RACSHIT BHANDARI

Email: racshit1234@gmail.com
Phone: 9823395898
LinkedIn: racshit-bhandari
Portfolio: racshit.github.io

SKILLS SUMMARY

- **Tools:** Splunk, MCAS, MDI, MDATP, Azure, Wireshark, MS Intune, Nozomi OT, Carbon Black.
- **Platforms:** XSOAR, Service-Now, Jira, Confluence.
- **Languages:** KQL, SPL, Bash, Python.

EXPERIENCE

- **Computer Incident Response Team*: (Jan 2022-present)***
  - Mitigation of alerts triggered by **SIEM** correlation technologies like Recorded Future and Splunk.
  - Handling incidents ranging from Azure Identity, MDATP, Nozomi OT, Carbon Black, etc.
  - **Remediation** of servers/workstations post confirmed compromise due to a **malware infection** or credential theft.
  - Raising alert tuning requests across several fields for incidents.
  - **Securing** the organization by restricting access to malicious domains via **proxy blocks**.
  - Standardization procedures of systems based on a malware download.
  - **Purging** of malicious emails in the whole organization by a questionable sender for continued security.

  <u>Additional responsibilities</u>:
  - **Interviewed** candidates in the **APAC and US** region for joining the team.
  - **Mentored** new joiners as well as co-workers from other teams on CIRT and Endpoint security.
  - Created several work instructions for **knowledge transfer** to analyst's handling those incidents.
  - **Renovation** of the orchestration platform to make it better suited for an analyst's requirements.
  - Involvement in **automation** of USB rights access and Defender group exception requests.

- **Endpoint Security Team: (*Jan 2021-Dec 2021*)**
  - Incident resolution in Cyber Security operations within **SLA breach** deadline and **CSAT rating**.
  - Experience with MDATP console involving remediation of ASR blocks due to potential security threat.
  - **Granting** USB rights access to several devices all across the company.
  - Splunk **Dashboarding** to provide quick insights about data to several teams.
  - McAfee EPO experience involving application/removal of tags along with pushing FRP keys to endpoint device.
  - Microsoft Bitlocker experience involving **compliance** and recovery key.
  - Server **Patching** and Vulnerability **Management**.

- **Computer science intern at Oracle: *(May 2019 – July 2019)***
  - Ideal Database Management using Exadata Machine.

- **Web dev intern at Selectigence HR Solutions: *(May 2018 – July 2018)***
  - Design and development of company website using front-end technologies.

CERTIFICATIONS

- CompTIA Security+ (SY0-601)
- Implementing the NIST Cybersecurity Framework (CSF)
- Microsoft Cyber Security: Learning Azure Security Center
- Cybersecurity Compliance Framework & System Administration

EDUCATION

Degree	University/school	Year	Percentage/CGPA
B.Tech – Computer Science and Technology with Specialization in Information Security	VIT, Vellore	2017-2021	8.51
12th Grade (Science)	Army Public School Kirkee, Pune	2016-2017	84.8%
10th Grade	Army Public School Kirkee, Pune	2014-2015	9.4

EXTRA CURRICULARS

- VIT Music Club member.
- Coordinator of Publicity and Marketing International Committee (Riviera).
- Coordinator of Simulatown (VIT Spartans).
- An avid gym and outdoor activity enthusiast.

SOCIAL SKILLS

- Extroverted and always looking out for challenges.
- Adaptability and flexibility.
- Team player and managerial skills.