**Kavan D**

**Cyber Security Engineer**

**PH No: 929-459-8188**

**Email:** **Kavan384@gmail.com**

**SUMMARY:**

**Professional Summary:**

* Experienced Technical Consultant having experience in handling Information security analyst and System Administrator responsibilities.
* Analyze, troubleshoot, and investigate security-related, information systems' anomalies based on security platform reporting, network traffic, log files, host-based and automated security alerts.
* Monitor and analyze output and performance of network and host-based security platforms including
* Vulnerability scanning systems and tools.
* Network-based Intrusion Detection/Prevention Systems (IDS/IPS)
* Host-based Intrusion Detection/Prevention Systems (HIDS/HIPS)
* Spam Emails Investigation.
* Security Information & Event Management (SIEM) platform
* Antivirus and anti-spyware logs and events
* Web proxy and filtering systems
* Execute routine and ad-hoc vulnerability scans and other tests to verify system security settings and configurations.
* Assist in maintenance of relevant system and process documentation
* Establish and maintain a strong working relationship with all team members.
* Provide off-hours support on and as needed basis IT professionals.
* Participated Ransomware attack investigation process.

**Trained on Technologies:**

IBM Qradar, Fireeye Incident Response and Forensic Investigation, Cisco AMP Endpoint Security, Firepower Management with Security Intelligence feature, Cisco IPS, Cisco Email Security,

Cisco Umbrella, Trend Micro Spam Filters, Nexpose, Fireeye HX, CyberArk, etc.

**CERTIFICATION:**

CompTIA Network+ (Dec 2019 – Dec 2022)- COMP001021604578

**EDUCATION:**

Bachelors in Electronic and Communication Engineer (ECE)

**TECHNICAL SKILLS:**

|  |  |
| --- | --- |
| **Networking**  | Packet Analysis (tcpdump, Wireshark), IDS (Bro, Snort), Splunk, Firewall, IDS/IPS, Access Control  |
| **Systems Administration** | Active Directory, DNS, FTP, SSH, DHCP, SMB, HTTP, Virtualization (ESX)  |
| **Vulnerability Assessment** | Nmap, Nessus, Ettercap, Metasploit, Honeypots (honeyD, INetSim), BurpSuite  |
| **End Point Security** | McAfee Suits (VSE, HIPS & HDLP), McAfee MOVE AV, Symantec McAfee Email Security Gateways GUI & CLI, McAfee Network Data Loss Prevention, McAfee NITRO SIEM Security Information and Event Management. |
| **Platforms/Applications** | Continuous Monitoring Vulnerability Management, Web Application Scanning, Threat Protect, Policy Compliance, Cloud Agents, Asset Management, Governance, Risk Management and Compliance, SolarWinds, Nexpose, Rapid7 Event Management RSA Archer, Blue Coat Proxy, IBM QRadar, NTT Security, LogRhythm, PenTest Tools Metasploit, Burpsuit, NMAP, Wireshark and Kali  |
| **Security Software** | Nessus, Ethereal, NMap, Metasploit, Snort, RSA Authentication, PIA  |
| **Programming Languages** | C, C++, Java, Python, JavaScript, Linux, PowerShell  |
| **Networking** | LAN, WAN, Wi-Fi, DNS, WINS, DHCP, TCP/IP, ISCSI, Firewalls/IPS/IDS  |
| **Protocols** | TCP/IP, L2TP, PPTP, IPSEC, IKE, SSL, SSH, UDP, DHCP, DNS, NetBIOS, SNMP, TLS etc.  |
| **Domain Knowledge** | Risk Management, BCP/DRP, ISO 27001, COBIT, Vulnerability [SWOT analysis, Cryptography, Incident Response, Penetration Test, Risk Assessment, SCADA Security, SCADA Audits, SIEM, NIST, FIPS] |

