

Curriculum Vitae

Nitu Kumar Sharma

Mobile: +91-9773780706

Email: nitusharma_coxhockey@yahoo.com



OBJECTIVE

To secure a position with a stable and profitable organization, where I can be a member of a team and utilize my business experience to the fullest.

PROFESSIONAL EXPERIENCE

- ✓ Working with **Aexonic Technologies Ltd.** as **Sr. Analyst Information Security** from **17th Nov 2023 till date.**
- ✓ Worked with **Evolent Health International Pvt. Ltd.** as **Analyst, Incident Response (Information Security)** from **11th May 2020 to 3rd Jul 2023.**
- ✓ Worked with **Rattan Enterprises (A division of R4 Solutions INC)** as **Security Analyst** from **21st May 2018 till 10th May 2020.**
- ✓ Worked with **HCL Technologies LTD.** as **Specialist (Coles Supermarkets)** from **7th Apr 2011 to 29th Sep 2017.**
- ✓ Worked with **iYogi Technical Services** as **Technical Specialist** from **Dec'2010 to Mar'2011.**
- ✓ Worked with **Wipro Infotech** as **Engineer Helpdesk Management** from **Apr'2008 to Dec'2010.**
- ✓ Worked with **Maruti Udyog Ltd.** as **Service Desk Analyst**, Represented HP (New Horizons CONSULTANCY) for **6 months.**
- ✓ Worked with **Magus Customer Dialogue** as **Customer Dialogue Executive (From Feb 2005 to Feb 2006)**

Technical Qualification:

Trained on **ArcSight (Administrator & Analyst).**

Trained on **Splunk Fundamentals 1&2.**

Trained on **Splunk Enterprise Security.**

Certified Information Security Manager (CISM)

Roles and Responsibilities



- ❖ Monitoring, Investigating, and analyzing the real-time security events on CrowdStrike and Rapid7 console.
- ❖ Involved in SOC operations such as log monitoring, log analysis, responsible for identifying the compromised attempts in client networks.
- ❖ Review the case creations and resolving the tickets based on playbooks.
- ❖ Understanding the different playbooks while ticket creations.
- ❖ Working on the incidents and providing feedback in client meeting for P1, P2 tickets.
- ❖ Analyzing the real time events for both network and security logs using CrowdStrike and Rapid7 tool.
- ❖ Investigating the security incidents by fetching the Risk Report and Computer status report from Rapid7.
- ❖ Good experience on handling the Phishing mails and raising the ticket if required.
- ❖ Providing deep investigation for all the alerts by analyzing.

- ❖ Good understanding on different types of attacks.
- ❖ Handling the client meetings and escalating the issues if necessary.
- ❖ Good Knowledge on preparing reports like Daily and Weekly as per client requirements.
- ❖ Good experience on ticketing tools such as Service now, Fresh service and Jira for ticket creations



Roles & Responsibilities

- ❖ Worked with SOC, including event monitoring which includes incident detection, tracking and analyzing on a real-time basis, and report generation.
- ❖ Providing effective security incident response for various clients by analyzing security events and identifying any security breach
- ❖ Managing the Information Security Operations for multiple clients based on Internal and External Frameworks
- ❖ Analyzing suspicious logs collected by various devices such as Firewall, IDS, IPS, and Windows Server and reporting them to the device owners.
- ❖ Trend Analysis of security events that occurred and identifying the root cause to reduce the number of security events.
- ❖ Created of CSIRT process or framework in Information Security.
- ❖ Created Standard Operating Procedures for SOC & CSIRT.
- ❖ Threat Hunting includes Analyzing logs, network traffic, and security data from various sources to identify anomalies or patterns that may indicate potential threats.
- ❖ Continuously monitoring security dashboards and tools to identify suspicious activity in real-time.
- ❖ Actively investigating and validating security alerts, incidents, or anomalies to determine their nature, scope, and impact.
- ❖ Collaborating with other SOC team members and relevant departments to gather additional context and information.
- ❖ Using various security tools and technologies, such as SIEM (Security Information and Event Management), EDR (Endpoint Detection and Response), network monitoring tools, and threat intelligence platforms, to assist in threat hunting activities.
- ❖ Collaborating with incident responders, IT teams, and other stakeholders to coordinate response efforts when a threat is identified.
- ❖ Collaborating with incident response teams to assist in the mitigation of identified threats and vulnerabilities.
- ❖ Monitor events, Logs analysis and Investigate incidents on a daily basis.

