Ishaan Srivastava

07xxxxxxx | contact@ishaansrv.com | Edinburgh (linktr.ee/ishaansri)

Summary

Experienced Threat Hunter with 4+ years in proactive detection, TTP-based hunting, and behavioural analytics across cloud and hybrid environments. Skilled in event correlation, detection engineering, and threat-led analysis. Passionate about reverse engineering, automation, and enhancing threat visibility through MITRE ATT&CK-aligned strategies.

Experience

Natwest Group | Edinburgh
Cybersecurity Analyst | 02/2024 - Present

- Performed host-based and network intrusion analysis using telemetry from **Microsoft XDR, Trellix, Carbon Black, FireEye, and CyberReason** platforms
- Executed proactive threat hunting using **KQL and Splunk** with log correlation; identified **detection rule gaps** and delivered optimization recommendations to engineering **enhancing overall threat coverage**.
- Investigated alerts and performed forensic analysis across **AWS, Azure, and GCP**, correlating multi-cloud evidence to identify insider threats and enhance detection accuracy.
- Reviewed triaged alerts to ensure consistency across SOC workflows, supporting analyst training and driving knowledge sharing across the team.
- Led incident response efforts including containment, eradication, and recovery guidance for DDoS attacks using **Akamai** sensors.
- Investigated phishing and email threats using OSINT tools and correlated data from O365, Cisco IronPort, and Cofense enhancing email threat detection and response capabilities.
- Collaborated with Detection Engineering, and Intelligence teams on **Purple Team** exercises to identify detection gaps
- Responded to **DDoS attacks** on AWS SaaS infrastructure by implementing a unified **response framework**—standardising detection and triage, coordinating cross-teams, and reducing downtime by 30% while strengthening cyber resilience.
- Integrated **Agile/Scrum methodologies** into security engineering projects—conducting sprint planning, stand-ups, retrospectives, and backlog refinement to deliver iterative improvements, align with development teams, and continuously enhance vulnerability management and detection pipelines.

Dar Al-Handasah (Dar Group) | MH
Cyber Security Engineer | 01/2020 - 09/2022

- **Achieved ISO/IEC 27001:2013 compliance** with zero non-conformities by embedding defence-in-depth and security governance across the enterprise.
- Led **incident response** during high-severity incidents, conducting **root cause analysis** and coordinating containment and remediation efforts.
- **Owned the SIEM lifecycle**—integrated log sources, built detection rules, and deployed SOAR playbooks—automating triage and reducing response time.
- Conducted intelligence-led threat hunting aligned to MITRE ATT&CK, developing **custom alert logic**—improving detection coverage by 30%.
- Delivered a full-stack SIEM refresh; **negotiated vendor terms and optimised architecture**—reducing CAPEX and enhancing log fidelity.
- **Deployed** Microsoft **Defender** for Endpoint across the estate, boosting endpoint visibility and incident detection at scale.
- **Authored** standardised **triage procedures**, increasing SOC consistency, analyst efficiency, and detection accuracy.
- Coordinated external **penetration** tests, translating findings into detection rules and **prioritised vulnerabilities**—enhancing security posture and team awareness.
- **Managed** deception controls with **honeypots** and decoys to detect lateral movement and early-stage compromise.
- Built and executed a threat-driven security roadmap using **RACI** (responsbile Actionable, Consulted and Informed) matrix and **vulnerability** data—reducing overall cyber risk by 40%.

Skills

Root cause analysis, Pattern Recognition, OSINT investigation, Cloud Threat Hunting, Incident Response, Threat Attribution, Malware Behaviour Analysis, Product Lifecycle Management, AWS Security

Education

Univeristy of Greenwich | London
Masters of Science in Computer Forensics and Cybersecurity

- Awarded **Distinction** in Batch.
- **Investigated HID hacking** incident through digital forensics, **analysing disk images and memory** using **EnCase**, **Volatility**, and **Autopsy**—recovering deleted data and extracting key evidence to support the case.
- **Dissertation** : Developed a scalable, open-source **SOC platform for hospitals**, simulating live attacks from **APT** groups targeting **healthcare** infrastructure using the full MITRE ATT&CK chain—demonstrating **effective detection** and response capabilities in critical environments.