**PROFESSIONAL EXPERIENCE:**

**Conduent, Austin, TX June 2019 to till Now**

**Cyber/Network Security Engineer**

**Responsibilities:**

* Interface with users, technicians, engineers, vendors and other Technical Maintenance personnel to install, update and debug automated systems.
* Ensure products and systems comply with cyber security standards and practices. Develop test routines and monitoring solutions. Penetration testing using Nmap and Wireshark.
* Provide day to day support of servers, workstations, network and other equipment. Document support procedures specific to systems to be utilized by the Technical Maintenance and Engineering departments.
* Plan, execute and oversee remediation activities for valid vulnerabilities which are identified using Application Scanning tools. Experience with application scanning to identify security vulnerabilities in the web application and architectural weaknesses.
* Effectively communicate with Business Operations and other functional areas on web application vulnerabilities. Experience in planning, installing, configuration, and administering IBM Security Identity Manager 7.0.1. Support, performance tuning and troubleshooting ISIM 7. Configure and manage ISIM 7 security e.g. configuration of single sign-on, secure communication with supported middleware etc.
* Hands-on technical experience with testing of web applications in Java or .NET, Experience with audits, e.g. A-123, SOC 1/2, FISCAM. Radius and Kerberos Server experience. API testing using Postman.
* Experience using DAST tools to detect potential vulnerabilities such as HP Web inspect, SolarWinds, Zap, Burp, Tenable, Splunk, Alertlogic, Symantec Endpoint Protection, Zscaler, McAfee security, Portswigger, Fiddler, Wireshark, Nmap, JIRA, Sonatype, Coverity. Experience in Palo Alto Networks and Firewall (PA-5000, PA-3000, PA-500) series, PA IPsec VPN Tunnel.
* Experience with Red hat Linux Server, macOS Server, Microsoft Windows Server, MS Active Directory, Azure AD, Configure and manage AWS/Azure Cloud Infrastructure, Virtualization (VMware NSX, Hyper-V). Extensive experience hands-on Azure IaaS / PaaS. Experience designing and building Azure solutions. PowerShell experience as it relates to Azure, AD, and Office 365.
* Deploy, manage and effectively maintain security systems and their corresponding or associated software, including firewalls, checkpoint firewall, squid firewall, blue coat proxy and routers, IDS, IPS, cryptography systems, Encryption (RSA, AES), Tokenization (OpenNMT), and anti-virus software. Experience in Python, PowerShell and JavaScript programming language.
* Audit and adjust permissions, access-lists, file shares, and any other access control mechanism in place. Troubleshoot and document network security incidents. Produce and present security reports for management. Monitor and analyze network security data.
* Experience setting up Firewalls, using NAV tools, Vulnerability Management platforms, Security Analytics platforms, Penetration Testing frameworks (Metasploit or Resolve).
* Advanced knowledge of Cisco wireless LAN controllers, Cisco access points, Cisco ISE, Cisco routers (Cisco 1921, Rv320, Rv215w, Rv042, Rv042G), Cisco L2/L3 switches, Cisco Prime, Generic Routing Encapsulation, load balancing (F5 BIG-IP Local Traffic Manager, Cisco Load Balancer, Citrix, Azure load balancer), QOS, PBR, WCCP, VPN, NAT, VoIP, IPsec, Multicast, DNS services, MPLS networks, LAN, WAN, Juniper Networks Firewall (Juniper EX series EX2300, EX4300, EX3400, QFX5100-48T, QFX10002-36, SRX series, Cisco ASA firewalls/Router (5508-x with firepower, 5516, 5585, 5545, 5555), Cisco Meraki MX100 Firewall, and network and routing protocols (Ethernet, TCP/IP, SNMP, VLAN Trunk, BGP, OSPF, ISIS, EBGP,IBGP,RIP).
* Experience utilizing Wi-Fi analyzers, Wi-Fi survey software tools (i.e. Air Magnet, Ekahau, etc.) and test equipment. Experience working across the full stack of enterprise security tools to include everything from the physical layer to the application layer. Cisco Nexus series 5k, 7k, 9k switches, Cisco Catalyst Switches (2960, 3560, 6500), Cisco 300/200 series.
* Ability to lead the design of network security infrastructure and the integration of new requirements into existing architectures. Experience leading compliance assessments of relevant cybersecurity frameworks.
* Remain informed on trends and issues in the security industry, including current and emerging technologies and policies.

