Taha Khan

☎ +92 312-5736191 ✉ taha.khan.cyber@gmail.com in https://www.linkedin.com/in/taha-khan-aa4a7828b/

Summary

Proactive **Cybersecurity Professional** with **one year** of experience in cybersecurity operations. Ranked in the top 2% on TryHackMe, showcasing strong analytical thinking, threat hunting, and investigative capabilities. Proficient with core cybersecurity tools and technologies including **SIEM**, **XDR**, **MDM**, **DLP**, and **PAM**. Adept at assessing threats, monitoring alerts, conducting indepth investigations, and supporting incident response to strengthen organizational security posture.

Technical Skills

SIEM Tools: WAZUH, IBM QRadar, Splunk, Elastic SIEM

MDM Tools: Microsoft Intune, Jump Cloud MDM, Hexnode MDM

EDR/XDR Tools: Trend Micro XDR, Sophos XDR, Microsoft Defender XDR

Other Advance Tools: Delinea PAM, Microsoft Purview DLP, Zscaler DLP, VPNs, IPS, IDS

Firewall: Cloudflare WAF, AWS WAF, pfsense

Virtualization: VMware Workstation, VMware Fusion and VMware ESXi

Operating System: Debian, Windows Server 2019, Centos 7, Ubuntu 22 Jammy Jellyfish, macOS

Experience

Ace Money Transfer — January 2025 – Present

Junior SOC Analyst — *Manchester, United Kingdom*

- **Experience**: Worked in a dynamic **Security** environment at a leading **FinTech** company.
- **Threat Monitoring**: Monitored alerts for more than **2500 hours** using **WAZUH**, **Splunk** and **IBM QRadar**
- **Incident Reporting**: Created detailed incident reports and added over **7000 IPs** in Monitoring Sheet.
- **Tools Implementation**: Tested and Implemented **Microsoft Intune**, **Jumpcloud MDM**, **Hexnode MDM**, **Sophos XDR**, **Microsoft Defender XDR**, **Microsoft Purview DLP** and **Zscaler DLP**.
- **Security Policy Enforcement**: Implemented security policies across **SIEM**, **MDM**, **XDR**, and **DLP** platforms.
- **Documentation**: Authored and maintained **SOPs**, Attack Reports, Team Plans, and Proposal drafts.
- **Cross-Functional Security Integration**: Collaborated with the Network Support (NSS) and external vendors.
- **Internal Training**: Completed sessions on **Information Security Risk and Governance**, **Cyber Security**, and **Whistle Blowing**.

Nets International Communications — August 2024 – December 2024

Cyber Security Intern — *Islamabad, Pakistan*

- **XDR Implementation**: Configured and tested policies in **Trend Micro Vision One XDR**.
- **Client Delivery**: Supported deployment of **Trend Micro Vision One XDR**.
- **SIEM & Identity**: Worked with **IBM QRadar**, **Elastic SIEM** and **Active Directory** to strengthen security.
- **Cert Prep**: Completed **CompTIA Security+** training from **Professor Messer**.
- **Technical Presentations**: Delivered structured presentations on Active Directory and Trend Micro Vision One XDR.

Certifications

Security Operations Center Associate (SC-200) — **Link** – Microsoft

Certified Ethical Hacker (CEH) — **Link** – EC-Council

Security Analyst Level 1 (SAL1) — **Link** – TryHackMe

ISO/IEC 27001:2022 Information Security Associate — **Link** – Skill Front

Certified in Cyber Security (CC) — **Link** – ISC2

Google Cybersecurity Professional Certificate — **Link** – Google

Security + — **Link** – CompTIA (exam in progress)

Trainings

High Impact IT Training of AI Integrated Blockchain — **Link** – NUST PDC

Privileged Access Management (PAM) — **Link** – Cybrary

Introduction To Threat Intelligence Landscape 2.0 — **Link** – Fortinet

Pre Security Certificate — **Link** – TryHackMe

Blockchain Security Specialization — **Link** – Infosec

Cyber Security Fundamentals Associate — **Link** – OPSWAT

Cyber Security Fundamentals — **Link** – Nets International

Cyber Security Training Workshop — **Link** – Ignite

Projects

Deployment of Hexnode MDM, Sophos XDR, and Zscaler DLP | *Hexnode, Sophos, Zscaler* **April – June 2025**

- Implemented robust **Mobile Device Management (MDM)** policies using Hexnode.
- Deployed **Sophos XDR** and enforced advanced endpoint protection by configuring custom security policies.
- Tested and successfully implemented **Zscaler DLP** policies in a live environment.

Deployment of Intune & XDR | *Microsoft Intune, Microsoft Defender XDR* **February - March 2025**

- Implemented and enforced robust security policies for users across multiple countries.
- Configured **USB Blocking**, **BitLocker Key Management & Rotation** etc for secure access control.
- Tracked alerts and performed remediation actions including **Quarentine** and **collected logs** remotely.
- Collaborated with **NSS** and external vendors, gaining hands-on experience in enterprise-level security implementations.

Security Monitoring and Analysis | *IBM QRadar, Splunk* **Feburary 2025**

- Explored and practiced SIEM concepts using **IBM QRadar** and **Splunk** through official learning platforms and labs.
- Monitored security alerts and offenses in QRadar.
- Analyzed Splunk dashboards and search queries to gain insights into log parsing, indexing and detection logic.
- Studied the underlying infrastructure, architecture, and integration workflows.
- Developed a foundational understanding of alert triaging, correlation rules, and detection engineering principles.

Security Documentation & Research | *Cloudflare, WAZUH, Purview, SOC Fortress Copilot* **January 2025**

- Developed **comprehensive security reports** and documentation to streamline SOC operations.
- Created **Attack Reports** and configurations for **Microsoft Defender, Intune, Cloudflare, and WAZUH**.
- Conducted in-depth research on **Microsoft Purview, SOC Fortress, and SOAR** to enhance security workflows.

Trend Micro Vision One XDR Deployment | *Trend Micro Vision One XDR* **November - December 2024**

- Supported the deployment of **Trend Micro Vision One XDR**.
- Assisted in **policy configuration and endpoint protection setup**.
- Created and tested policies for **Server** to ensure comprehensive security coverage.
- Attended technical sessions on advanced threat detection and response strategies.

SIEM Implementation and Monitoring | *Elastic SIEM, IBM QRadar* **October 2024**

- Designed and implemented a custom SIEM setup using **Elastic SIEM**.
- Monitored and analyzed log data in **Elastic SIEM** for real time threat detection and incident response.
- Configured and maintained **IBM QRadar** to monitor offenses and security events across multiple data sources.

Active Directory Policies Implementation | *Enhancing Security and User Management* **September 2024**

- Implemented comprehensive Active Directory policies to enhance organizational security.
- Created and managed **Organizational Units (OUs)** and **Groups** to streamline user management and access control.
- Developed and tested **User Password Change Policies** and **Password Strength Requirements** to enforce robust security standards.
- Conducted thorough testing and validation of policies to ensure compliance with organizational security protocols.

Education

Federal Urdu University of Arts Science & Technology **Sep. 2020 – Aug. 2024**
Bachelor of Science in Computer Science *Islamabad, Pakistan*