**PROFESSIONAL SUMMARY:**

* Cisco Certified Network Engineer with 10+ years of experience in the industry, which includes expertise in the areas of Routing, Switching, Firewall and Load Balancing.
* Strong hands on experience in installing, troubleshooting, configuring of Cisco 7200, 3800, 3600, 3400, 2800, 2600, 2500, 1900, 1941, 1921 and 1800 series Routers, Cisco Catalyst 6800, 6807, 6500, 4500, 3750, 2950, 2960 and 3500XL series switches.
* Managed RADIUS logs to monitor access attempts and troubleshoot authentication failures, improving overall network security.
* Worked with multicast address allocation and registration to ensure efficient and non-overlapping multicast group management.
* Monitored network performance on Arista switches, using Telemetry and Analytics to ensure uptime.
* Provided training and support to network teams on SDN concepts, tools, and best practices.
* Implemented redirects and rewrites to improve HTTP/HTTPS traffic management.
* Managed Azure Kubernetes Service (AKS) for containerized application deployments and security.
* Monitored cloud resource performance and availability using Azure Monitor, Application Insights, and custom alerts.
* Integrated BGP with MPLS for large-scale network deployments, ensuring reliable connectivity across multiple sites.
* For improved application functionality, SQL has been integrated with various programming languages (such Python and Java).
* Created reusable Python modules and functions to streamline code development and maintenance.
* Solid knowledge and hands-on experience in configuring datacenter infrastructure with Cisco Nexus 9K, 7K, 5K series switches (5548, 7010) and Cisco Nexus Fabric Extenders (2232, 2248).
* Expert in configuring 802.1d STP and 802.1w rapid-spanning tree protocol (RSTP), Cisco per VLAN spanning Tree (PVST+) / Multiple Spanning-tree 802.1s, VLAN & Dynamic Trunking Protocol (VTP/ DTP) and 802.1x port-security on access layer switches.
* Implemented network segmentation and security policies on Arista equipment to safeguard sensitive data.
* Documented Ciena configuration processes and provided training to junior network engineers.
* Implemented policy-driven automation in SDN environments, increasing network agility and reducing errors.
* Hardened HTTP servers against attacks like DDoS, cross-site scripting (XSS), and injection.
* Created and maintained documentation on Zeek configurations and standard operating procedures.
* Integrated Palo Alto solutions with cloud services and automated security workflows.
* Deployed guest Wi-Fi solutions with secure and isolated network segmentation.
* Conducted firmware and software updates on Ciena equipment to maintain security and performance.
* Performed wireless site surveys to identify signal strength and interference sources.
* Implemented search optimization techniques to improve document retrieval on the intranet.
* Provided Visio training and support to team members to optimize their use of the tool.
* Developed custom subnetting solutions to accommodate VPN clients and remote workers while maintaining security.
* Configured OSPF stub and totally stub areas to optimize routing in smaller network segments and reduce overhead.
* Hands on Experience in configuring, implementing and troubleshooting SDWAN devices like Velocloud and Versa Networks
* Monitored system health and performance metrics, utilizing Nutanix's built-in monitoring and analytics tools.
* Troubleshooted and resolved issues related to Cisco Nexus 9K VPC, VXLAN, and Layer 2/Layer 3 configurations.
* Expert level knowledge of troubleshooting, implementing, optimizing and testing of static and dynamic routing protocols such as EIGRP, OSPF, BGP, ability to interpret and resolve complex route table problems.
* Implementation traffic filters on Cisco routes using Standard, extended Access list and expert level knowledge about TCP/IP and OSI models.
* Facilitated data backup and disaster recovery solutions using Azure Backup and Site Recovery.
* Managed firmware updates and security patches for Wi-Fi devices.
* Upgraded wireless hardware and software to the latest standards.
* Integrated RADIUS with Cisco, Juniper, and Fortinet devices to manage device access and policy enforcement.
* Implemented AWS Route 53 for domain management, traffic routing, and failover across distributed environments.
* Utilized BGP confederation and route reflectors to optimize large-scale iBGP deployments, reducing the number of peerings.
* Optimized Django applications for performance, reducing load times and improving user experience
* Managed and maintained Windows client systems across the organization, ensuring consistent software deployments, updates, and compliance with IT policies.
* Integrated dynamic IP addressing using DHCP within subnetted networks, simplifying IP management for large-scale environments.
* Trained team members on Zeek’s use for network monitoring and incident response.
* Monitored intranet usage to identify areas for performance improvement.
* Implemented Azure Backup and Azure Site Recovery (ASR) for disaster recovery planning and business continuity.
* Experience of OTV, VXLAN with Strong understanding of SDN and SDWAN.
* Created additional site-to-site IPsec VPN to Connect SD-WAN to Zscaler for cloud-based security.
* Assisted in migration from DMVPN to Cisco Meraki SD-WAN.
* Updated training Silver Peak SDWAN, SolarWinds, Splunk, Aruba wireless, F5 LTM/GTM & Cisco.
* Design expertise for the SD-WAN (Versa & Viptela), SD-LAN and WAN optimization technologies for efficient delivery of the application data across LAN and WAN.
* Facilitated employee training on effectively navigating the intranet platform.
* Configured AWS S3 lifecycle policies for automated data archiving and cost-effective storage management.
* Collaborated with teams to design and develop Python-based solutions for complex business challenges.

