#### Image result for MCSE**Sandeep**

**PROFESSIONAL EXPERIENCE**

* **A Professional Expert and Technical Architect with 10+ Years of IT experience which** including 5.2 years in Information Security, with security operations including Incident management, Intrusion detection and prevention, Endpoint security and logs analysis through SIEM. Experience on working in operations of SOC team, offering log monitoring, security information management, threat monitoring, treat hunting and team management and **comprehensive experience in End-to-End IT management, Solution Designing, Modern Workplace, DaaS, SaaS, IaaS, O365 and Cloud Migrations**
* Experience in **Security Operations Centre** as **Information Security Analyst, Senior Security Analyst, and Team Lead** from June 2015 – till date.
* Advance Cyber breach investigation/Analysis/Remediation (Botnet, CnC, Ransomware, and Phishing attacks).
* Deep logs investigation and analysis using security device such as Intrusion Detection & Prevention (IDS / IPS), Trend Micro APT and Symantec Endpoint Protection.
* Good understanding of network fundamentals and protocols like TCP/IP, UDP, DHCP, FTP, DNS, SMTP, SSH, SSL, HTTP and HTTPS.
* Handling the team for providing proper support to other Analysts in BAU.
* Have sound knowledge and exposure in IT Sox compliance, Control Testing and Proficiency in ITGC (IT General Controls) and Applications Controls.
* Identified risks and integrity controls by assisting in mapping and documentation of processes.
* Conducting risk assessment and identifying controls are in place to mitigate identified risks.
* Conducting risk assessment and identifying controls are in place to mitigate identified risks.
* Documenting identified in risk register/ risk log with defined timelines to mitigate along with recommendations.
* Conducted walkthroughs with asset owners and performed TOD (Test of Design), TOE (Test of operating effectiveness) for respective domain level IT General controls.
* Involved in successful transition of an audit process and singlehandedly driving the audit process and ensure that the controls around user access management are working efficiently.
* Responsible for tracking and monitoring the progress of remediation plans advised by auditors’ during the external audits.
* Managed the timely revisiting of past decisions to evaluate if conditions have changed; and repeating the processes as needed.
* Implementing systems & manuals for internal controls & audit while adhering to statutory compliances where needed.
* Ensure appropriate treatment of risk, compliance, and assurance from internal and external perspectives.
* Conducted follow-up on both open and past due internal audit and SOX observations.
* Enthusiastic and have capability to learn new technology and business domains quickly.
* Regular interaction with the associated customer to update regarding security issues being noted in their infrastructure and provide them daily, weekly, and monthly Reports.
* Taking part for preparing proper documents like Playbooks, Client DL /asset list, SOPs, and other standard operational documents.
* Knowledge of Malware analysis, Vulnerability assessment and BCP/DR.
* Knowledge on Physical security in information security.
* Worked on Qualys VA and Forcepoint DLP tool POC.
* Worked on Carbon Black EDR solution and Tanium endpoint security solution.
* Having working experience on Project management and team management.
* Having working experience on Microsoft products like : MDE, MDI, MDO and O365
* Basic working experience and acquiring knowledge on Mergers & Acquisitions.
* Strong ability to handle multiple cross functional teams and prioritize multiple tasks to develop and deliver cost and time-effective business solutions.
* Having working experience on Project management and team management.
* Having working experience on Microsoft products like : MDE, MDI, MDO and O365
* Basic working experience and acquiring knowledge on Mergers & Acquisitions.
* Expertise and defect Management Process, (AECM) Adverse Events and Complaint Management (Identifying, analyzing, reproducing, and fixing of bugs)
* Good Experience in training and onboarding of new members in team. Acted as **Onsite Coordinator** and delegating the projects to the offshore
* Proficient in preparing documentation, Support notes for the Application Support.
* Excellent problem-solving skills with a strong technical background and good interpersonal skills.
* **SCCM 2007 & 2012 CAS Primary and secondary site Installation.**
* Expert knowledge on Microsoft Debugging Tools (SYS Internals), Fiddler, MS Office & Windows Registries.
* Recognized for delivering leading edge solutions that consistently meet complex business requirements.
* An out of the box thinker with proven track record of establishing processes, SOP’s, streamlining workflow and creating team work environment to enhance productivity.
* Have good knowledge on Network Administration, Linux OS, Layers, OSI model and TCP/IP model.

