HARSHIL GUPTA

Bangalore • +91-9008200689 • harshilsklgupta@gmail.com • GitHub

---

EXPERIENCE

Cybersecurity professional with over **2.9 years** of experience as a SOC Analyst

- Experience with SIEM – MITRE framework, ESM and SOAR, Incident Response.
- Experience in monitoring, identifying and analyzing security events from Antivirus, Firewall, Proxy, IDS, IPS and other network devices.
- Experience in Phishing e-mail analysis.
- Working Knowledge of network penetration testing and techniques.

EDUCATION/ CERTIFICATIONS

- **VTU – Bachelor of Engineering, Information Science and Engineering (2014-2018)**
- **KSecure – Advanced Malware and Intrusion Analysis (Oct, 2018)**
- **EC-Council – Certified Ethical Hacker (CEH) (March, 2021)**
- **AZ-900 Microsoft Azure Fundamentals (June, 2021)**

SKILLS

- SIEM, ESM – QRadar, Splunk
- SOAR – Demisto
- Endpoint Security – FireEye Managed Defense, Carbon Black
- Log Monitoring: Antivirus, IDS/IPS, Windows Authentication Server & Firewall
- Network Analysis Tools: wireshark, burpsuite
- VAPT Tools: Metasploit, Nessus
- Device Management – ScienceLogic SL1, RestorePoint

CAREER

Wipro Technologies, Bangalore, India — October 2018 to March 2020

L1 Analyst – Global Security Operations Center (GSOC)

- Initial screening of security alerts from various sources, confirm true positive/false positive based on the initial analysis
- Recommend use case optimization based on the MITRE framework for alerts that are considered as false positive during initial screening
- Initiate threat hunting campaign during major outbreaks that impacts wide range of organizations
- Make use of OSINT to collate all the evidence of IoC in the security incident report and assist Level 2 team to consolidate
- Tools: QRadar and ServiceNow

L2 Analyst – Global Security Operations Center (GSOC)

- Level 2 analysis and investigation of security events which are considered as true positives during L-1 screening
- Correlate events and document a security incident report with all collected data from various sources such as Antivirus, Firewall, Proxy, IDS, IPS and other network devices.
- Validate the use case optimization for the false positive alerts which are screened during L-1 analysis and advise the content development team for appropriate amendments.
- Monitor spam and phishing email alerts through Demisto, initiate playbook action – advise end users to handle those emails cautiously.
- Follow up on the security incidents generated and drive it to the closure. Respond and provision data/logs to customers on ad-hoc basis whenever there is such requirement.
- Assist the track lead to create and delegate Weekly/Monthly Governance Report to interact with customers to discuss findings and resolutions.
- Mentoring the L1 Analysts.
- Tools: QRadar, Demisto and ServiceNow

NTT Ltd., Bangalore, India July 2020 to Current

Senior Associate Security Analyst – Security Event Response Team

- Responsible for monitoring security devices, handling security incidents and health status checks of the security devices and handling suspicious alerts in the client network.
- Perform duties and tasks for clients as part of a cross-functional team related to:
  - Setup, configure, and monitor services
  - Triage, analyse, scan, and troubleshoot as needed
  - Notify, escalate or resolve alerts or incidents
- L1 triage for Device Management, Threat Detection, ESM
- Contribution to preparing SOC documents including SOP, internal playbook, and other process related documents.
- Tools: Splunk, ScienceLogic SL1, RestorePoint, Carbon Black

PERSONAL PROJECTS/ INTERESTS

ATtiny85 Rubber Ducky

The Attiny85 Rubber Ducky acts like a keyboard when plugged into any unlocked device, allowing it to perform various tasks through programmed malicious payloads. The Rubber Ducky injects keystrokes to the host machine when inserted through a USB port.
Project Repository: ATtiny85 Rubber Ducky

CTF Challenges

Actively take part in various CTF challenges (TryHackMe, HackTheBox).

PERSONAL INFORMATION

- Name: Harshil Gupta
- DOB: 5th October 1996
- Sex: Male
- Nationality: Indian
- Blood Group: B^{+ve}
- Linguistic Ability: English, Hindi and Kannada
- Current Location: Bangalore, Karnataka

DECLARATION

I hereby declare that the above written particulars are true to the best of my knowledge and belief.