KARTIK YADAV

Kartik1902@gmail.com | +91- 9999097567 | Sec-51, Gurugram, Haryana, 122003
www.Kartik1902@gmail.com

SUMMARY

A meticulous engineer and a cybersecurity enthusiast, diversified at solving multiple tasks and working under pressure, experienced with excellent customer finesse, and a voracious cyber event reader.Adept with technology, and client business demands. An individual focusing on the redressal of malicious events and building a good rapport with the client, and providing a responsive environment for rectifying illegitimate cyber activities with robust solutions.Strong organizational skills coupled with leadership roles and an excellent driven communication to accelerate office activities and facilitate smooth workflows.

WORK EXPERIENCE

Cybersecurity operations engineer, (NOKIA) **(March 2024 - Present)**

- Worked on splunk (SIEM) and splunk enterprise security.
- Worked on Falcon crowdstrike (EDR) dashboards.
- Proficient in BMC (IT) ticket management generation.
- Worked on Alog requests and gave affirmation for online and offline hosts on EDR.
- Improvised and incorporated new splunk queries and usecases.
- Worked on database of identity SSO portal.
- Worked on SIEM Qradar.
- Worked on sentinel (SIEM+SOAR) cloud native solution workspace.
- Worked on NDR tool (Seceon) monitoring and alerting via RDP.
- Worked on python to incorporate new automation in splunk reports.
- Guided and supported team members and helped them in grasp things in SOC via KT sessions and inperson discussions.

Higher Cybersecurity certifications preparations. **(May 2023 - Dec 2023)**

- ISC2 certified cyber defence analyst.
- CEH certified by ECCOUNCIL.
- Splunk certified security operations and the defence analyst
- Splunk certified basics of security
- Comptia CYSA+ certified.

Cybersecurity operations analyst, (VTPL Solutions) **(Dec 2020 - April 2023)**

- Supported senior team members with splunk usecases, attending meetings, handover reports, fostering effective communication and preparing dashbord reports.
- Taking followups/reminders of different tickets and worked on different usecases via interacting with engineering and build teams and worked on multiple IR plans of different usecases.
- Worked on syslog and alog requests from the node owner.
- Assisted in the beaking down of different queries, took initiative to participate in client meetings, ensuring a high level of professionalism and meticulously discussing new plans to help run the soc operations smoothly.
- Suggesting different ways to remove obselete false positive cases.

EDUCATION

Bachelor's of Technology (2016-2020) **(Jan 2019 - Feb 2021)**

- Northcap University, Gurugram Haryana

(10+2) High school certification **(April 2014- May 2015)**

- Rishikul senior secondary school

10th Matriculation **(April 2013- May 2014)**

- Colonel's central academy

KEY SKILLS

- Comptia Security +
- SIEM:Mcafee, Splunk, Sentinel.
- EDR: Crowdstrike in 24/7 SOC environment. Exposure to the basic functioning of various tools such as (SIEM, EDR, OSINT and SNOW) in SOC and mitigation.
- Creating an investigation report, daily and weekly dashboards.
- Network detection and response (NDR) on seceon tool.
- Hands on experience on BMC IT ticketing tool and service management.
- Knowing about SSO identity portal of Airtel.
- Following up on the incident response lifecycle.
- Proficient Communication Skills
- Certified in Cybersecurity (CC) from ISC2, Certified in Ethical Hacking (CEH) from EC-Council, Splunk Certified E-learner, Splunk Certified Security Operations and the Defence Analyst, CompTIA CySA+ certified.

ACHIEVEMENTS

- CBSE zonal district level participation competition in basketball.
- Cleanliness campaigns in college.
- Debate and extempore participation in college organised by ministry of jal shakti..
- Fashion show participation for three consecutive years (2016-2018).

LANGUAGES KNOWN

- English
- Hindi