**TRAININGS & CERTIFICATIONS:**

* Scrum master
* **Certified Azure Administrator**
* Certified in Microsoft 365 Certified: Endpoint Administrator Associate
* Trained in Microsoft 365 Certified: Endpoint Administrator Associate
* **Attended training on Azure Security Associate AZ-500, preparing for Certification**
* **Attended Qualys Cloud Security Assessment Training.**
* **Completed training on MS products like MDO, MDE and MDI**
* **Trained on Verizon NDR (Protect wise) product.**
* **Trained on Trend Micro Cloud One Deep Security tool**
* **Trained on Certified Information Systems Security Professional(CISSP)**
* Windows Server 2008 Active Directory Configuration (MCTS)
* Trained in Cisco Certified Network Administrator (CCNA)
* Trained in Software Center Configuration Manager (SCCM) & Microsoft INTUNE
* **Salesforce Certified Administrator**

**TECHNICAL SKILLS**

SIEM Tool/Analytics : SIEM- ArcSight ESM/Logger, QRadar, DNIF, Alien Vault, ELA, EIQ, Splunk,

Wireshark(basic), Nessus, Nmap

Technologies : SCCM, Scrum master, Intune, Azure AD, Ivanti, PowerShell,

CyberArk, IBM MAAS360, MS SQL, Tanium, Salesforce Administrator.

Mobile Device Management (MDM), Modern Workplace Solutions

ITGC : IT General Controls, ISO/IEC 27001, TPRM, Internal Audit, SOX 404

Mobile Device Management (MDM), Modern Workplace Solutions

Cloud Technologies : Microsoft Azure, AWS cloud platform, VM Ware one, Cloud flare Debugging Tools : Microsoft WinDbg, ProcMon, ProcDump, Process Explorer, Apple Diagnostics.

Reporting/CRM Tools : ServiceNow, BMC Remedy & Salesforce, ITSM, OTRS.

Project Management Tools : GitHub & ServiceNow Dashboards, MS Project, Rally, Jira

Business process : Project Management, Data security and compliance

Methodologies : Waterfall, Agile (SAFe, Scrum), Hybrid, Kanban, Access Management

Change Management

Project Management Tools : GitHub & ServiceNow Dashboards, MS Project

Platforms : Windows 7/8/10, Linux (RedHat, Ubuntu, Kali).

Networking : TCP/IP, OSI, VPN, Various Protocols.

Programming : C, MySQL, HTML/CSS

Other Skills : Malware Analysis and Vulnerability Management, Basics of Cloud Security,

Knowledge on Red Team activities.