- ❖ Monitoring event which includes incident detection, tracking and analyzing on real time basis, report generation.
- ❖ Microsoft Azure alert monitoring.
- ❖ Built the Cyber Security Incident Response Team to handle Security Incidents.
- ❖ Collecting, aggregating, and indexing security-related data and logs from various sources into Splunk. This may include logs from firewalls, IDS/IPS, antivirus, endpoints, and more.
- ❖ Continuously monitoring the Splunk console for real-time alerts and anomalies, such as suspicious network traffic, system logins, or abnormal user behavior.
- ❖ Reviewing and triaging alerts generated by Splunk, assessing their severity, and taking appropriate actions, including escalating incidents if necessary.
- ❖ Incident Investigation: Conducting in-depth investigations into security incidents and breaches using Splunk to analyze historical data, identify attack vectors, and understand the extent of the compromise.
- ❖ Designing and customizing dashboards and visualizations within Splunk to provide real-time visibility into security posture and trends for SOC personnel and management.
- ❖ Proactively searching for signs of advanced threats or vulnerabilities within the organization's data using Splunk, often through the process of threat hunting.
- ❖ Prioritizing and categorizing security alerts based on their severity, potential impact, and relevance to the organization
- ❖ Managing the onboarding and configuration of new log sources or devices into Splunk to ensure comprehensive visibility.
- ❖ Log Analysis includes Collecting and ingesting logs from various sources, including firewalls, IDS/IPS, antivirus software, servers, network devices, and applications into the SIEM (Security Information and Event Management) system.
- ❖ Continuously reviewing logs and events generated by various systems to identify suspicious or anomalous activities.
- ❖ Scanning logs for security events, such as unauthorized access attempts, malware activity, and unusual network traffic.
- ❖ Monitoring security alerts and notifications generated by the SIEM or other security tools. Prioritizing alerts based on severity and potential impact.
- ❖ Policy Management (Policy modification & renewal etc.)
- ❖ Working on phishing mail analysis.
- ❖ Escalate issues as per the escalation matrix to the operation heads or senior authorities for faster and better resolution.
- ❖ Imparting Training and organizing training for Information Security Team.



Day-to-Day Activities:

- ❖ Managing a Team of 10 members. Creating/modifying Process documents for team and client.

- ❖ Mentoring new joiners to bring them on par with tenured engineers.
- ❖ Managing Shift management for team members and people management.
- ❖ Taking part in daily, weekly, and monthly meetings with clients and process owners/teams.
- ❖ Preparing daily dashboards/reports and sharing them with clients in weekly meetings.
- ❖ Manage 24x7 operations at SOC, including event monitoring which includes incident detection, tracking and analyzing on a real-time basis, and report generation.
- ❖ End device integration with ArcSight. (Baselining, Logging, Communication)-Entry Level.
- ❖ Basic Implementation of Smart Connectors, Custom Queries, Filters, Rules, Active Channels, Dash Boards.
- ❖ Monitor events, Log analysis, and Investigate incidents on a daily basis.
- ❖ Escalate issues as per the escalation matrix to the operation heads or senior authorities for faster and better resolution.
- ❖ Having a basic idea of the Installation and Integration of smart connectors.
- ❖ Malware Analysis includes monitor alerts and logs to detect indicators of malware infections within the organization's network and endpoints.
- ❖ Collect relevant logs and data from infected endpoints and network traffic to facilitate malware analysis.
- ❖ Identify and classify malware strains and families to understand their behavior and potential risks.
- ❖ Perform static and dynamic analysis of malware samples to determine their functionality, attack vectors, and capabilities.
- ❖ Analyze malware code, behavior, and communication patterns to assess the level of threat posed.
- ❖ **SIEM Tool: HP Arc Sight SIEM 6.11 (Security Information and Event Management).**

EDUCATION

Ch.Charan Singh University, Meerut, Uttar Pradesh, India
Bachelor of Arts March 2004

LANGUAGES

English – Excellent reading, writing and speaking
Hindi – Excellent reading, writing and speaking

THANKS

Nitu Kumar Sharma