**Mandeepsinh Ranavat**

**Cyber Security/ Digital Forensics Lead**

**PROFESSIONAL SUMMARY:**

* 7 years of IT Experience in Cyber Security with good experience in Implementation, Administration, Operation and Troubleshooting of enterprise data networks
* Experience in planning, developing, implementing, monitoring and updating security programs, and advanced technical information security solutions, and sound knowledge in SOX and PCI compliance requirements and understanding of NIST and ISO standards
* Experience as a Splunk Engineer configuring, implementing and supporting Splunk Server Infrastructure across Windows, UNIX and Linux environments
* Configure, maintain and design network security solutions including firewalls (Checkpoint, Cisco ASA and Fortinet), IDS/IPS (Cisco, Checkpoint and Sourcefire), VPN, ACLs, Web Proxy, etc.
* Hands on experience on Operations and management of Aruba based wireless network providing multiple SSID platform for DoD users
* Hands on experience on Web Application Firewalls and attack mitigation techniques
* Work closely with clients Information Assurance analysts to oversee the preparation of a comprehensive and executive and Accreditation (C&A) packages for approval of an Authorization to Operate (ATO); generate, review and update System Security Plan (SSP) against NIST and NIST requirements
* Establish a strong GRC (Governance, Risk and Compliance) practice to ensure adherence to best practice, regulatory requirements and ISO 27001
* Facilitate implementations of information security policies, account security policies and standards for logical and physical security
* Perform Risk Assessment, Gap analysis & create Risk Mitigation plan
* Good experience to provide remediation consultation to organizations and system owners, ensuring vulnerabilities are remediated IAW DISA/NIST and Cyber Threat Intelligence research
* Modernize assessment tools by researching emerging technologies and outlining their procurement to increase productivity and effectiveness.
* Developing and implementing risk management strategies, policies, and procedures to mitigate operational risks. This involves establishing risk appetite, tolerance levels, and controls.
* Having good understanding and Knowledge for implementation for ISO 27001, NIST 800 - series, DIACAP, and FISMA guidance/governance
* Implemented and configured CASB solution including Netskope to secure the enterprise with a cloud.
* Maintain ongoing review and monitoring of SIEM alerts (Splunk) and SOAR alerts.
* Strong knowledge under Imperva web application firewall for monitoring for in-depth analysis of attacks and SIEM tools such as Splunk, HP ArcSight for analysis and log monitoring.
* Worked with CASB such as NetSkope and Skyhigh.
* Led an effort to create a new process in filtering and manage IPS events by automating the process and streamline Security Operation Center (SOC) triage efforts.
* Strong knowledge in DNS, DHCP, IP addressing. Experience of IP Service - DNS, DHCP, IPAM and Active Directory DNS.
* Project managed the efforts of identifying the controls and processes required to comply with CISA (PCI DSS) when they implemented online prepaid-card system. Evaluated and tested the controls and processes relating to credit card data and systems. Identified the gaps in the security of the systems and recommended the practical solutions.
* Managed HBSS Mcafee EPO, configured HIPS 8.0 policies, verified and created server tasks, monitored events, created and enforced DLP policy, managed Rogue System Detection.
* Support deployment of all HBSS point products and updates to include Mcafee agent, HIPS, VSE, DLP. Perform HBSS policy tuning, HIPS, IPS tuning, and all related tasks.
* Experienced with Proxy and Malware-mitigation (Blue Coat, Redware/ApplXcel/Alteon, FireEye), threat detection and data leakage protection (Network DLP/Vontu/Symantec, Bluecoat Security Analytics.
* Resolved vulnerabilities in the WebEx and FedRAMP GRC environments, POA&M & NIST, using automated scripts created in Python, PowerShell, Bash.
* Dedicated, multifaceted, and detail-oriented professional with progressive experience in Cybersecurity operations; complemented with wide-ranging knowledge of McAfee ePolicy Orchestrator (EPO) and networking technologies such as firewalls, switches, and routers.
* Analysed the Policy rules, monitor logs and documented the Network/Traffic flow diagram of the Palo Alto Firewalls placed in the Data Center with MS Visio.
* Worked on various projects involving security systems to bring in security data to the SIEM. Systems such as Splunk, Tanium, various IPS event data sets, Blue Coat, Net Witness to just name a few.
* Understanding of TCP/IP networking, IP routing, Server Load Balancing, and Network Security architecture and core technologies, Firewalls, ACLs, DNS, DHCP, IPAM, LDAP, NFS.
* Expert level configuration of Layer 2 technology including VLANS, Trunking, STP, RSTP, PVST, MST, VTP in addition to port-security, Uplink fast, Backbone fast, Port fast, BPDU guard & filter and Ether channel including LACP & PAGP negotiations.
* Management and administration of Juniper and ASA Firewalls at various zones including DMZ, Extranet (Various Business Partners) and internal.
* Aggregate, correlate, and analyse log data from network devices, security devices and other key assets using QRadar. Analysis of various use cases in the QRadar console like Malware, AD related issues.