Web Services : EC2, EBS, IAM, S3 and Lambda function

End-point security tools : Mcafee, Microsoft defender, crowd strike falcon

**PROFESSIONAL EXPERIENCE**

**Client: Mercedes-benz, USA. Feb 2022 to Aug 2023**

**Role: Security consultant /Lead**

**Responsibilities**

* Advance Cyber breach investigation/Analysis/Remediation (Botnet, CnC, Ransomware, and Phishing attacks).
* Deep logs investigation and analysis using security device such as Intrusion Detection & Prevention (IDS / IPS), Trend Micro APT and Symantec Endpoint Protection.
* Good understanding of network fundamentals and protocols like TCP/IP, UDP, DHCP, FTP, DNS, SMTP, SSH, SSL, HTTP and HTTPS.
* Handling the team for providing proper support to other Analysts in BAU.
* Solutions Architect for Mercedes-Benz & Daimler Trucks Client – Managing more than 3.5Lakh end points.
* Responsible for managing Infrastructure Operations and Delivery which includes Providing Technical Consultation, Solution Implementation and Expert support.
* Internal Control: Covering system access controls and IT General controls Worked with SMEs to get the patches implemented on time and remediated the missing patches as well the Access Control Management audits and assessments, internal audit for all SOX, critical, & ISO 270001 scoped applications.
* Third Party Risk Management: My role on TPRM was to monitor and update system alerts to/from third party relationship owners to ensure that their relationship, contracts and action plans are current and meet program requirement And also did Vendor Risk Management, Technology Risk, Information Security.
* Analysing the responses from the responses received from the vendors.
* Collecting the evidences and validating as per the responses received from the vendors.
* Understanding of Cyber security, Risk control Framework.
* Managed and monitored day to day Logical access request for New Hire, Terminated and Transferred employees.
* Coordinated disaster recovery planning, testing, implementation and participate in business continuity planning.
* Dedicated Endpoint Security Engineer with 3 years of experience specializing in McAfee products and solutions.
* Proven track record of implementing and managing endpoint security measures to safeguard organizations from cyber threats.
* Proficient in deploying, configuring, and managing McAfee endpoint security solutions, including McAfee Endpoint Security, McAfee ePolicy Orchestrator (ePO), and McAfee VirusScan.
* Expertise in creating and enforcing security policies, ensuring endpoint devices are compliant with industry standards.
* Implemented advanced threat detection and prevention measures to safeguard endpoint devices from malware, ransomware, and other threats.
* Successfully reduced security incidents through proactive monitoring and threat mitigation.
* Managed patching processes, ensuring all endpoint devices are up to date with the latest security updates and vulnerability patches.
* Achieved significant improvements in patch management efficiency, reducing vulnerability exposure.
* Developed and executed incident response plans for prompt identification, containment, and resolution of security incidents.
* Played a key role in minimizing data loss and system downtime during security breaches.
* Established real-time security monitoring systems to detect and respond to suspicious activities and anomalies on endpoint devices.
* Implemented advanced security information and event management (SIEM) integration for enhanced visibility.
* Collaborated with other engineering teams to understand their systems and help improve them.
* Developed Internal and customer facing cloud services (Server less and container-based) in AWS using AWS ECS
* Rotated IAM access keys regularly and standardized on a selected number of days for password expiration to ensure that data cannot be accessed with a potential lost or stolen keys
* Restricted access to RDS instances to decrease the risk of malicious activities such as brute force attacks, DOS or SQL injection.
* Inventoried and categorized all existing AWS resources.
* Proficient in implementing and managing Single Sign-On (SSO) solutions for user authentication and access control.
* Successfully integrated SSO with various web applications, enhancing security and user experience.
* Demonstrated expertise in configuring SSO protocols such as SAML, OAuth, and OpenID Connect.
* Developed custom SSO solutions to meet specific organizational requirements, resulting in streamlined user access and reduced login friction.
* Monitored and analyzed cloud security events and logs and identifying, responding to security incidents in real-time, resulting in a 50% reduction in potential security risks.
* **Modern Work Place Expert worked on Modern Device Management & Hybrid Workplace Flexibility.**
* Responsible for Simplified End-of-Life Management, Scalability and Agility, Technology Refresh and Expert Support.
* Lead large teams across different locations (EUC, IaaS, DaaS, SaaS, Collab, CyberArk, VDI, Printing, SCCM, Exchange, SPO, Office 365).
* **Worked closely with other Infrastructure teams and successfully designed and implemented Security Polices for DaaS such as: IAM, PIM, DLP, Azure Firewall, NSG’s, EDR and Azure Monitor.**
* Taking ownership of critical incidents, coordinating with resolution parties, and establishing effective communication between stakeholders for post-incident reviews
* Project Planning, Implementation & Execution, Service Improvements & Automations. Working closely with Technical Leads and Architects across all Daimler locations - to design process and maintain set Service Level Agreements for smooth operations.
* Reviewing and Fine-tuning optimization of services, Accountability for service delivery performance, meeting customer expectations and driving future demand.
* Practicing ITIL Process and Managing In-house Infrastructure, which includes IT Hardware and End Clients, Operating Systems, Software Procurements and technical assistance.
* Communicate maintenance schedules, operational issues and impacts to IT management.
* Strong focus on service excellence and ownership for resolving customer issues.
* Working with global colleagues to provide globally consistent processes and procedures.
* Responsible for managing team budgets, keep a track and forecast the requirements accordingly.

Manage the support group to ensure ticket resolutions met with set SLA’s.