**TJX Companies, Marlborough, MA Jun’ 2018 to May’ 2019**

**Sr. Cyber Security Analyst**

**Responsibilities:**

* Analyze, troubleshoot, and investigate security-related, information systems' anomalies based on security platform reporting, network traffic, log files, host-based and automated security alerts.
* Monitor and analyze output and performance of network and host-based security platforms including: Vulnerability scanning systems and tools, Network-based Intrusion Detection/Prevention Systems (IDS/IPS), Host-based Intrusion Detection/Prevention Systems (HIDS/HIPS), File integrity verification and monitoring software (FIM), Security Information & Event Management (SIEM) platform, Data Loss Prevention (DLP), Log Indexing and Correlation tools, Anti-virus and anti-spyware logs and events, Web proxy and filtering systems.
* Execute routine and ad-hoc vulnerability scans and other tests to verify system security settings and configurations.
* Execute, organize and distribute reoccurring and ah-hoc reports for network and host-based security solutions
* Proficient in understanding application level vulnerabilities like XSS, SQL Injection, CSRF, authentication bypass, weak cryptography, authentication flaws etc.
* Assist in maintenance of relevant system and process documentation.
* Establish and maintain a strong working relationship with all team members.
* Acquainted with various approaches to Grey & Black box security testing.
* Generate and present reports on Security Vulnerabilities to both internal and external customers.
* Manual and Dynamic penetration testing of web applications using Burp Suite and App Scan.
* Configuration of the IBM App Scan tool to meet individual scanning requirements.
* Security assessment of online applications to identify the vulnerabilities in different categories like Input and data Validation, Authentication, Authorization, Auditing & logging.
* Vulnerability Assessment of various web applications used in the organization using Paros Proxy, Burp Suite and HP Web Inspect.

