

SIMRAN KAUR BHATTI

ENDPOINT SECURITY CONSULTANT

CONTACT

+91 8433587943

simran.kb589@gmail.com

Ghansoli, Navi Mumbai, India

AWARDS

Highlighted in Client spotlight

Acknowledged and featured in client spotlight for exceptional performance and contributions to endpoint security initiatives.

SKILLS

EDR: CrowdStrike Falcon & SentinelOne Administration and Deployment

AV: Symantec Endpoint Protection & TrendMicro Cloud One Security

Email Security: Symantec Message Lab

OSINT Tools: VirusTotal & MXToolbox

SIEM: Splunk

Key Skills

- Deployment of EDR agents
- Expertise in Sensor communication issues
- Expertise in USB Management
- Proficient in Email security

CERTIFICATIONS

- MICROSOFT AZ-900
- MICROSOFT AZ-500
- MICROSOFT SC-900
- SPLUNK FUNDAMENTALS

Education

Bachelor Of Engineer (IT)
Pillai's College of Engineering, Mumbai
University 2015-2019

PROFILE

CyberSecurity professional with 5+ years of experience seeking a role as cyber security analyst where i can leverage my knowledge of EDR and email security skills.Dedicate to contribute to a dynamic team environment while continuously expanding my skills and staying updated with industry best practices.

WORK EXPERIENCE

Capgemini

March 2020-Present

Associate Consultant

September 2022- Present

- Monitoring and managing CrowdStrike Falcon endpoint security platform , including deployment and maintainance.
- Investigating on alerts to detect potential threats on CrowdStrike console
- Expertise in resolving sensor upgradation and sensor communication problems for hosts.
- Proficient in developing Static/Dynamic Groups and USB management policies in accordance to client requirement.
- Proficient in deploying, configuring and managing SentinelOne EDR solution to safeguard endpoints against advanced threats and malware.
- Worked on Trendmicro CloudOne security for handling non-compliant servers.

Senior Analyst

March 2021-August 2022

- Investigating on blocked emails and analysing the email header on Symantec Message Labs.
- Whitelisting and blacklisting of email addresses and domains on Symantec Message Labs.
- Many times received happy signals from client for solving the blocked emails issue.
- Maintaining 100% compliance of all servers and workstations on Symantec Endpoint Protection.
- Became team lead and managed alerts and threats on Symantec Endpoint.
- Implemented many SIPs for client based on Symantec Endpoint Protection.
- Meeting Service Level Agreements (SLAs) by resolving the incidents and service tasks on time.

Analyst

March 2020-March 2021

- Performing Healthcheck, monitoring the threat events,generating reports on virus and malware infections, and analyzing the data to identify potential security threats on Symantec Endpoint Protection.
- Creating policies and adding exclusions with Client's approval by explaining the issue and requirement to client through email communication.