* Regular interaction with the associated customer to update regarding security issues being noted in their infrastructure and provide them daily, weekly, and monthly Reports.
* Taking part for preparing proper documents like Playbooks, Client DL /asset list, SOPs, and other standard operational documents.
* Knowledge of Malware analysis, Vulnerability assessment and BCP/DR.
* Knowledge on Physical security in information security.
* Knowledge on AWS cloud platform.
* Worked on Qualys VA and Forcepoint DLP tool POC.
* Worked on Carbon Black EDR solution and Tanium endpoint security solution.
* Having working experience on Project management and team management.
* Having working experience on Microsoft products like : MDE, MDI, MDO and O365
* Plan and deploy Enclave Boundary Defence systems and programs including firewall, proxy server and other devices and applications to all DTRA enclaves.
* Plan and deploy De-Militarized Zones (DMZs) for each DTRA NTS managed firewall
* Verify devices are configured in accordance with DISA Security Technical Implementation Guides (STIGs)
* Basic working experience and acquiring knowledge on Mergers & Acquisitions.
* Deep investigation on critical alerts from SIEM for proactive prevention of threats Monitoring, analyzing and alerting real time incidents
* Monitoring, analyzing logs from various security appliances using Sentinel console.
* Strategic technical lead who will oversee the vision, roadmap, trade-offs and delivery across the enterprise with a relentless focus on balancing security with simplification.
* Serve as a cyber security counsel to senior leadership
* Operate as a trusted advisor on cyber security as well as for a specific technology, platform and/or capability domain, helping to shape use cases and implementation in an unified and consistent manner
* Brings in a larger context to a larger software teams and architects across multiple domains/departments and guide their architecture evolution in response to business changes
* Builds awareness, increase knowledge and drive adoption of modern technologies, sharing consumer and engineering benefits to gain buy-in experience in cloud security
* Support day-to-day cybersecurity threat detection and incident response operations through indicator pivoting, campaign analysis, and tactical intelligence
* Identify and enhance processes where automation has the potential to improve efficiencies, provide actionable data, and facilitate collaboration across CSOC
* Leverage Security Orchestration, Automation, and Response (SOAR) or Security Information and Event Management (SIEM) tools to identify threat patterns, enrich investigations, and build automation-supported workflows
* Deconstruct multi-source reporting into actionable intelligence including Tactics, Techniques, and Procedures (TTPs) data objects, campaign analysis, and threat patterns.
* Regularly analyze malware reports to track adversary behaviors and support the construction of a TTP repository
* Proactively build and maintain relationships with partner teams, including but not limited to Cyber Intelligence, Red Team, Insider Threat, and Hunt teams.
* Conduct time-sensitive analysis during cyber investigations, including active threat hunting, malware analysis, and campaign enrichment
* Routinely identify gaps in detection and collaborate with teams across the Cyber organization to mitigate risk, including blocking of malicious indicators, tuning vendor signatures, and instrumenting custom detection rules
* Support the tactical intelligence-to-detection pipeline, to include malware reverse engineering, TTP analysis, and association mapping in a TIP (threat intelligence platform) for future pivoting
* experience in cloud security
* Worked on EDR, MCAS, MDATP.
* Creating the Documents of incidents Response of various Incidents received
* Prepared daily, weekly and monthly and ad-hoc reports.
* Deep Analyzing the incidents through Microsoft EDR.
* Monitoring, analyzing logs from various security appliances using LogRythm console.
* Reporting device/interface down events to maintain maximum uptime and thus helping in preventing any log loss or minimizing any delay.
* Analyzing and looking after proactive solutions of the spam emails
* Creating the Documents of incidents Response of various Incidents received
* Prepared daily, weekly and monthly and ad-hoc reports.
* Modern Work Place Expert worked on Modern Device Management & Hybrid Workplace Flexibility.
* Involved in SCCM Deployment process deployment.
* Deploy mobile devices to employees and configure them according to company standards
* Install and update device firmware, applications, and settings in MDM
* Responsible for managing Infrastructure Operations and Delivery which includes Providing Technical Consultation, Solution Implementation and Expert support.
* Project Planning, Implementation & Execution, Service Improvements & Automations. Working closely with Technical Leads and Architects across all Daimler locations - to design process and maintain set Service Level Agreements for smooth operations.
* Responsible for configuring & managing App Protection Policy and Configuration Policy
* Maintain an accurate inventory of all mobile devices within the organization.
* Track and manage device assignments, replacements, and retirements
* Handling the team for providing proper support to other Analysts in BAU.
* Regular interaction with the associated customer to update regarding security issues being noted in their infrastructure and provide them daily, weekly, and monthly Reports.
* Taking part for preparing proper documents like Playbooks, Client DL /asset list, SOPs, and other standard operational documents.
* Modern management of Windows 10 using Windows Autopilot
* Deep Analyzing the incidents through Redline and getting preliminary cause of an alert
* Troubleshooting of Fire Eye communication issues on servers and Endpoint machines Creating Acquisitions of incident Triggered machines
* Knowledge sharing with team members

