**Harvijaysinh D Gohil**

**SR. CYBER SECURITY ANALYST (SOC)**

+91 9925281818 [hdgohil@gmail.com](mailto:hdgohil@gmail.com)

# Summary

* Having 13 + years of experience in IT including 9+ years of experience in Cyber Security/SOC Domain.
* Solid understanding of common network, security & system concepts and protocols.
* Good knowledge on cyberattacks and attack vectors.
* Working level knowledge on Incident Response, MS Defender Endpoint(EDR/XDR),Dark Web Monitoring, VAPT, Security solutions like Antivirus, Firewall, IDS/IPS, Email Gateway ,Threat intelligence , VA Scanners
* Strong hands-on experience in security management tools like Splunk Security Incident and Event Management (SIEM),Incident Response, Malware And Phishing Analysis, Endpoint Security, email security ,Cyber Security Awareness Training
* Basic Knowledge and understanding about MITRE ATT&CK frameworks/Cyber Kill Chain Process,
* Exposure to related areas of cyber security including Host Security, Network Security, Vulnerability Management, Penetration Testing, Managing DLP Alerts.
* Capable of independently learning new technology by utilizing available documentation and vendor support resources.

# Tools & Technologies

* + SIEM (Splunk)
  + Incident Response
  + MITRE ATT&CK /Cyber Kill chain
  + Virus total, IBM X-Force
  + Dark Web Monitoring,
  + JIRA
  + MS Defender for Endpoint(EDR)
  + Phishing Email Analysis

# Certifications

* + SOC Expert Certified
  + Information Security & Ethical Hacking(IADL,USDLA)-New Delhi
  + CCNA & Computer Hardware(BASIC)
  + Malware Analysis
  + Tenable Nessus
  + Cyber Threat Intelligent
  + Mxtoolbox
  + Opensearch
  + OSINT tools
  + KnowBe4 Tool
  + Servicenow

# Education

* Master of Science in Information technology –MSC IT-2013
* Bachelor of Computer Application –BCA-2010

# Work History

## 

**Incident Response Analyst in SAP at NTT Data Business Solutions| Dec 2023 – Till Date(Remote from India)**

## Actively monitor and respond to security alerts for cloud-hosted products to identify and mitigate potential threats.

## Investigate security alerts and work with the Central Security Operations Center (SOC) team to triage and respond to security incidents.

## Perform proactive basic threat hunting using the SIEM tool to identify indicators of compromise (IoC) and anomalous behaviour across the network and endpoints.

## Conduct vulnerability management and implement remediation measures to enhance product security.

## Provide customer support through ticketing systems, addressing both security and non-security queries.

## Collaborate with the Product Security and Response Team (PSRT) to ensure effective incident management and resolution.

## Deliver training sessions to new team members to strengthen their understanding of security protocols and processes.

## Prepare and submit monthly security reports to the BISO,PASO and Lead Manager, ensuring transparency and accountability.

## Develop and deliver cybersecurity awareness Campaign training programs for employees..

## Utilize SIEM Splunk for log analysis and threat detection to support proactive security measures.

## Report directly to the Lead Manager, maintaining alignment with organizational security objectives.

## Working in a 24/7 rotational shift model to ensure continuous monitoring and response capabilities.

* Participate in daily shift handovers to ensure that ongoing incidents are effectively.

## Hyfun Foods pvt ltd

**Assistant Manager-Cyber Security Analyst | March 2023 – May 2023**

* One of Function as an information security interface in between internal leads and business units and reporting to CTO(Chief technology Officer)
* Monitor and maintain the security of endpoints (workstations, servers, mobile devices) across the organization..
* Managing firewalls to protect against unauthorized access, network attacks
* Install and configure security software, such as antivirus and endpoint protection tools.
* Investigate and respond to any security incidents or breaches involving endpoints.
* Work closely with our technology teams (IT infra , Cloud Operations, R&D, etc.) to establish and optimize internal processes.
* Skilled in deploying and maintaining intrusion detection and prevention systems (IDPS) to detect and block potential network attacks, malicious activities, and suspicious traffic patterns. Monitor firewall logs and traffic patterns to identify potential security risks and anomalies.
* Establish and maintain an incident response plan to effectively handle and mitigate security incidents Plan.
* Analyze and investigate suspected phishing emails or other social engineering attacks.
* Lead incident response efforts, including containment, eradication, and recovery. Conduct post- incident analysis and provide recommendations for process improvements and preventive measures.
* Develop and deliver cybersecurity awareness Campaign training programs for employees. Create educational materials, presentations, and interactive workshops to promote cybersecurity best practices.