**PROFESSIONAL SKILLS:**

**Cyber Security:**STIX, TAXII, Trustor

**DLP:**Websense, Symantec & McAfee

**SIEM:**HP ArcSight, Splunk, Net forensics, QRadar

**Load balancer:**BigIP F5 LTM and GTM

**Network:**Cisco Routers, Switches

**Network Security:**Snort

**Database**: My SQL

**Programming Languages**: Java/J2EE, JSP, PHP, HTML, Python

**Operating Systems:**Windows, Linux

**Cloud Technologies:**Amazon Web Services (AWS): SDK, Dynamo DB, Lambda, Elastic Beanstalk

**Application Servers:**Apache Tomcat, AWS Lambda, AWS Elastic Beanstalk

**Virtualization Services & Technologies:**Amazon EC2, GitHub

# **Education & Credentials**

## **Masters in Cybersecurity**

DePaul University Chicago, IL | November 2017

Related Course Work: Network Security, Software Security Assessment, Cryptology, Information Storage and Management, Distributed Systems, Computer Forensic, Info Security Management, Security Capstone

## **Bachelors in information technology**

Rajasthan Technical University Kota, India | October 2014

**Professional Certifications**

CCNA (Routing and Switching) (Aug 2019) | 200-125 CSCO13056131 CompTIASecurity+ (Oct 2026) | 0LBLWPMFLGVQQ6KG

AWS Certified Cloud Practitioner (Oct 2025) | 9K3 K81DCRMVEQ5 SPv Splunk Training and Conference (Nov 2017)

Training for GCFE FOR50 0: Advance Windows Forensic Analysis. (Nov 2018) Training for GASF FOR58 5: Advance Mobile Forensic Analysis (Nov 2022)

**Training for GCIH SEC504:** Hacker Tools, Techniques, and Incident Handling (2023 in Progress)

# **Areas of Expertise**

|  |  |  |
| --- | --- | --- |
| * Cyber Threat Analysis * Digital Forensics * Corporate Investigation * Incident Response * Network Security * Security Data Analysis * DLP Solutions | * Cloud Platforms Protection * Fraud Analysis * Security Risk Mitigation * Performance Management * Teamwork & Capability Building * Risk Management * Application Security | * Security Incident Investigation * Malware Analysis * SIEM Technologies * Compliance Maintenance * Talent Management * IAM and SSO Solutions * Project Management |