**Client: Bei gene biotech, USA. Apr 2018 to FEB 2022**

**Role: Security Matter expert**

**Responsibilities**

* Monitoring, analyzing logs from various security appliances using Arc Sight ESM console, Arc Sight Logger and connectivity troubleshooting issues.
* Created filters, active channels, queries in Arc Sight for monitoring purpose.
* Tracking and reporting the configuration changes in routers, switches through dashboard.
* Reporting device/interface down events to maintain maximum uptime and thus helping in preventing any log loss or minimizing any delay.
* Monitoring Active Channels and Dashboards.
* Plan and deploy De-Militarized Zones (DMZs) for each DTRA NTS managed firewall
* Builds awareness, increase knowledge and drive adoption of modern technologies, sharing consumer and engineering benefits to gain buy-in experience in cloud security
* Support day-to-day cybersecurity threat detection and incident response operations through indicator pivoting, campaign analysis, and tactical intelligence
* Proficient in deploying, configuring, and managing McAfee endpoint security solutions, including McAfee Endpoint Security, McAfee ePolicy Orchestrator (ePO), and McAfee VirusScan.
* Expertise in creating and enforcing security policies, ensuring endpoint devices are compliant with industry standards.
* Implemented advanced threat detection and prevention measures to safeguard endpoint devices from malware, ransomware, and other threats.
* Implemented and managed endpoint encryption solutions to protect sensitive data on laptops and mobile devices.
* Ensured compliance with data protection regulations and data privacy requirements.
* Conducted employee training on best practices for endpoint security, reducing the risk of social engineering attacks and data breaches.
* Conducted regular security assessments and vulnerability scans on endpoint devices to identify and remediate security weaknesses.
* Have sound knowledge and exposure in IT Sox compliance, Control Testing and Proficiency in ITGC (IT General Controls) and Applications Controls.
* Identified risks and integrity controls by assisting in mapping and documentation of processes.
* Conducting risk assessment and identifying controls are in place to mitigate identified risks.
* Conducting risk assessment and identifying controls are in place to mitigate identified risks.
* Documenting identified in risk register/ risk log with defined timelines to mitigate along with recommendations.
* Conducted walkthroughs with asset owners and performed TOD (Test of Design), TOE (Test of operating effectiveness) for respective domain level IT General controls.
* Involved in successful transition of an audit process and singlehandedly driving the audit process and ensure that the controls around user access management are working efficiently.
* Maintained documentation of assessment results and mitigation strategies.
* Maintained comprehensive documentation of security policies, procedures, and incident response plans.
* Ensured that endpoint devices were consistently compliant with regulatory and company-specific security requirements.
* Collaborated closely with McAfee and other security solution vendors to optimize security products, resolve issues, and receive timely support.
* Kept up-to-date with the latest trends and threats in cybersecurity, attending relevant training and certification programs.
* Identify and enhance processes where automation has the potential to improve efficiencies, provide actionable data, and facilitate collaboration across CSOC
* Rotated IAM access keys regularly and standardized on a selected number of days for password expiration to ensure that data cannot be accessed with a potential lost or stolen keys
* Restricted access to RDS instances to decrease the risk of malicious activities such as bruteforce attacks, DOS or SQL injection.
* Inventoried and categorized all existing AWS resources.
* Monitored and analyzed cloud security events and logs and identifying, responding to security incidents in real-time, resulting in a 50% reduction in potential security risks.
* Leverage Security Orchestration, Automation, and Response (SOAR) or Security Information and Event Management (SIEM) tools to identify threat patterns, enrich investigations, and build automation-supported workflows
* Deconstruct multi-source reporting into actionable intelligence including Tactics, Techniques, and Procedures (TTPs) data objects, campaign analysis, and threat patterns.
* Developed Internal and customer facing cloud services (Server less and container-based) in AWS using AWS ECS
* Regularly analyze malware reports to track adversary behaviors and support the construction of a TTP repository
* Proactively build and maintain relationships with partner teams, including but not limited to Cyber Intelligence, Red Team, Insider Threat, and Hunt teams.
