Designation**-End point Security Engineer**

Total years of work experience**- 2 to 4 years**

Office Location- **Andheri East**.

Office Time-**10.00 a.m - 07.00 p.m**

Working days- **Monday to Saturday full day working, only 03rd Saturday will be full day Off**

Description:-

- The selected candidate will deliver consulting project activities, ranging from client identification through final invoicing through medium to long term engagements requiring varied interpersonal and technical skills.

- Technical responsibilities include problem identification, system architecture definition, hardware/software specification and/or design, implementation, testing, client training, and solution deployment.

- Identify, assess and upgrade customer information technology infrastructure regarding risks and vulnerabilities.

- Document (textual and graphical as appropriate), communicate, recommend and take appropriate action to resolve, risks and issues associated with security vulnerabilities across the Customer IT Environment.

What you will be doing: -

- Install, maintain, stage, automate and operate Security Services (Services, Equipment and Software), including virus Software and definitions/signatures, patches, host-based agents, Data Loss Prevention (DLP), web filtering, spam prevention and other Monitoring software, based upon supplier version release keeping the Customer IT Environment updated at N Release Level at all times, subject to Customer-approved waivers.
- Perform e-mail security management, with a focus to reduce spam, filter inappropriate content, and Viruses.
- Provide, maintain (at N Release Level) and administer end point security management tools: (a) anti-virus (e. g., Symantec, Palo Alto and TrendMicro), (b) data loss prevention (DLP) (e. g., Web Sense and Palo Alto), (c) web filtering (e. g., Web Sense and Palo Alto) and (d) spam filtering (e. g., Proofpoint) across Customer IT Environment, Authorized Users, data center and Network Assets

Key Responsibilities: -

- Monitor end point security tool sets, including NIDS, HIDS, DLP Systems, and Network behavioral analysis tools (e. g., Arbor PeakflowX).

- Document, maintain (at N Release Level) and manage DLP (host and Network) existing Equipment, software and tools.

- Manage DLP rules based on Customer policies and procedures.

- Notify Customer of Viruses and System vulnerabilities or threats that could lead to adverse effects on Customer; such notice shall be provided within agreed SLA of the Virus, System vulnerability or threat being published by industry-recognized sources or identified by Service Provider.

Candidate Requirements:

3+ relevant experience into End point security
Bachelor's degree or equivalent
Excellent written and spoken communication skills CrowdStrike.
Carbun Black
Palo Alto networks XDR
FireEye HX
Cisco AMP
ETC