**WORK EXPERIENCE:**

**Client: Deloitte, Akron, OH** **February 2018–Present**

**Cyber Security Engineer**

**Responsibilities:**

* Developed custom SIEM deliverables in Splunk/McAfee/QRadar/ArcSight to meet customer needs in a variety of domains: IT security, financial, IT ops, human resources, physical security, etc.
* Design, development, implementation, tuning and testing of standard and nonstandard content for Mcafee SIEM (Nitro).
* Perform Digital forensics and Incident Response (IR) using tools Autopsy, Magnet, Stinger, etc. 28 DOL agencies
* Served as the primary SME for RSA SecurID and all multi-factor authentication products including Azure MFA.
* Maintained GIT repositories, branches and tags and Experience in Administering GITHUB repository.
* Played a key role in deploying Symantec Endpoint Protection Manager and clients on a closed network.
* Supported the GRC implementation of RSA Archer 6.2 Regulatory and Corporate Compliance, Incident, Task and Risk Management Solutions/Use Cases and maintenance of technology for the Compliance Management.
* Worked as a PCI-DSS consultant to perform a 3rd party audit.
* Establish and maintain an IT Compliance program for Financial Security Infrastructure team that minimize risks to IT objectives through effective, efficient, scalable, and cost-effective design and operation of controls, including Sarbanes Oxley (SOX), ITGC (IT General Control) using COBIT framework, and other domestic and international compliance requirements.
* Involved in DLP data encryption, monitoring/reporting and remediation of internal and external threats/vulnerabilities.
* Evaluating the potential impact and likelihood of operational risks through quantitative and qualitative analysis. This includes using risk indicators, key risk indicators (KRIs), and risk assessment frameworks.
* Provided Azure Security and Compliance reviews and solutions for government systems to facilitate the secure and compliant use of Azure for government agencies and third-party providers building on behalf of government.
* Serving as a Cloud Access Security Broker (CASB) Security Specialist with a primary focus on Confidential CASB/Skyfence.
* Troubleshoot and configured connectivity issues related to VPN, DHCP, DNS, Firewall DMZ.
* Identifying current and future customer needs by establishing a personal rapport with potential and current customers to better understand and fulfill their cyber security/CASB needs.
* Ensured Azure Government system was compliant to meet a FedRAMP Provisional Authority to Operate (P-ATO) and DoD Provisional Authorization (PA).
* Understand the threat landscape as related to vendors and perform vendor risk assessments
* Works with Encase, FTK, Cellebrite, Gargoyle, IEF, tools, plus dozens of utilities for ripping, extracting, repairing, copying, de-duplicating, automating and more
* Played an Integral role in migrating company's security firewall environment from FortiOS 4.0 firewall platform to Fortigate FG 100D.
* Performed incident response activities using the Symantec (Netskope and Skyhigh) DLP tools (across network, VPN, e - mail system, at rest storage, file shares, etc.
* Assist penetration testing and investigation.
* Collaborate with Internal audit, External Audit, SOX PMO in a regular cadence, discuss changes to the control environment and prepare effective, efficient compliance and substantive test plans and SOX Calendar.
* Work closely with the Risk and finance teams to associate a monetary value to security risks within the User Behavior Analytics (UBA) tool.
* Worked on projects moving to cloud services such SOARas Azure, Office 365 and Amazon Web Services (AWS).
* Interacted with Cloud Service Provider (CSP) to conduct Incident Response (IR) and Contingency Plan (CP) exercises for Disaster Recovery Plan (DRP) and procedures.
* Expertise in development of Information Security Programs based on frameworks such as NIST, NIST, NIST, ISO 27002, COBIT 5.0, FFIEC, GLBA, SOX, PCI & PII with IT Risk drivers KPI's and KRI's to ensure Financial regulatory compliance and data security.
* Conduct internal and external security audits based on standard cybersecurity frameworks from ISO 27002, COBIT, NIST, OWASP and Cloud Security Alliance
* Worked extensively in Configuring, Monitoring Elk, Extrahop.
* Built proof of concept (POC) for Localization to use AWS for some transcoding workloads. AWS services used were EC2, S3, Lambda, Elastic Transcoder. Second phase would be to add Captions and Digital Rights Management (DRM).
* Assessment guidance/standards used; NIST SP, NIST, NIST, ISO27002, ISO27005, to ensure regulatory compliance and proper assessment of risk.
* Using Confidential Phantom Security Orchestration, Automation, and Response (SOAR) system to evaluate notable event for correlation alert.
* Develop documentation for new/existing policies and procedures in accordance with Risk Management Framework (RMF), NIST SP requirements.
* Used GZIP with AWS Cloud front to forward compressed files to destination node /instances.