* Conduct time-sensitive analysis during cyber investigations, including active threat hunting, malware analysis, and campaign enrichment
* Routinely identify gaps in detection and collaborate with teams across the Cyber organization to mitigate risk, including blocking of malicious indicators, tuning vendor signatures, and instrumenting custom detection rules
* Support the tactical intelligence-to-detection pipeline, to include malware reverse engineering, TTP analysis, and association mapping in a TIP (threat intelligence platform) for future pivoting
* Serve as a cyber security counsel to senior leadership
* Operate as a trusted advisor on cyber security as well as for a specific technology, platform and/or capability domain, helping to shape use cases and implementation in an unified and consistent manner
* Brings in a larger context to a larger software teams and architects across multiple domains/departments and guide their architecture evolution in response to business changes
* Verify devices are configured in accordance with DISA Security Technical Implementation Guides (STIGs)
* Product lifecycle management and upgrades to include installation of hotfixes, patches, and any other features to improve product performance
* Maintain all current applicable firewall and proxy appliance policies to include DoD, DISA, and DTRA
* Analyzing and looking after proactive solutions of the spam emails
* Manage queries, reports, Filters, Connectors, and Active Channels in Arc Sight.
* Creating the Documents of incidents Response of various Incidents received
* Prepared daily, weekly and monthly and ad-hoc reports.
* Responsible in Sending Weekly & Monthly reports on SLA’s and Metrics to Senior Management.
* Implementing Performance Improvement Plans for team members and design Functional goals for every assessment year. Drive continual improvement initiatives by providing regular feedbacks.
* Communicate maintenance schedules, operational issues and impacts to IT management.
* Strong focus on service excellence and ownership for resolving customer issues.
* Responsible for managing team budgets, keep a track and forecast the requirements accordingly.
* Manage the support group to ensure ticket resolutions met with set SLA’s.
* Responsible in Sending Weekly & Monthly reports on SLA’s and Metrics to Senior Management.
* Implementing Performance Improvement Plans for team members and design Functional goals for every assessment year.
* Drive continual improvement initiatives by providing regular feedbacks
* Triage collection of infected machines and analyzed using (Redline) Tool.
* Deep Analyzing the incidents through Redline and getting preliminary cause of an alert
* Troubleshooting of Fire Eye communication issues on servers and Endpoint machines Creating Acquisitions of incident Triggered machines
* Creation, mapping, troubleshooting the issues of Identity Access Management Tool (PIM)
* Assigning and troubleshooting of 2 factor (RSA SECURE ID) authentication issues.
* Working in Security Operation Center (24x7), monitoring of SOC events, detecting and preventing the Intrusion attempts.
* Monitoring real-time events using SEIM tools like HP ArcSight, IBM Qradar.
* Monitoring, analyzing and responding to infrastructure threats and vulnerabilities.
* Ad hoc report for various event sources customized reports and scheduled reports as per requirements.
* Collecting the logs of all the network devices and analyze the logs to find the suspicious activities.
* Creating the tickets in ticketing tool Service Now.
* Investigate the security logs, mitigation strategies and responsible for preparing generic security incident reports.
* Responsible to preparing the root cause analysis reports based on the analysis.
* Analyzing daily, weekly and monthly reports.
* Creating case for the suspicious issue and forwarding it to Onsite SOC team for further investigation.
* Responsible for applying security updates and patches on servers, desktops, and laptop
* Involved in **SCCM Deployment process** deployment.
* Responsible for **managing Infrastructure Operations and Delivery which includes Providing Technical Consultation**, Solution Implementation and Expert support.
* **Modern management of Windows 10** using Windows Autopilot
* Responsible for configuring & managing App Protection Policy and Configuration Policy.
* **Real time troubleshooting related to SCCM issues**.
* Involved **in SCCM patching process** deployment.
* **Check health of device every week and sharing report of device** **in Intune**
* Creating the **software update group**.
* Creating the individual search for Windows Updates.
* **Adding the security updates Windows Updates to update groups**.
* Downloading the software updates.
* Deploying the security updates to **UAT, PILOT & Production**.

