Greetings Dhana,

I am looking for a Project that matches my skill set. Please find the attached resume

Profile description:

Having 4.9 years of Experience in IT

Security Tools Worked on Cybereason, Carbon black, CrowdStrike, MDE (defender for Endpoint), Qualys, Netskope

Profile Summary in Brief

EDR tool Administrator, Policy management in EDR tools, Providing Application exclusions in security tools, Blocking IOCs in EDR consoles based on advisories received from SOC, Collaborated with SCCM Intune teams for deploying EDR agents (sensor coverage), Fixing devices running in RFM & bypass mode in CrowdStrike & Carbon black (sensor health check),Integrated Cybereason with Splunk Handling performance issues in Carbon Black and CrowdStrike, including high CPU and memory usage due to EDR agents ServiceNow ticket management related to security tools , closing the tickets with in the SLA (Incident , Request, Change task), alert review and investigation, Resolving sensor connectivity issues when sensor failed to connect with cloud, Knowledge in Proof Point Isolation, TAP,TRAP.

Automation :

* Automated the McAfee DAT(signature version) and DLP compliance reports by using PHP as Backend language and SQL as database.
* Successfully automated the generation of onboarded devices reports for 17 operating companies, utilizing APIs to extract data from the Carbon Black console. Reduced the report generation time from one hour to just 5 minutes.
* Developed a script which accepts machine names as input and will provide the ping status of the machines if the machines are connected our client network.
* Restrict app execution automation in Microsoft Defender for endpoint.

I hope this message finds you well.

As I will be releasing from my current project by this month end, I am seeking a project that aligns with my skill set. Please find my attached resume.

Employee Name : Vanamadi Girish

Employee ID : 2281922

Having 4.9 years of experience in IT, I have worked with various security tools including Cybereason, Carbon Black, CrowdStrike, Microsoft Defender for Endpoint (MDE), Qualys, and Netskope.

Profile Summary in Brief

EDR tool Administrator, Policy management in EDR tools, Providing Application exclusions in EDR/NGAV tools, Blocking IOCs in EDR consoles based on advisories received from SOC, Collaborating with SCCM Intune teams for deploying EDR agents (sensor coverage), Fixing devices running in RFM & bypass mode in CrowdStrike & Carbon black (sensor health check),Integrated Cybereason with Splunk ,Handling performance issues, including high CPU and memory usage due to EDR agents ServiceNow ticket management related to security tools , closing the tickets with in the SLA (Incident , Request, Change task), Vendor collaboration, alert review and investigation, Resolving sensor connectivity issues when sensor failed to connect with cloud, Knowledge in Proof Point Isolation, TAP,TRAP. Asset scanning, creating and scheduling Vulnerability reports (Qualys) and working with respective teams to fix the identified vulnerabilities , reviewing firewall rules.