* Dynamic monitoring and analysis of Intrusion Detection Systems (IDS) to identify security issues for remediation. Analyse, recognize, correlate, and report any potential, successful, and unsuccessful intrusion attempts and compromises thorough reviews and analyses of relevant event detail and summary information from AccelOps SIEM, Snort logs and Checkpoint FW logs.
* Consulted with business and technology partners to create and provide security recommendations and best practices.
* Assisted CSO with completion of established goals, objectives, and streamlining of internal office procedures.
* Deployed the following Azure services to enable IT Security and IT Operations to move applications into the Azure cloud environment by allowing for monitoring and alerting: Azure Operations Management Suite (OMS), Service Map, Network Watcher, and Wire Data
* Conducted onsite penetration tests from an insider threat perspective.
* Performed host, network, and web application penetration tests.
* Provided leadership in architecting and implementing security solutions towards Qualys and SIEM tools like Splunk, Solution ARY, LogRhythm, SCCM, Altiris, LANDesk, BigFix, McAfee/Symantec.
* Push configurations and updates to multiple Splunk Enterprise instances via the Splunk Deployment Server
* Worked with Security Operations Center (SOC) web application security log analysis and Malware Analysis, Phishing / Spam email Investigation, EDR tool (Titanium / Crowd Strike/Carbon black and other relevant tools.
* Support the reporting and outputs from cross-functional teams related to the vendor risk assessment process
* Provide IT Governance, Risk, and Compliance (GRC) service to fulfil client requirements.
* Experience with SIEM platforms (Splunk, QRadar, McAfee/Nitro, ArcSight, LogRhythm, Carbon Black)
* Utilized Security Information and Event Management (SIEM), Intrusion Detection & Prevention (IDS / IPS), Data Leakage Prevention (DLP), forensics, sniffers and malware analysis tools, SSL/TLS, SOAP/XML, TCP/IP, HTTP and expertise in open ssl. Moreover, Experience in deploying and administering Dynatrace, APM Tools like Synthetic, DCRUM, UEM, & AppMon.
* Managed Cyber Security threats through prevention, detection, response, escalation and reporting in effort to protect Enterprise IT Assets through Computer Security Incident Response Team (CSIRT).
* Responsibilities for CSIRT included SIEM, Context Filtering, Web Security, Incident Tracking, IPS/IDS and Malware Analysis.
* Responsible for troubleshooting and resolving firewall software and hardware issues, including VPNs, connectivity issues, logging, cluster configurations, and hardware installations for Checkpoint and Palo Alto firewalls.
* Performed risk analysis using State approved risk analysis methodology based on NIST SP and ISO IEC 17799 methodologies.
* Increased productivity by fine-tuning their IPS security policies allowing analysts to quickly identify threats on the network. Tune HIPS and VirusScan policies to support mission requirements as needed.
* AWS CLI Auto Scaling and Cloud Watch Monitoring creation and update
* Participate in design efforts for network security related portions of new applications along with application development areas and the network design for disaster recovery efforts.
* Experience spans over SIEM, Threat Intelligence, Penetration Testing and Vulnerability Assessment, Security Architecture, PCI-DSS and Security Research.
* Provide expertise with incident response, security event monitoring, vulnerability management, asset security compliance and data loss prevention utilizing McAfee Nitro (SIEM), McAfee EPO, McAfee DLP.
* Performed investigation by traced IP using SIEM, Elasticsearch, Splunk, Adallom, Skyfence, Ping Identity, CA SSO Siteminder, Netskope for searching/indexing data including development for a new dashboard for IP Hopping, Brute force attack, emails user account, locate the perpetrator, records all footprint, location, IP Address, create report on evidence that can be collected.
* Expertise in development of Information Security Programs based on frameworks such as NIST, NIST, NIST, ISO 27002, COBIT 5.0, FFIEC, GLBA, SOX, PCI & PII with IT Risk drivers KPI's and KRI's to ensure Financial regulatory compliance and data security.
* Advise and implement Symantec Best Practices and configuration management in the environment.
* Working with a team where my primary responsibility is planning, installation, configuration, performance tuning, problem determination, and administration of a Security Information and Event Management (SIEM) solution.
* Initiated a vendor risk assessment program
* Used virtualization tools such as VMWARE and VIRTUAL BOX to build server infrastructure for ArcSight security solutions.
* Coach and mentor new analysts in our Third-Party Vendor Risk Assessment Program.
* POC and assisted in deployment for Bluecoat Security Analytics across BOA Data centres and remote offices, scripting and data extraction for SSL/TLS CPS utilization, Malware, Firewall and F5 capacity management and high availability planning.
* Design and implement a vendor risk assessment scorecard - to establish a risk benchmark, identify areas needing improvement, and as a periodic tool to assess overall risk status.
* Configuring and implementing F5 BIG-IP, LTM, GTM load balancers to maintain global and local traffic.