**Client: Daimler, Bengaluru. Oct 2014 to Apr 2018**

**Role: System Administrator**

**Responsibilities**

* Escalation Lead for a Team of 6 Tier2 System Administrators for In-House IT Support.
* Strong Knowledge on Windows Administration and Providing L3 level support.
* Complete Asset Management handled seamlessly.
* Installing server operating system windows Server (2003, 2008, 2012)
* Installation and configuration SCCM Client & WMI remediation.
* Sending project milestones and updating the client about the progress of the project regularly.
* Managing the SCCM reports for patching and client’s status.
* Performed remote installations and product fixes, as well as various troubleshooting support.
* Providing Trainings to New Associates and Send Weekly, Daily Reports to the Management representing Infrastructure Teams.
* Extensive Experience with troubleshooting Windows Installer (MSI) & Windows Installer Transforms (MST) installation and runtime errors.
* Creating configuration items.
* Creating configuration base lines.
* Deploying baselines to respective collections.
* Distribute the content to Distribution point and groups.
* Deploying the application model and package model to device collections.
* Deploying the application for self-service portal.
* Creating package model for deployments.
* Configuring Servers Roles - AD, DHCP, DNS, Exchange.
* Configuration and Troubleshooting File Server, Print Server for Domain Access.
* Installing and Managing Anti-Virus Software (Symantec, McAfee) for all Clients and servers
* SCCM patch management: OS deployment through SCCM OSD and MDT.
* Creation and configure packages, programs, advertisement and collections for Software Distribution.
* Handling with Antivirus Server and server related queries with User Updates.
* Creating Local Profiles to the local users for customizing desktop settings.
* Testing Different Application Packages before Pilot Release on Windows 7 and Investigate the Application Connectivity from different Applications, Vendors and Partnered Networks.
* Testing application model and package model in UAT and PILOT environment and rollout it in production.
* Creating the individual search for Windows Updates.
* Adding the security updates Windows Updates to update groups.
* Downloading the software updates.
* Deploying the security updates to UAT, PILOT & Production.
* Documentation of every month patches.
* **Documentation of every month patches**.
* Preproduction testing of patches.
* **Troubleshooting and diagnosing the SCCM log files for patching related issues for users**.
* Knowledge of installation and configuration WSUS / Integrated SCCM Patch management.
* **Knowledge on 3rd party patching with SCUP.**
* **Knowledge on integration of SCUP with WSUS and SCCM.**
* Migrations, Software Distribution & Local IT Support.
* Collaborating with business to define solutions to meet business requirement and Infrastructure Governance.
* Working closely with Program Manager to maintain and set Service Level Agreements and reduce escalations.
* Communicate maintenance schedules, operational issues and impacts to IT management.
* Strong focus on service excellence and ownership for resolving customer issues.
* Responsible for Windows OS Migrations from Win7 to 10 (targeted to 20 thousand end clients).
* Automated few tasks on Windows10 OS, which includes folder redirection, home drive synchronization.
* Subject Matter Expert for WinServer2012, 2016 & Windows7, 8.1 and 10 Client Operating Systems.
* Working with global colleagues to provide globally consistent processes and procedures.
* Responsible for managing team budgets, keep a track and forecast the requirements accordingly.
* Manage the support group to ensure ticket resolutions met with set SLA’s.
* **Hands-on Experience in Managing enterprise environment using various virtualizations**
* Streamlined the processes and working closely with leaders of various other CoE's.
* **Creating the Task sequence according to the requirement.**
* Targeting the **task sequence** to the collections.
* **Customizing SQL queries, reports as per requirements.**
* **Having knowledge on creating custom reports by report builder**.
* Creating datasets for drop down options in reports.
* Having knowledge on how to creating query-based collection by using power shell
* Initiate hardware and software inventory by using power shell on remote machines.
* Responsible in Sending Weekly & Monthly reports on SLA’s and Metrics to Senior Management.
* Implementing Performance Improvement Plans for team members and design Functional goals for every assessment year. Drive continual improvement initiatives by providing regular feedbacks.
* Actively participating in Innovation and Automation
* Having knowledge on modifying MOF files to extend Hardware inventory.
* Installation of various software and applications according to company policies
* Installing and troubleshooting hardware and software issues.

**EDUCATION**

* B. Tech (ECE) from Jawaharlal Nehru Technological University Kakinada with First Class degree in 2010
* M.Tech (**Information security and cyber forensics**) S.R.M University Chennai with First Class degree in 2013