## 

## Krish Media and Marketing US CLIENT |

## Cyber Security Consultant SOC Analyst| OCT 2016 – Dec 2022

* Deep dive analysis of triggered alerts using SIEM and other analysis tools
* Investigate and respond to security incidents escalated from Level 1 Analysts or detected by security monitoring tools. This involves analyzing logs, network traffic, and security alerts to determine the nature and extent of the incident.
* Monitor security alerts and events generated by various security tools, such as firewalls, intrusion detection systems (IDS), antivirus, and log management systems, Also Monitor, Verify and remediate dark web activity using Intsight tools
* Execute predefined incident response procedures for known and low-level security incidents. This may include isolating affected systems, blocking IP addresses, or following other response protocols.
* Perform basic malware analysis to understand the nature and behavior of malicious files and assist in developing appropriate responses.
* Performing the Monitoring ,Alert Detection and Alert Response -Triage security events and incidents, detect anomalies, and report remediation actions including Phishing and Malware Analysis.
* Worked on SIEM Tool for analyze, monitor, extract data from any log that has been indexed in Splunk indexer. I can process any log and based on the log can make various reports, alerts, and dashboards in Splunk. Configure Splunk Indexer, Universal Forwarder. Monitor log from Servers.
* Assist in conducting regular vulnerability assessments and coordinate with IT teams for timely patch management and vulnerability remediation. Review and manage DLP alerts.
* Leverage threat intelligence to stay ahead of emerging threats and incorporate this knowledge into incident response strategies. Document detailed incident investigation reports, including the analysis, response actions taken, and recommendations for future improvements.
* Create and manage incident tickets response plan in the incident tracking system to ensure all incidents are documented and properly tracked throughout the resolution process. Follow-up with different team for remediation
* Participate in shift handovers to ensure that ongoing incidents are effectively.

## ACSG Homeland Security |Information Security Consultant| Feb 2015 – Sept 2016

* + Worked in a 24x7 Security Operation center (SOC) environment
  + Handling escalated alerts L1 Security Analysts
  + Investigating incidents, remediation, tracking and follow-up for incident closure with concerned teams, stakeholders
  + Advise incident responders on the steps to take to investigate and resolve computer security incidents.
  + Onboarding log source using different collection methods
  + Actively involved in threat hunting activities from building hypothesis to finding evidence and enhancing security controls and detection logic
  + Review security alerts generated by various security systems and tools, such as firewalls, intrusion detection systems, and antivirus software.
  + Investigate the incident to determine its nature and scope. This may involve reviewing logs, analyzing network traffic, or consulting with other teams.
  + Continuously monitor the organization's security systems to detect potential security incidents and to ensure that the systems are functioning as intended.
  + Assist in managing and maintaining security tools and technologies used in the SOC, ensuring they are up to date and functioning correctly.
  + Collaborate with other teams, work closely with other teams, such as network operations, incident response, and security engineering, to ensure a coordinated and effective response to security incidents.
  + Maintain detailed records of security events, incidents, and actions taken during incident response in the incident tracking system.
  + Provide security training to users and other members of the organization to educate them on best practices for information security.
  + Use various tools to scan the target systems and applications for known vulnerabilities and weaknesses.
  + Document incidents in detail, including their cause, impact, and resolution. This documentation will be used to inform future incident response efforts and to improve the organization's overall security posture.
  + stay up to date with the latest attack techniques, tools, and best practices, and continuously Improve their skills and knowledge.
  + Participate in shift handovers to ensure that ongoing incidents are effectively

## HCL Infosytem Ltd |Tech Support Engineer| March 2011 – Aug 2014

* + Monitor the organization's security systems, including firewalls, intrusion detection systems, and antivirus software, to ensure that they are functioning properly and alerting on any potential security incidents.
  + Investigating security incidents, If security incidents are detected, responsible for investigating them to determine their nature and scope, and taking action to contain and resolve them.
  + Responsible for installing software updates, patching systems, and ensuring that all systems are running the latest security software and firmware.
  + Collaborating with other teams, work close such as network operations, incident response, and development teams, to ensure that the organization's security posture is aligned with the overall goals and objectives of the organization.
  + Documenting security incidents, including their cause, impact, and resolution, and using this information to improve the organization's security posture.
  + Provide technical assistance to users with hardware, software, and network-related issues. This may include installing software, configuring devices, and troubleshooting network connectivity issues.
  + Setting up and configuring new laptops and desktops as per client requirement
  + Monitoring and Administration of the IT Infrastructure like Laptop, Desktop & Printer, Installation, and configuration of Windows and Linux Operating System
  + Providing training and guidance to users on how to use security systems and software, and best practices for information security.