Subhash Huchagond

SOC Team Lead

+91 9096180995
huchsub@gmail.com

AREAS OF INTERESTS:

- Incident response.
- Threat Hunting.
- Threat Intelligence.
- Splunk Engineer.
- Malware Analysis.

CERTIFICATIONS:

- CompTIA Cyber Security Analyst +
- Splunk Core Certified Power User.
- Azure Fundamental (AZ-900).
- Azure Security Engineer (AZ-500).
- Qualys VM Certification.

EXPERIENCE:

- NTT India GDC Private Limited:
  SOC team lead
  Mar 2022 - Till Date

- Accenture Private Limited:
  Senior Security Analyst
  Nov 2018 – Mar 2022

- Tata Consultancy Services:
  Senior Security Analyst
  Feb 2014 – Nov 2018

- Infosys Private Limited:
  Technical Support Executive
  May 2012 – Feb 2014

EDUCATION:

Bachelor of Computer Application.
From Shivaji University | 2011

PROFESSIONAL SUMMARY

- Overall, 10 years of experience as SOC Team Lead and Analyst, Incident Responder and Splunk Engineer.
- Able to lead the team independently with little support.
- Hands on experience on various SIEM tools like Splunk, SecureWorks Portal, SAP ETD, ArcSight.
- Hands on experience of Splunk implementation and managing the Splunk ESM platform.
- Threat & Incident management handling skills, including knowledge of common probing and attack methods, network/service discovery, system assessment, viruses, and other forms of malware.
- Good understanding of security controls and best practices to secure various platforms (i.e., network, operating system, databases, application layers, endpoint).
- Knowledge of confidentiality of information, privacy protection, data security and other important information security fundamentals.
- Good understanding of the following technologies: MITRE ATT&CK, Vulnerability Management, SOAR, UEBA, SIEM, Information Security, E-mail and Web Gateway, Encryption, IPS and HIPS.
- Ability to carry out the incident analysis and the knowledge of incident response life cycle.

TOOL EXPOSURE:

SIEM	:	Splunk ESM, SAP ETD, ArcSight
End point Security	:	Crowdstrike EDR, Defender ATP (Security Centor)
Analysis Tool	:	IPVoid, VirusTotal
Ticketing Tool	:	SNOW
SOAR	:	Demisto
Email Security	:	Proofpoint

Roles And Responsibilities

SOC Team Lead(L3):	• Assisting in building SOC workflow, processes, and procedure. • Ensuring alerts/investigations are assigned and processed within SLA time. • Working with management to develop information security policies, standards, procedures and guidelines across multiple platform and application environment. • Assisting with development of meaningful security metrics. • Coordinate, plan, and execute change management procedures. • Ensuring quality of service by validating proper execution of SOPs for the respective alerts/investigations. • Managing the load/distribution of alerts/investigations among the analysts. • Informing team members if someone is missing the shift due to sickness or other reasons and this affects shift coverage. • Recording lessons learned to improve the quality and performance. • Assisting pattern improvement of existing correlation pattern or recommending new pattern.
Incident Monitoring and Response:	• Monitoring alerts received from the SIEM tool and take appropriate action based on the defined processes. • Developed Standard Operating Procedures (SOP) for incident remediation. • Perform analysis of security logs and offences generated by SIEM to pinpoint potential points of attack. • Fine tuning of existing SIEM rules to reduce false positives and creation of new rules from new use cases. • Provide sound recommendations to remediate or reduce security risks. • Security Implementation and Enhancement as per Architecture across regions. • Tracking, coordination, and escalation of security events to relevant teams in organization. • Ensure timely preparation / escalation of Incident Reports in collaboration with risk, assessment, and design teams in information security. • Perform security reviews and identify security gaps in security architecture, resulting in recommendations for the inclusion into the risk mitigation strategy. • Creation and managing of reports (SLA, KPI), dashboards, metrics for SOC operations and presentation to Management. • Weekly walk-through of latest attack trend, IOCs and TTPs to the team. • Engage with vendor support to troubleshoot issues with SIEM platform.
Splunk Support Engineer:	• As Splunk Engineer, takencare of the health checks, updates and developed Splunk content (reports, dashboards, correlation rules, queries etc.) as per business needs/ customer requirement. • Reporting/Analysing the license usage of Splunk on a regular basis. • On- Boarding data sources into Splunk as expanding SIEM monitoring scope. • Real time monitoring in Splunk by active channel, Analysis of events/ Offenses and act as per Criticality/impact to respective teams/business units.