**Client: DePaul University, Stamford, CT** **February 2016–November 2017**

**Cyber Security Analyst**

**Responsibilities:**

* Proactively implemented updates, maintained, managed, monitored, and supported enterprise network and systems security operations infrastructure throughout the shared services environment.
* Perform daily DLP Incident monitoring, analysis and reporting, solution checks, client interaction, and day-to-day DLP operations.
* Managing SIEM - Net forensics
* Create and run routine reports and data analytics in Excel and Tableau. Audit and validate data/reports
* Responsible for delivering an end to end continuous integration - continuous delivery system for the products in an agile development approach using Chef/Ansible and Jenkins and Shell Scripts.
* Wrote Ansible playbooks to setup Continuous Delivery pipeline and this primarily consists of a Jenkins and Sonar server, the infrastructure to run these packages and various supporting software components such as Maven.
* Managed the large security, risk and compliance initiatives of SOX-404 IT, PCI DSS and HIPAA/HITECH, Privacy Act, and FTC including security policies, procedures and controls.
* Experience with Windows, Linux, vulnerability assessment tools, firewalls, IDS/IPS, HIPS/HIDS, Nessus, NMAP, SIEM, Splunk, Rapid7 Nexpose and Insight VM, WAF, routers, switches, VMware, Endpoint Security, Cloud Security, Symantec Endpoint Protection.
* Assesses a residual risk rating for the vendor based upon their control environment.
* Worked on various network and system security technologies including SIEM, EDR, Malware analysis, Threat Intel, Email Security, IPS/IDS, Perimeter Security
* Monitor, analyse and 0respond to network incidents and events. Participate in disaster recovery implementation and testing under NIST framework, HIPPA, & HITECH standards.
* Developed approaches for industry-specific threat analyses, application-specific penetration tests and the generation of vulnerability reports.
* Work with the network team to architecture Azure and AWS VPN, AWS Direct Connect, and Azure Express Route connections.
* Built the Security Orchestration, Automation and Response (SOAR) program centered on ServiceNow, Swimlanes, Qualys Vulnerability Scanner, Carbon Black, Symantec DLP, and Splunk.
* Providing proper remedy to fix vulnerability in the client network after analysing security incident queries alerted by ArcSight Performing Vulnerability Assessments and taking the required counter actions and measurements to ensure the security of the IT infrastructure / systems.
* Analysis and documentation of network & information security requirements and define security policy for enterprise client and business critical servers.
* Perform daily duties supporting and trouble-shooting digital rights management on a Windows and Linux Platform, while defining and implementing patching
* Build and operate a security & awareness program relating to vendor risk management program
* Experience implementing/architecting cloud-based Active Directory solutions for Azure and AWS
* Performing system auditing using audit reduction tools; following up on audit findings; maintaining authorization documents; and supporting the local Information Systems Security Manager (ISSM) as needed to maintain system authorization.
* Implementation of Symantec Mail Security for SMTP and Symantec Endpoint Protection.
* Experienced with tools like Metasploit/Qualys/Network forensics technologies
* Respond to inbound security monitoring alerts, emails, and inquiries that arose from various monitoring tools that included Symantec DLP.
* Performed application security and penetration testing using IBM Ashcan.
* Perform vendor risk assessments as assigned. Work with vendors and business owners to gather documentation and develop vendor remediation plans.
* Addressed critical areas of potential information security risks and opportunities with gap analysis for Data protection, Cloud Security and Data Classification and handling of tools (Trend Micro and IBM QRadar).
* Used Microsoft Azure Security centre to monitor the cloud environment.
* Worked on AWS designing and followed Info security compliance related guidelines.
* Collaborate across the entire organization to bring Splunk access to product and technical teams to get the right solution delivered and drive future innovation gathered from customer input.
