NISHANT SINGH CHAUHAN

nishantchauhan03@gmail.com | +91-9982678047 | linkedin.com/in/nishant-singh-chauhan2507

PROFILE

Committed to maintaining secure and stable IT infrastructure and delivering exceptional technical support. Experienced in the security domain with hand-on work in Implementations, configurations, upgrades, health checks, patching, and proactive system monitoring.

SKILLS

Data Loss Prevention | Drive Encryption | Incident & Evidence Monitoring | Event Management | Data Classification | Product Testing | Mobile Device Management | Endpoint Security | Web Filtering | Application Control | Device Control | Project Planning & Execution | Data Monitoring | Data & User Management | Implementing Backup & Recovery | Process Implementation | Troubleshooting

PROFESSIONAL EXPERIENCE

Deputy Manager – IT
Aavas Financiers Ltd **Sept-21 to Aug-24**

Project Responsibilities

➢ **Trellix / McAfee ePO 5.10 (Data Loss Prevention & Drive Encryption)**

- ❖ Manage Trellix (McAfee) ePolicy Orchestrator for Drive Encryption (DE) and Data Loss Prevention (DLP) across an enterprise environment of 7,000+ users, ensuring consistent security enforcement.
- ❖ Define, configure, and fine-tune DLP policies and rules to detect, monitor, and prevent unauthorized data transfer across endpoints, networks, and storage systems, aligned with evolving threats and business requirements.
- ❖ Implement and administer Trellix Drive Encryption for Windows devices, including secure encryption/decryption processes and performing data recovery using WINPE and Trellix DEtech tools to prevent data loss.
- ❖ Monitor daily DLP incidents, analyze evidence related to policy violations, and generate regular activity and compliance reports for management and audit purposes.
- ❖ Ensure all Trellix agents (DLP, DE) remain up-to-date with patches, upgrades, and security fixes to maintain optimal performance and reduce vulnerabilities.
- ❖ Collaborate with IT, Security Operations, Compliance, and CISO teams, integrating DLP with SIEM solutions to enhance security visibility, incident response, and overall data protection posture.

➢ **VMWare Workspace One UEM & ACCESS**

- ❖ Manage 750+ devices—including Windows laptops, MacOS systems, iPhones, iPads, and Android devices—through the VMware Workspace ONE UEM console, ensuring consistent configuration and compliance.
- ❖ Monitor overall UEM environment health and performance while managing user accounts, roles, permissions, and multiple profile/group settings for internal and public environments.
- ❖ Configure and enforce device management and access control policies, and manage the full mobile application lifecycle (catalog creation, distribution, and updates) across Android and iOS platforms.
- ❖ Provide virtual support to users for device enrollment, application installation, troubleshooting, and handle escalated Service Desk incidents related to Workspace ONE/Airwatch.
- ❖ Deploy and manage connectors on on-prem servers for Active Directory integration and O365 Exchange authentication, ensuring seamless connectivity between Workspace ONE UEM and Access.
- ❖ Collaborate with VMware Support for issue resolution and generate MIS reports for CISO and management teams covering device enrollment, application deployments & device compliance.

- **Data Discovery & Data Classification**

  - Utilized automated data discovery tools (Trellix /Klassify/ GTB) to map structured & unstructured data across On-Prem, SAAS, and Multi-Cloud environments.
  - Performed sensitive data discovery using Pattern Matching (Regex), Keyword lookups, Exact Data Matching (Fingerprinting), Contextual Analysis (Proximity) and Metadata Inspection, often enhanced by Machine Learning to find & Validate sensitive Content.
  - Developed and enforced a tired classification framework (Restricted/confidential, Internal, and Public) to align data sensitivity with security controls, encryption & access permissions.
  - Led sensitive data discovery and protection efforts across PII, PHI, PCI, and IP by applying automated labeling.
  - Implemented regulatory –compliant data handling with GDPR, CCPA, HIPAA, DPDP, etc.

- **Seqrite Endpoint Security 7.6 Total**

  - Designed, implemented, and documented Seqrite Endpoint Security solutions tailored to enterprise architecture, security standards, and compliance requirements.
  - Provided comprehensive operational support—managing system performance, performing scheduled and unscheduled maintenance, and resolving endpoint security issues.
  - Installed, configured, updated, and troubleshot Seqrite agents across Windows, MacOS, and Linux platforms to ensure consistent endpoint protection.
  - Analyzed requirements and configured endpoint policies, including Application Control, Device Control, and Web Filtering, aligned with organizational security needs.
  - Performed initial malware scanning, log analysis, and basic forensic review of user activity to support incident investigation and threat identification.
  - Integrated Seqrite with external security vendors and SIEM platforms to enhance threat visibility, while training and preparing documentation for L1/L2 teams and generating customized security reports for stakeholders.

- **Druva: Insync Endpoint Backup Solution**

  - Manage Druva Data Resiliency backups for 750+ users, ensuring protection against data loss, corruption, and intellectual property risks across the organization.
  - Automate and administer backups for diverse data sources—including endpoints, servers, databases, and cloud applications—ensuring reliable and policy-driven data protection.
  - Configure and maintain Druva environments by creating profile groups, defining backup policies based on data types, and monitoring agent communication for consistent backup and recovery operations.
  - Conduct routine maintenance activities, including system upgrades, configuration enhancements, and patch installation to maintain platform performance and security.

- **Project Involvement (Monitoring & POC Security Tools)**

  - Conducted Successful POCs on Data Loss Prevention Tool like (Forcepoint DLP, Data Resolve: Indefend & GTB) on Multiple platforms (Windows/Ubuntu/MacOS).
  - Perform Multiple POCs for Mobile Device Management (MDM) solutions, assessing their effectiveness in securing and managing personal or corporate devices across diverse organizational environments.
  - Worked closely with various teams in IT Dept. to ensure smooth implementation of security solutions, coordinating for multiple configurations with SIEM-related activities.

Sr. Executive – IT
RUJ WOODCRAFT Pvt. Ltd **Aug-19 to Sept-21**

- Configure and manage Active Directory, User Groups, Group Policy, and many more.
- Managed Office 365 Admin portal for user profile management, mail flow monitoring, data security, reports generating compliance, threat management, data privacy, and supervision.
- Managed Seqrite Endpoint Security Antivirus for web filtering, content filtering, Bandwidth monitoring, and user access control centrally.
- Managed checkpoint firewall to configure ISP network, Quality of Service Control, monitoring logs, User and System Access policies, Threat Prevention, remote access, and configured VPN site to site or tunnels.
- Managed On-premises software and Licenses like Teams, Office 365, windows license, and Seqrite antivirus, designing and developing software (AutoCAD, Photoshop).
- Monitoring and Maintaining CCTV, Servers, and network devices. Responding promptly to service issues and requests.
- Providing technical support across the company (this may be in person or over the phone).

EDUCATION

Master's in Computer Application **2016 - 2018**
Maharishi Arvind Institute of Science & Management Rajasthan Tech. University

Bachelor's in Computer Application **2013 - 2016**
Maharishi Arvind Institute of Science & Management Rajasthan University

TOOLS

Druva: Data Resiliency cloud | Trellix (McAfee ePO) ePolicy Orchestrator & McAfee DEtech Data Recovery Tool | VMWare Workspace One UEM & Access | GTB Data Loss Prevention | Quick Heal Seqrite Endpoint Security