**Solera Holdings, Austin, TX Sep’2016 –Jun’2018**

**Sr. Cyber Security Engineer/Analyst**

**Responsibilities:**

* Establish a strong GRC (Governance, Risk and Compliance) practice to ensure adherence to best practice, regulatory requirements and ISO 27001.
* Adept with QRadar, Symantec PCAP, Symantec CloudSOC, PAN Firewall, PAN Wildfire, PAN TRAPS, PAN Redlock, FireEye, ThreatQ, Microsoft SCEP, Microsoft O365 Security and Compliance Portal, Proofpoint.
* Working with McAfee ePO for managing client's workstations for providing end point security.
* Facilitate implementations of information security policies, account security policies and standards for logical and physical security.
* Worked on SIEM, as well as solar winds, Symantec end to end point security for malware detection and threat analysis.
* Experience with national, international, and/or sectoral cloud security assurance/compliance regimes and frameworks such as Federal Risk and Authorization Management Program (FedRAMP), Federal
* Responsible for performing application penetration testing on web, thick client, and other types of applications to identify significant vulnerabilities that threaten the confidentiality, integrity, and availability of customer systems.
* Implementation and configuration of the network infrastructure in Business environment.
* Installation and maintenance of McAfee Drive Encryption used to encrypt all workstation hard drives in the environment to secure the data stored on them.
* Installation, maintenance and monitoring of McAfee Data Loss Prevention Endpoint, one piece of the Removable Media Encryption suite
* Installation "maintenance and monitoring of McAfee File and Removable Media Protection, the second piece of the Removable Media Encryption suite
* Setup and configuration of test benches includes configuring Cisco UCM, 29xx/3800 series routers, Cisco 7975/9971 IP Phones, RSVP gateways, POE switches and Media servers implemented all VMware configurations for CUCM installs using vSphere.
* Implemented and configured CASB solution including Netskope to secure the enterprise with a cloud.
* Tested and certified new software such as Tanium Protect (an access control software) and PEGA trouble ticketing software.
* Audit Support: Facilitated the PCI DSS external audit for the client, took charge of end to end co- ordination and support during the onsite assessment.
* Oversee the design and development of security solutions and manage cross-platform integration of a range of on-premised and public cloud security designs and configurations, Amazon CloudFront and Amazon Route 53.
* Troubleshooting day to day issues in IT infrastructure in Business Environment tools like Splunk, ArcSight, Solutionary, PIA, LogRhythm, SCCM, Altiris, LANDesk, BigFix, McAfee/Symantec.
* Automated DLP Incident metrics using Splunk. Developed monthly, weekly metrics and dashboards using Splunk.
* Provided leadership in architecting and implementing security solutions towards Qualys and SIEM tools like Splunk, ArcSight, Solutionary, LogRhythm, SCCM, Altiris, LANDesk, BigFix, and McAfee/Symantec.
* Configured Advance CyberArk integration with AD through LDAP, 2factor authentication & email integrations.
* Utilizing Tanium Endpoint Security to create reports to resolve various information security issues.
* Experience with Risk assessment, Cobit I help Malware Analysis.
* Coordinates closely with disaster recovery and data security teams.
* Enhancing Risk culture across the organization based on COSO framework. Applying and implementing COSO framework across organization
* Allocate/coordinate work within a team/project. Provides value input into risk reports. Presents reports to the business areas and CTS management.
* Working as Device Management in-charge to provide technology support, install, maintain, upgrade, and troubleshoot server's issues, networks, other security products, providing solutions to complex hardware/software problems.
* Working as a dedicated resource for a Scrum Project to provide timely firewall support and configuration for ongoing high priority Scrum Projects.
* Vulnerability Assessment and Management (Nessus &Qualys), Security risk analysis; reporting using SPLUNK.
* Conduct daily IDS analysis/monitoring for potential compromise, intrusion, deficiency, significant event or threat to the security posture and security baseline and numerous activities against spam.
* Utilize Security Information and Event Management (SIEM), Intrusion Detection & Prevention (IDS / IPS), Data Leakage Prevention (DLP), forensics, sniffers and malware analysis tools
* Implemented multiple tools including Symantec DLP, and QRadar SIEM.
* Deploying and configuring McAfee products for client. Providing SME for McAfee suite of products like McAfee ePO, McAfee Endpoint Encryption, McAfee DLP Endpoint
* Manage IBM QRadar configuration files like inputs, props, transforms, and lookups. Upgrading the IBM QRadar Enterprise and security patching.
* Leading a SOC team for cyber incidence and compliance towards PCI DSS, NIST framework.
* Installed, configured and administered Splunk Enterprise Server and Splunk Forwarder on Redhat Linux and Windows servers.
* Configuration and Maintenance of MPLS between satellite locations and Data center. Rule Management for MPLS routers.
* Tracks all the incidents happened in all the stores and used for recovery and settlements using RSA Archer.
* Experience with SIEM platforms (Splunk, Qradar, McAfee/Nitro, ArcSight, LogRhythm, Carbon Black)
* Administration experience of CyberArk vault with Safe creation, integration with LDAP and other authentication methods & Creation of policies and reports in PVWA.
* Had to deal with SIEM solutions such as Rapid7 Nexpose, Forcepoint, Splunk
* Experience in analyzing the logs and Trouble Shooting issues in Integration of other applications using CA SiteMinder (Access Management) and Identity Management tools along with LDAP and Web-server agents and SiteMinder federation services.
* Projects that installed deployed and/or maintained multiple security solutions for security tools such as Nexpose Rapid 7, Comodo, Qualys, and threat stop.
* Installation and configuration of CyberArk Vault, Password Vault Web Access (PVWA), Central Password Manager (CPM) and Privileged Session Manager (PSM) in Prod and PIA.
* Working on the Security tools like Deep Security, HIPPM, Nessus, and Symantec Control Compliance Suite 11.