* Design, Deploy, support and maintain Splunk cluster infrastructure in a highly available, geo-redundant configuration Develop, implement, and execute standard procedures for the administration, content management, change management, version/patch management, and lifecycle management of the firm’s enterprise security platforms
* Use Carbon Black (CB Défense), McAfee Nitro and Splunk Enterprise SIEM security tools to monitor environment
* Judged DIAR on the 12 PCI-DSS audit requirements as well as the 80 Sub-Requirements to determine strengths and weaknesses for audit preparedness.
* Worked on projects moving to cloud services such as Azure, Office 365 and Amazon Web Services (AWS).
* Knowledge and experience in IT risk or compliance disciplines including risk assessment.
* Establish a strong GRC (Governance, Risk and Compliance) practice to ensure adherence to best practice, regulatory requirements and ISO 27001.
* Websense, Symantec Endpoint Protection and Active Directory (User Account Management specific) events monitoring and analysis.
* Infrastructure security design and implementation expertise (Firewall, IDS/IPS, SIEM, Proxy services, Antivirus, Vulnerability Management, Key management, Web application firewall and PKI).
* Management of Cloud security, Vulnerability assessment, and security audits.
* Review and updated System Security Plan (NIST SP), Risk Assessment (NIST SP), and Security Assessment Report (NIST SP A).
* Reducing Proofpoint Digital Risk to defend impersonation of the brand to harm current market.
* Managing SIEM - Net forensics, its prevention controls, Penetration testing
* Perform personnel interviews during assessments and review proper analysis of testing results.
* Review documentation as applicable to controls for compliant/non-compliant status.
* Ability to provide an independent assessment per control and ensure security controls are implemented correctly; operating as intended; and are producing the desired outcome.
* Designed and documented Compliance logging & auditing strategy, provide analysis and trending of security log data from security devices, provide threat and vulnerability analysis as well as security advisory services.
* Exposure to EDR Tools such as CrowdStrike Falcon, Vulnerability Scanning Tools like Tenable Nessus, as well as Kali Linux, SentinelOne.
* Co-ordinating pen testing and application security testing audits with Pen Test Tools like Metasploit, NMAP, Wireshark and Kali on Linux/Unix operating system.
* Monitoring and remediating daily security alerts generated by end users with the tools like Intel/McAfee SIEM, Forcepoint’s Websense, and Intel/McAfee EPO 5.X and also responsible for effectiveness of tools and scans, as well as assessing and tracking risk of exposure.
* Respond to security incidents and follow through to resolution, reporting, and lessons learned phases.
* Cisco ASA/Palo alto firewall troubleshooting and configuring policy based on change request, allowing/denying communication between different segment of the network based on requested ports.
* The SOAR program now handles 75% of security events. Took a leading role in developing the Identity Access Management (IAM) program using CyberArc.
* Conduct vulnerability scans to support to our risk/threat/vulnerability management program including resolving risks and the documentation of any residual risks.
* Maintain serviceability of assessment tools with latest software and firmware resulting in zero equipment failure during assessments
* Identifying flaws and weaknesses in information systems that may be exploited to impact the confidentiality, integrity and availability of a system.
* Prioritize vulnerabilities/assets that should be patched during maintenance cycles.
* Analyse vulnerability assessment results, identify remediation strategies and provide timely reports to management for review.
* Configured AWS Identity Access Management (IAM) Group and users for improved login authentication.
* Solution partner product compatibility validation with Cisco UCS servers. Functional and Feature testing of various datacentre and IT solutions and extracting test results for the quarterly marketing press release for Cisco partners.
* Investigate, document, and report on information security issues and emerging trends, Implemented Strategy for Security Compliance and Auditing (HIPAA, SOX). Coordinate with Symantec technical support to resolve product issue escalations to assist in faster resolution and reduce unplanned downtime.
* Used Splunk to analyse Bluecoat, Palo Alto, Juniper firewall, Windows Infrastructure logs. Configured UTM policies in juniper SRX 3600.