

Sumanshu Sohal

(240)-988-8443 • sumanshu.95s@outlook.com • <https://sumanshusohal.github.io/>

WORK EXPERIENCE

Trellix

Washington DC, USA

FireEye SOC Analyst (Contract)

September 2023 – Present

- Refined SIEM correlation rules and detection logic, and conducted proactive threat hunting using KQL, to improve threat detection and reduce false positives by 30%.
- Investigated and triaged complex security incidents, performing digital forensic analysis and log correlation to determine root cause and produce post-incident reports, and recommend security control enhancements.
- Onboarded and tuned cloud and third-party log sources and partnered with infrastructure and application teams to refine network architecture and data flows, boosting log visibility and ingestion efficiency by 40% and enhancing threat detection accuracy across on-prem and hybrid environments.
- Conducted quarterly risk assessments with Tenable and enhancing compliance alignment with security frameworks (CIS, SOC 2 and GDPR) to improve compliance and security posture by 25%.

WithSecure, Inc.

New York City, USA

Pentesting Intern

June 2022 – August 2022

- Scoping: Collaborated with clients on scoping calls to identify the scope of the assessments.
- Assessment: Conducted web and network vulnerability assessments for clients based on the scope.
- Remediation & Report Writing: Presented detailed findings and recommendations for remediation to clients to strengthen their security measures.
- Research: Conducted independent research on Windows malware, to enhance the understanding of threats.

HCL Technologies Pvt. Ltd.

Noida, UP, India

Cybersecurity SOC Specialist

October 2017 – July 2021

- Led the response to security incidents and breaches, ensuring prompt containment, comprehensive root cause analysis, and effective resolution.
- Collaborated with cross-functional teams to develop incident response plans and communicated key findings to senior leadership, improving stakeholder awareness.
- Matured the SOC's security use cases by implementing the MITRE ATT&CK Framework, enhancing the organization's threat detection capabilities.
- Performed quarterly risk assessments with Qualys, identifying and documenting vulnerabilities while tracking remediation timelines to improve security posture.

TECHNICAL SKILLS

- **Technology and Tools:** SIEM (Helix, ArcSight, QRadar, Splunk, LogRhythm), EDR Tools (FireEye HX, Crowdstrike), SOAR Tools (Siemplify, Demisto), ITSM (ServiceNow), O365, Vulnerability Management (Tenable IO, Qualys Guard, Rapid7 Insight VM), Anti-phishing software (Proofpoint), NMAP, Wireshark, IDS & IPS (NX), Operating Systems (Windows & Linux), Languages (Python, KQL, NIM, REGEX, SQL), Frameworks (MITRE ATT&CK, CIS & NIST), Cloud (AWS & Azure)

PROJECTS

- **Endpoint Modules Health Check Automation:** Automated endpoint health checks with a Python tool to reduce manual effort by 90% and ensure continuous endpoint protection.
- **Cloud Security Architecture & Migration Plan (AWS):** Designed and implemented a secure cloud migration strategy for a business's transition to AWS, mitigating risks and establishing a strong security foundation.
- **EDR Evasion Research & Malware Development:** Researched EDR evasion techniques and developed custom malware to identify detection gaps, strengthening the organization's defensive posture.

EDUCATION

The University of Maryland, A. James Clark School of Engineering

College Park, MD, USA

Master of Engineering in Cybersecurity, 3.94 GPA

May 2023

CERTIFICATES

- CompTIA Security+