

Resume

Aditya Gajanan Dandge.

Mobile No : - +91 9075675741

E-Mail Id : - adityadandge2@gmail.com

Career Objective:

To leverage my skills in cybersecurity and threat analysis to monitor, detect and mitigate security incidents in real time. Dedicated to safeguarding organizational assets by employing advanced tools and techniques, enhancing incident response strategies and contributing to a secure IT environment through proactive threat management and continuous learning.

Professional Summary:

- **SIEM Tools:** Splunk and Splunk Enterprise Security.
 - **Vulnerability Management:** Nessus.
 - **Incident Analysis Tools:** CISCO Talos, Mx Toolbox, Virus Total, IBM-XForce etc.
 - **Ticketing Tool:** Service Now.
 - **Certification:** Certified SOC Expert,CTI, CEH.
 - **EDR Crowdstrick.**
 - **XSOAR.**
-
- A competent professional with **8 Months** of experience in Worldsec technologies Pvt. Ltd as **Security Analyst Intern.**
 - A competent professional with **6 Months** of experience in CyberVault Securities Solutions Pvt. Ltd. as **SOC Analyst L1.**
 - Cyber Security Analyst with proficient and thorough experience and a good understanding of information technology. Specialized in proactive network monitoring of SIEM.
 - Good understanding of security solutions like Anti-virus, Firewall, Sentinel, IPS/IDS, Email Gateway, Proxy etc.
 - Hands on experience with Splunk SIEM tool for logs monitoring and analysis, using Service Now ticketing tool for incidents response.
 - Good knowledge on networking concepts including OIS Model, TCP/UDP,IP, Ports, DNS etc.

Organizational Experience:

1. **From Oct 2024 To May 2025 in Worldsec Technologies Pvt. Ltd. as Security Analyst Intern.**
2. **From June2025 To Till Now in CyberVault Securities Solutions Pvt. Ltd. as SOC Analyst L1.**

Job Responsibilities:

- Working in a 24x7 Security Operations Center.
- Monitoring the customer network using Splunk SIEM.
- Act as first level support for all Security Issues.

- Analyzing Realtime security incidents and checking whether its true positive or false positive.
- Performing Real-Time Monitoring, Investigation, Analysis, Reporting and Escalations of Security Events from Multiple log sources.
- Raising true positive incidents to the respective team for further action.
- Creating tickets on service now and assigning it to the respective team and taking the follow-up until closer.
- Escalating the security incidents based on the client's SLA and providing meaningful information related to security incidents by doing in-depth analysis of event payload, providing recommendations regarding security incidents mitigation which in turn makes the customer business safe and secure.
- Contacting the customers directly in case of high priority incidents and helping the customer in the process of mitigating the attacks.
- Work closely with business units to ensure that they know what and how to feed data into the SIEM.
- Co-ordinate with networking teams to maintain and establish communication to remote ArcSight Connectors.
- Investigate malicious phishing emails, domains, and IPs using Open-Source tools and recommend proper blocking based on analysis.
- Good knowledge of Splunk Distributed cluster Architecture.
- Detail knowledge of the working functionality of various components of Splunk such as Indexer, Search head, Heavy forwarder, deployment server etc.
- Experience in onboarding of data sources with Splunk such as Windows, Linux, Fortinet Firewall etc.
- Installing Splunk apps and Addon on the Splunk.
- Experience in installation of Universal forwarder on the servers for logs collection.
- Responsible for upgrading the Forwarders to the newer versions.
- Doing the troubleshooting in case any device is not reporting to the Splunk.
- Knowledge of Creating dashboard, Reports in Splunk.
- Knowledge and experience in creating Correlation Searches/Rules in Splunk.
- Working experience searching and Reporting in Splunk having good SPL knowledge.
- Excellent Hands on experience on Crowdstrike EDR module.
- Sound knowledge in handling the detections.
- Good at using performing the searches and building up the report and dashboards.
- Good at understanding sandboxing reports.
- Good at creating the policies and managing them.
- Better understanding on EDR and its operation.
- Investigated and resolved 100+ security incident monthly using XSOAR, reducing mean time to respond by 25%.
- Enriched alerts with threat intelligence feeds (e.g. Virus Total) in XSOAR improving incident context and accuracy.
- Executed and monitored automated playbooks for malware containment, endpoint remediation, and phishing analysis.
- Reduce incident response time by 30% through the effective use of XSOAR playbook and

automation.

- Improve the efficiency of incident response by using XSOAR to automate containment and remediation steps.
- Improved the accuracy of incident investigation by leveraging XSOAR enrichment capabilities.
- Executed playbooks to automate containment and remediation steps, reducing manual effort by X hours per week.

Education:

Qualifications	Board/ University	Year
B.Sc. (computer Science)	SGB Amravati University	2023
H.S.C. (Science)	SGB Amravati University	2017
S.S.C.	SGB Amravati University	2015

Personal Details:

- **Name** : Aditya Gajanan Dandge
- **Date Of Birth** : 09/01/2000
- **Nationality** : Indian
- **Marital Status** : Unmarried

Declaration: I Here declare that the above given information is correct to the best of my knowledge and belief.



(Aditya Dandge)