**Hospira, Lake Forest, IL Feb’2015 – Aug’2016**

**Cyber Security Engineer**

**Responsibilities:**

* Experience with many of the following technologies/roles: Privileged Account Management, Two-Factor Authentication, Web filtering, Web Application Firewalls, Virtualized computing environments, Encryption-at-rest and encryption-in-transit, Vulnerability Management.
* Installation and configuration of networks and network devices such as web application firewalls, network firewalls, switches, checkpoint firewall, squid firewall, blue coat proxy and routers.
* Network Security configuration, audit, and management of Windows servers. Installation, configuration, audit, and management of security tools.
* Security configuration, audit, and management of applications and databases. Leading security incident investigations, including basic forensic analysis and reporting. Deploying, automating, maintaining and managing AWS cloud-based production system, to ensure the availability, performance, scalability and security of productions systems.
* Maintenance and monitoring of network and host intrusion detection and prevention technologies. Implementing security controls. Experience with using a broad range of AWS technologies (e.g. EC2, RDS, ELB, EBD, S3, VPC, Glacier, IAM, CloudWatch, KMS) to develop and maintain an Amazon AWS based cloud solution, with an emphasis on best practice cloud security.
* Implemented physical and procedural safeguards for information resources within the facility. Communicate effectively with senior management, peers, staff, and customers both inside and outside the corporation.
* Administered access to information resources and makes provisions for timely detection, reporting, and analysis of actual and attempted unauthorized access to information resources.
* Proposed and assisted with the acquisition of security hardware/software. Develops and maintains access control rules. Experience with VOIP systems.
* Maintains user lists, passwords, encryption keys, and other authentication and security-related information and databases.
* Experience using DAST tools to detect potential vulnerabilities such as HP Web inspect, SolarWinds, Zap, Burp, Tenable, Splunk, Alert logic, Symantec Endpoint Protection, Zscaler, McAfee security, Portswigger, Fiddler, Wireshark, Nmap, JIRA, Sonatype, Coverity. Experience in Palo Alto Networks and Firewall. Experience in maintaining local and remote networks.
* Lead the design, implementation, and migration of enterprise infrastructure and application services to software defined networks. Experience in Palo Alto networks and firewall. Configure and manage AWS/Azure cloud infrastructure.
* Develops and leads procedure for testing disaster recovery plan. Provides help-desk-style assistance.
* Administered MS Windows Server, Red Hat Linux Server, and Network/Security Administration.
* Advanced knowledge of Cisco wireless LAN controllers, Cisco access points, Cisco ISE, Cisco routers, Cisco L2/L3 switches, Cisco Prime, Generic Routing Encapsulation, load balancing (F5 BIG-IP Local Traffic Manager, Cisco Load Balancer, Citrix, Azure load balancer), QOS, PBR, WCCP, VPN, NAT, VoIP, IPsec, Multicast, DNS services, MPLS networks, LAN, WAN, Juniper Networks Firewall, Cisco ASA firewalls and network and routing protocols (Ethernet, TCP/IP, SNMP, VLAN Trunk, BGP, OSPF, ISIS, EBGP,IBGP,RIP).
* Excellent written and verbal communication skills. Ability to create, update and maintain technical documentation. Ability to work independently. Experience with ServiceNow.
* Provided guidance and policy regarding the administration of all computer security systems and their corresponding or associated software, including endpoint security, intrusion detection systems, and application whitelisting.
* Participated in strategic security relationships between internal resources and external entities, including government, customers, vendors, and partner organizations.
* Experience with using a broad range of AWS technologies (e.g. EC2, RDS, ELB, EBD, S3, VPC, Glacier, IAM, CloudWatch, KMS) to develop and maintain an Amazon AWS based cloud solution, with an emphasis on best practice cloud security. Extensive experience hands-on Azure IaaS / PaaS. Experience designing and building Azure solutions. PowerShell experience as it relates to Azure, AD, and Office 365.

**IMI Mobile, India Jun’2013 – Dec’2014**

**Security Analyst**

**Responsibilities:**

* Performed grey box testing of the web applications
* Executed and crafted different payloads to attack the system for finding vulnerabilities with respect to input validation, authorization checks, and more
* Reviewed and Validate the User Access Compliance on a quarterly basis
* Reviewed the requirements for privileged access on an everyday basis and provide recommendations
* Reviewed and validate the privileged users and groups at Active Directory, Databases and application on a periodic basis
* Documented information security guidance in step by step operational procedures
* Performed static code reviews with the help of automation tools
* Performed a threat analysis on the new requirements and features
* Burp Suite, DirBuster, Hp Fortify, NMap tools were used as part of the penetration testing, on daily basis to complete the assessments
* Established and improved the processes for privileged user access request
* Reviewed firewall rules and policies in web proxy
* Highlighted the user access and privileged user access risks to the organization and providing the remediation plan.