Harsimran Sidhu

SECURITY OPERATIONS & THREAT INTELLIGENCE ANALYST

harsimransidhu770@gmail.com | harsim.ca | linkedin.com/in/harsimransidhu | github.com/PKHarsimran

Security operations analyst specializing in incident response, endpoint security, WAF investigations, and detection engineering. Translates real-world investigations into clear, practical playbooks for analysts and technical teams.

EXPERIENCE

Security Operations Center Analyst

Columba System Inc, Remote | Nov 2022 - Present

- Monitor endpoint activity with Cortex XDR to identify and investigate potential threats.
- Implement Splunk rules and alerts that support advanced threat detection and triage.
- Manage incident tickets in Jira and escalate critical issues to IT teams for response.
- Automate compliance checks and URL verification with custom scripts.
- Analyze email headers and login patterns to identify and prevent attacks.

Cyber Security Analyst

SecureOps, Remote | Oct 2021 - Nov 2022

- Investigated alerts in Microsoft 365 Defender and managed incident escalation.
- Used Splunk, Azure Sentinel, and AWS Sandbox in daily security operations.
- Applied Kusto Query Language (KQL) to filter and investigate security data.
- Performed packet analysis with Wireshark and worked with cybersecurity frameworks.
- Maintained clear operational communication through Microsoft Teams.

Information Technology Specialist

Telecom Metrics Inc, Kingston, Ontario | Jan 2021 - Aug 2021

- Led IT security projects supporting infrastructure development and server maintenance.
- Provided customer support and remote technical troubleshooting.
- Implemented high-availability solutions and automated operational tasks with Python.

CORE CAPABILITIES

Security operations: Incident triage, threat investigation, endpoint security, WAF analysis, email security, alert escalation, detection engineering
Platforms and tools: Cortex XDR, Splunk, Microsoft 365 Defender, Azure Sentinel, AWS Sandbox, Jira, Wireshark
Querying and automation: KQL, Python, Shell/Bash, Git and GitHub
Working strengths: Problem solving, teamwork, prioritization, technical writing, curiosity

EDUCATION

Cyber Security

University of Toronto Continuing Education, Toronto, ON | Jan 2020 - Aug 2020

Studies focused on cybersecurity strategy and digital information protection.

Bachelor of Engineering in Technology

Cape Breton University, Sydney, NS | Sept 2017 - Apr 2019

Engineering principles and technological systems management.

Electromechanical Engineering - Advanced Diploma

Humber College, Toronto, ON | Sept 2013 - Apr 2016

Practical technical skills and electromechanical theory.