Kingdom, Mitcham |Ghana, Accra*

- Working with developers, as a security consultant, to implement application security with respect to the *OWASP* in the *SDLC*. Also, carrying out penetration tests, drafting detailed reports and performing information security risk assessment reports on security weaknesses, outlining possible business risks, and drafting recommendations/ controls.
- *AWS Sysops Admin:* Strong understanding of AWS security, design, and integration, big data, and data analysis.

- Extensive expertise in both private and public cloud environments, including AWS, Azure, and Google Cloud. Specialized in building robust monitoring systems that enhance business security and operational efficiency. My experience includes designing and implementing comprehensive security architectures, integrating advanced threat detection, and ensuring compliance across diverse cloud platforms. Through my work, I enable businesses to maintain high availability, scalability, and proactive threat management.
- Implemented automated security compliance checks and vulnerability assessments using tools like AWS Config, AWS Inspector, and Nessus.
- Developed and enforced IAM policies, ensuring granular access controls and secure authentication mechanisms across cloud and on-premises resources.
- Designed and deployed secure, scalable architectures in AWS, leveraging services such as EC2, S3, Lambda, and CloudTrail for monitoring and logging.
- Implemented automated security compliance checks and vulnerability assessments using tools like AWS Config, AWS Inspector, and Nessus.

Sep 2016 - Jan 2018

Role: Cybersecurity Postgrad Researcher. *(Penetration-tester and Cloud security specialist - Part-time Contractor)*

Company: University of Surrey, United Kingdom

- Paid contracts: Embarked on several consulting projects as a short-term contract, these included, penetration testing, cloud security consulting (AWS, Google), network packet analysis.
- Dissertation: Designed a statistical anomaly intrusion detection system using naturals laws *(Benford's and Zipf's laws [Power laws])*, to detect malicious e.g., DDOS and non-malicious traffic network traffic. *[Being published [Distinction (A)]*
- Cloud Computing: Securely designed and implemented, a front and backend scalable multi-cloud application which employed hands-on experience with Amazon Web Services *(AWS)* and Google App Engine *(GAE)*.
  Available on: https://hudd-157916.appspot.com.
  Data Science: Completion of the dissertation and cloud computing projects employed hands-on experience with security related large datasets that employed statistical methods/ techniques *(return series etc.)* using Python to derive insights.

Sep 2015 - Aug 2016

Role: *Systems/ Network Security Engineer*

Company: First October Network Academy, Ghana

Sep 2014 - Sep 2015

Role: *IT/Systems Engineer*

Company: Ministry of communication, Ghana

June 2014 - Nov 2014

Role: *Fiber Optic Network Technician*

Company: Admintelecom Academy, Ghana

Jan 2012 – May 2014

Role: Systems Admin/ *Network Security Technician*

Company: First October Network Academy, Ghana

Education

MSc Information Security | GCHQ certified, Sep 2016 - Sep 2017
University of Surrey, United Kingdom
[Aggregated Level Mark Achieved, 69.25]

Modules: Dissertation A, Symmetric cryptography A, *Asymmetric cryptography* A, Network Security A, Secure Systems A, Information Security Management B, Multimedia and digital forensics GitHub, GitHub, Cloud computing, Databases.

Penetration Testing *(INNOBUZZ)*, July 2015 - Aug 2016
Shiv-India Institute of Mgmt. &Tech http://innobuzz.in/examination/verify Cert. No.*29223*

Ability to write custom penetration testing tools.

BSc Hons Telecommunication Engineering, Sep 2010 - Jun 2014
Ghana Technology University College *(GTUC)*.

First three *(3)* years of computer engineering modules, final *(1)* year of telecommunication modules

Computer Hardware and Networking, May 2008 - 2009
IPMC College of Technology.

Custom assembly of computer and troubleshooting hardware issues

A-Level Equivalent- *(WASSCE)* Course: **General Science**, Sep 2005 - May 2008
ST Thomas Aquinas Senior high school, Ghana

Further Math. *(Calculus, Statistics etc.)* C, English Lang. C, Integrated Science B, Geography B, Chemistry B, Physics B

Technical Solutions Experience

About Artificial intelligence	Prompt engineering, LLMs *(Llama2,3),* ChatGPT API integrations, Ollama, Private GPT, Pandasai, Spacy, Mistral, hugging face etc.
Other Data warehousing components & solutions	Apache Spark, Storm, superset, Tableau, Beats, Splunk, MongoDB, Syslog-NG, Kafka, Zeppelin, Jupyter-notebook, Cloudera, Horton Works, Apache Metron, ELK, Redis, Memcached, HBase, zookeeper, etc.
Analytics *(Visualizations)*	Pandas, streamlit, Gradio, Grafana, Kibana, Vega, matplotlib etc.
ASM & EDR	Tenable SC, App Spider, Metasploit Pro, CrowdStrike, Endgame, Elastic Security etc.
Incident response *(SOAR)*	SIFT Workstation, CyberSponse *(Forti SOAR)*, Siemplify *(developed connector & playbooks) etc.*
Threat Intelligence	Crowdstrike *(threat intelligence)*, Virus total, CRITS, MISP, Exploit DB, Open CTI, YETI, Spiderfoot, etc.
Developed parsers *(python, ruby, GROK, Regex) and* integrations for	Bluecoat *(Proxy),* McAfee EPO, Imperva, Symantec email gateway, VMware ESXI, Meta defender, Forescout, Endpoint protector *(EPP), Net scaler etc.*
Other Solutions	VMware, Darktrace, Splunk, Securonix etc.
Cloud Computing *(DevOps/ Scripting)*	G42 (Huawei), Azure, AWS, Google *(GAE), Ansible, Vagrant, containers (Dockers) etc.*
Standards & Frameworks *(Risk Assessments)*	ISO 27001 & 27002, NIST SP 800-61, NIST 800-60, MITRE, GDPR, HIPAA, PCI-DSS, security policies, risk management frameworks
Regulation Awareness	Data Protection Act 1998, Computer Misuse Act 1990, Freedom of information Act 2000, PCI DSS, GDPR, OWASP.
SecDevOps	Secure CI/CD pipelines, automated security testing, vulnerability assessments etc.
Infrastructure as code	AWS cloud formation, terraform, Kubernetes, docker-compose etc.
Programming/Scripting	Python, Shell scripting, CI/CD integration (Jenkins, GitLab, GitHub Actions)
Soft Skills	Team leadership, mentoring, project management, excellent communication skills

Certifications	*OSCP [In-progress], GCHQ, MSC Information Security,* Certified Ethical Hacker *(CEH),* *CCNA Certified & Training Certificate, FOR508: Advanced Digital Forensics and Incident Response [In-progress], CISSP[In-progress], AWS Sysops Admin, AWS-Solutions Architect, AZ-Security Engineer,*
Hobbies	Researching latest technologies and trying to invent something new (I used to thing I was Nikola Tesla or Newton), Teaching, Watching YouTube webinars, Gaming *(team),* Motorbike enthusiast,
References	➢ Would be provided upon request