Swapnil Kshirsagar

Security Analyst

Email:swapnilks6783@gmail.com

LinkedIn: linkedin.com/in/swapnil-kshirsagar-95049a331

Contact Number: +91 9623514767

Kolhapur,Maharashtra,416211

Objective -:

To give my career in the IT Industry and to work as a positive catalyst in a challenging environment for the growth of the organization and with the Development of my career. Dynamic and result oriented Security Analyst experience in the Security Domain.

Skills -:

- **SIEM -** Splunk & QRadar
- **EDR -** Sentinel One
- **Ticketing Tool -** ServiceNow
- **Good knowledge of Reference Set, Active list, Rules & IOCs configuration in SIEM.**
- **Phishing & Email Analysis -** Proofpoint
- **Suspicious File Analysis, Antivirus Incident Response**
- **Security Monitoring Enterprise Security**

Experience -:

Security Analyst at OpenView Technology Pvt. Ltd. Pune,India
Dec 2022 - Present

- Good experience in SIEM tools Splunk,QRadar & EDR tool Sentinel One.
- Monitor and manage SIEM setup, which includes ESM, logger, and connectors.
- Preparing daily, weekly, and monthly reports as per client requirements.
- Investigating and creating a case for the security threats, and forwarding it to the concerned team for further consideration, investigation, and action.
- Performing log analysis and analyzing the crucial alerts on an immediate basis.
- Filling the Daily health checklist.
- Preparing reports as per client request, preparing knowledge base and use cases.
- Reporting weekly / monthly dashboards to customer.
- Recognizing attacks based on their signatures.
- Knowledge on security vulnerability assessment.
- Having knowledge in device integration.
- Proficient in identifying, analyzing, and containing security breaches, with a focus on minimizing.
- Organizational risk and ensuring regulatory compliance.
- Skilled in utilizing incident response frameworks and tools to swiftly detect and respond to threats, while
- Maintaining the integrity of systems and data.
- Adapt at coordinating with internal teams and external stakeholders to implement remediation measures and strengthen incident response capabilities.

Education -:

- Dr.D.Y.Patil Prathishthan's College of Engineering, Salokhenagar, Kolhapur--------- March 2020
  Bachelor of Engineering: Computer Science & Engineering

- Dr.A.D.Shinde Institute of Technology, Gadhinglaj, Kolhapur----------March 2017
  Diploma: Information Technology

Roles & Responsibilities -:

- Working in Security Operation Centre (24x7), monitoring of SOC events, detecting and preventing the Intrusion attempts.
- Responding to various security alerts, incidents for various clients.
- Monitoring real-time events using SIEM tools like Splunk, Qradar tools.
- Monitoring of SOC events, detecting and preventing the Intrusion attempts.
- Collecting the logs of all the network devices and analyses the logs to find the suspicious activities.
- Investigate the security logs, metigation strategies and Responsible for preparing generic security incident report.
- Having experience on Sentinel One EDR solution as anti-virus and involved in the IOCs management.
- Handling Alerts from multiple Security Log sources such as Proxy, Anti-Virus and EDR.
- Investigate the security logs, mitigation strategies and responsible for preparing generic security incident reports.
- Responsible to preparing the root cause analysis reports based on the analysis.
- Analyzing daily, weekly and monthly reports.
- Website Anti-Malware and Defacement monitoring and real-time alerting based on anomalies detected.
- Troubleshooting SIEM dashboard issues when there are no reports getting generated or no data available.
- Monitoring of SOC events, detecting and preventing the Intrusion attempts.
- Investigating the events based on particular criteria by creating an Active Channel.
- Handling the failed logins issues from the different systems.
- Using Service Now to handle & track al kind of incidents.
- Coordinates with all the teams to Mitigate/Remediate the issue.

Declaration -:

I hereby declare that the above-mentioned information is correct up to my knowledge and I bear that responsibility for the correctness of the above-mentioned particulars.

Swapnil S. Kshirsagar