Ishaan Srivastava

Edinburgh, Scotland, UK
07xxxxxxxx • contact@ishaansrv.com • https://linktr.ee/ishaansri

---

Professional Summary

Threat Hunter and Detection Engineer with 4+ years' experience in proactive detection, TTP-based hunting, and behavioural analytics across cloud and hybrid environments. Skilled in event correlation, detection engineering, and threat-led analysis, with a focus on improving visibility using MITRE ATT&CK-aligned strategies. Passionate about reverse engineering, automation, and building resilient, detection-first security operations.

Core Skills

- **Threat Hunting & Detection Engineering**: TTP-based hunting, hypothesis-driven investigations, SIEM use-case development, rule tuning, correlation logic, coverage gap analysis.
- **Incident Response**: Alert triage, containment, eradication, recovery support; DDoS response coordination; root cause analysis.
- **Threat Intelligence & OSINT**: TI/OSINT enrichment pipelines, IOC validation, severity scoring, investigation acceleration.
- **Cloud & Infrastructure**: Security investigations and log analysis across AWS, Azure, and GCP; hybrid enterprise environments.
- **Platforms & Tools**: Splunk (SPL), Microsoft Sentinel/KQL, Microsoft XDR, LogRhythm SIEM/SOAR, Akamai, Cisco IronPort, Cofense.
- **Languages & Frameworks**: Python, Regex, MITRE ATT&CK, Agile/Scrum.

Experience

NatWest Group — Edinburgh

Feb 2024 – Present
Security Analyst – Detection Engineer

- Designed and implemented high-fidelity detection rules and correlation logic for new and evolving threat use cases within enterprise SIEM platforms (Splunk/SPL, KQL).

- Built, tested, and tuned detection content to reduce false positives and improve correlation quality across enterprise telemetry.
- Developed and maintained SOAR playbooks to automate triage actions, enrichments, and standardised incident workflows.
- Automated detection content deployment and change control using CI/CD-style workflows, enabling consistent and auditable detection management.
- Integrated subsidiary and partner organisations' security systems into the central SOC, unifying alert pipelines, event sources, and detection logic.
- Analysed and documented existing detection workflows across business units to identify coverage gaps and standardise alert tuning methodologies.
- Collaborated with SOC analysts to refine detection correlation, reduce false positives, and optimise response efficiency.
- Served as a subject matter expert (SME) for SOC operations and incident response, providing technical guidance on investigation workflows.

Security Analyst

- Performed host-based and network intrusion analysis using telemetry from Microsoft XDR, Trellix, Carbon Black, FireEye, and Cybereason platforms.
- Executed proactive threat hunting using KQL and Splunk with log correlation; identified detection rule gaps and delivered optimisation 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 improve detection accuracy.
- Reviewed triaged alerts to improve consistency across SOC workflows, supporting analyst coaching 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 to enhance email threat detection and response capabilities.
- Collaborated with Detection Engineering and Intelligence teams on Purple Team exercises to identify and prioritise 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 and continuously enhance vulnerability management and detection pipelines.

Dar Al-Handasah (Dar Group) — MH

Cyber Security Engineer
Jan 2020 – Sep 2022

- Engineered LogRhythm SIEM detection rules and correlation logic to improve threat identification and investigation quality across the enterprise.
- Built raw log parsers and normalisation pipelines using Regex to onboard new log sources, improving event quality, field extraction, and searchability.
- Unified SOC operations across sister companies by onboarding and fully integrating their environments into a single SOC and detection umbrella (standardised telemetry, alerting, and triage).
- Enriched SIEM alerts using threat intelligence from Recorded Future and Group-IB plus OSINT (Abuse.ch, MalwareBazaar, AlienVault OTX) via STIX/TAXII-style integrations, improving context and investigative confidence.
- Contextualised indicators as true IOCs vs. benign artefacts, improving severity scoring and enabling faster analyst decisions during triage.
- Reduced mean time to respond (MTTR) by improving alert enrichment, prioritisation, and investigation readiness.
- Developed and maintained LogRhythm SOAR playbooks executed via agent-run batch command workflows to automate triage steps, data collection, and analyst guidance.
- Led intelligence-driven, TTP-based threat hunting aligned to MITRE ATT&CK, improving detection coverage by 30%.
- Acted as SME for threat and incident investigations; supported high-severity incident response with root cause analysis, containment, and remediation coordination.
- Designed and delivered SOC analyst training on alert triage processes and playbook-led response to improve consistency and speed of investigations.
- Led a full-stack SIEM refresh (hardware upgrades and software optimisation), reducing CAPEX and improving log fidelity.
- Supervised external penetration testing engagements (scope/test parameters) and converted findings into actionable detection use cases and rule sets.
- Deployed deception-based detection capabilities (honeypots/decoys) to increase early-stage visibility and reduce dwell time.
- Implemented ISO/IEC 27001:2013 compliance with zero non-conformities, strengthening security governance and control assurance.
- Built and executed a threat-driven security roadmap using RACI and vulnerability data, reducing overall cyber risk by 40%.

Education

University of Greenwich — London

MSc Computer Forensics and Cybersecurity — Distinction

- Investigated an HID hacking incident through digital forensics, analysing disk images and memory using EnCase, Volatility, and Autopsy to recover deleted data and extract 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.