

# ASHISH MARUTI DORUGADE

Security Analyst

✉ [ashish.dorugade11@gmail.com](mailto:ashish.dorugade11@gmail.com)

☎ 9970854368

📍 Gadhinglaj Dist-Kolhapur

📅 11/03/1990

🇮🇳 Indian

💍 Married

## 📄 Summary

As a Security Analyst with 8 years of experience in the field of (Security Operations Center) SOC team, specializing in working on multiple EDR solutions and have good exposure to SIEM platform. I have leveraged these tools to proactively detect and mitigate a range of threats including advanced threats such as malware, ransomware, lateral movement, and network attacks. Additionally, I have handled threat escalations, collaborating with senior colleagues to investigate and resolve complex security threats. I have also played a role in training and mentoring new team members, sharing my knowledge and expertise in EDR solutions and good exposure of security information and event management (SIEM) platform.

## 📄 Skills

EDR Tools - Hands on experience on EDR tools Sentinelone.

SIEM Tool - Hands on experience on Eventracker & Pearch.

SME - Working as SME(Subject Matter Expert)

Calls - Inbound & Outbound Calls to US/UK Partners

Tools - Working on Ticketing tools like Freshdesk & JIRA

Analysis - Investigating on Alerts and notifying the partners with the mitigation steps.

## 📄 Certifications & Trainings

### **Certified Ethical Hacker (CEH)**

CompTIA Security+ (Training done)

CCNS V. 6 (CMS Certification A+ & N+) from CMS Training Institute

**Microsoft Certified Information Technology Professional (MCSA) in Windows Server 2008.**

- 70-640 Server 2008, Active Directory, Configuring.
- 70-642 Server 2008, Infrastructure Services, Configuring.
- 70-646 Server 2008, Server Administrator.

## 📄 Educational Qualification

- Bachelor of computer application(BCA) 2013, karnatak university, dharwad.

## 📄 Professional Experience

**Security Analyst, Connectwise Pune, Jul/2017 to Current.**

- Part of Global SOC team monitoring over 2 million endpoints across different organizations, initially utilized separate EDR solutions Hands-on experience on EDR (SentinelOne) & SIEM Tools Perch
- Detailed Email Header Analysis for phishing email detections to stop the cyber-attack in its initial phase as most cyber-attacks are initiated by phishing email.
- Investigation and analysis of threats and attacks using various tools.
- Handling Alert Call Escalations at Level 1 and taking necessary actions, and if necessary, escalating it to next level.
- Take appropriate mitigations actions based on alert type and severity.
- Analysed and investigated security alerts, reducing false positives, and enhancing the accuracy of threat detection by Blacklisting and whitelisting hash value, URL's and file paths as per the analysis and partner approval.Skilled in incident response processes, including triaging alerts, investigating security incidents, containing threats, and coordinating with Level 3 analysts and client for remediation and resolution.
- SentinelOne agent installation and testing for Windows.

**Desktop support Engineer, Progressive Infovision Pvt. Ltd | New Delhi.**Sep/2015-Jul/2017

- Software and network technical support to Varroc Engineering(Wipro client) end users.
- Assembling of computer, Installation of Operating Systems and other software.
  
- Prioritizing user satisfaction by timely response to mails and calls. Seek support from Team Lead or Manager for issues requiring further support.
- New user creation, Distribution List, Generic mailbox, External User ID and Guest ID Creation.
- Handling Escalation & Coordination with various levels of support within the organization.
- Managing user access level / Permissions on file server
- Monitoring and ensure the overall assigned tickets (Incidents & Work orders) meet the response and resolution SLAs.

 **Awards**

**Monthly, Quarterly & Yearly Performance, *Connectwise***

I have received multiple awards as a performer.

---

Ashish Maruti Dorugade.