**TECHNICAL SKILLS:**

|  |  |
| --- | --- |
| Networking Technologies | LAN/WAN Architecture, TCP/IP, Frame Relay, VPN, VLAN, VTP, NAT, PAT, STP, RSTP, PVST, MSTP |
| Networking Hardware | Cisco Switches, Cisco Routers, ASA/Pix/Palo Alto/Fortinet/Juniper firewalls. |
| Routing Protocols | OSPF, ISIS, EIGRP, RIP, MPLS, IS-IS, BGP, Multicasting, Velocloud |
| Security Technologies | PAP, CHAP, Cisco PIX, Blue Coat, Palo Alto, ASA, Fortinet, Checkpoint |
| Network Monitoring | SolarWinds, Wireshark, HRping, Whatsupgold, Infoblox |
| Operating Systems | Windows 7, Vista, XP, 2000, LINUX, Cisco IOS, IOS XR, IOS-XE, NX-OS |
| Routers | CISCO 4300, 4400, 4500,2600, 2800,3800,7200, Juniper M & T Series, ASR 1000 |
| Load Balancers | F5 Networks (BIG-IP), NetScaler (Citrix), Avaya |
| Capacity & performance | Cascade Riverbed (Flow Monitor), WAN Killer |
| Switches | CISCO 2960,3750,3850, CAT 9300, CAT9400, CAT 9500,4500,6500,6800 Nexus 9K,7k,5k,2k, Arista, Avaya |
| Programming Languages | Ansible, Python |
| Simulation Tools | GNS3, VMware, OPNET IT GURU, OPNET Modeler, Cadence |
| Firewalls | Juniper Net Screen (500/5200), Juniper SRX (650/3600), Pix (525/535), ASA (5520/5550/5580), McAfee Web Gateway, Checkpoint, Palo Alto firewalls. |
| AAA Architecture | TACACS+, RADIUS, Cisco ACS |
| Features & Services | IOS and Features, HSRP, GLBP, VRRP, IPAM IRDP, NAT, SNMP, SYSLOG, NTP, DHCP, CDP, DNS, TFTP and FTP Management, Open Stack, IVR’s, HLD and LLD documents, Dell equal logics |

**PROFESSIONAL EXPERIENCE:**

**BNY Mellon, Irving, TX**  **Oct 2021 – Present**

**Senior Network Engineer**

**Responsibilities:**

* Involved in complete LAN, WAN development (including IP address planning, designing, installation, configuration, testing, maintenance etc.).
* In-depth understanding of the TCP/IP protocol stack, including TCP, UDP, IP, and ICMP, for seamless network communication.
* Configured Cisco SNA to monitor network behavior, detect anomalies, and mitigate cybersecurity threats in real-time.
* Configured Cisco ISE for role-based network access control and to enhance network security posture.
* Used Netconf for remote configuration and management of network devices.
* Configured and customized SolarWinds modules to monitor network performance and identify potential bottlenecks.
* Managed and configured iEN for secure and efficient edge connectivity in distributed networks.
* Configured and managed Ciena optical networking solutions, enhancing data transport efficiency and network capacity.
* Designed and deployed SDN architecture for enterprise networks, improving network flexibility and scalability.
* Monitored and analyzed network traffic patterns to detect signs of APT activity and infiltration.
* Configured SSH servers with strong encryption algorithms to secure remote access.
* Configured and optimized OSPF in multi-area environments, including stub and totally stub areas, to reduce routing table size and improve convergence.
* Conducted User Acceptance Testing (UAT) for network automation solutions to ensure end-user requirements are met.
* Used RSVP to establish LSPs that meet specific QoS requirements for critical applications.
* Configured and maintained DNS servers, ensuring reliable name resolution.
* Hands-on experience with Fortinet firewalls, configuring policies to control inbound and outbound network traffic.
* Troubleshot RSVP signaling and reservations to maintain uninterrupted service in multi-site networks.
* Configured Arista switches and routers to enhance data center connectivity and support scalable network architectures.
* Monitored HTTP traffic for suspicious patterns, such as unusual requests and headers.
* Managed and secured Industrial Control Systems (ICS) and SCADA networks, ensuring the integrity and availability of critical infrastructure.
* Configured F5 BIG-IP Local Traffic Manager (LTM) to optimize application delivery, including load balancing HTTP/HTTPS traffic using advanced algorithms like least connections and round-robin.
* Monitored infrastructure health using SolarWinds NPM for early identification and resolution of network issues.
* Experienced in configuring and troubleshooting network services such as DNS, DHCP, and NAT within TCP/IP environments.
* Analyzed network traffic data using SNA to uncover unusual patterns and potential breaches across multi-site environments.
* Configured TACACS+ for centralized user authentication, ensuring secure access control to network devices.
* Monitored network health and performance from the NOC, ensuring 24/7 availability and uptime.
* Configured and managed enterprise WLAN deployments for high availability and secure wireless access.
* Implemented 802.1X authentication policies with Cisco ISE to control network access based on device identity.
* Worked with Nokia SR OS for configuring high-performance IP/MPLS networks.
* Implemented iEN solutions to support low-latency applications at network edges, enhancing user experience.
* Configured SDN controllers like OpenDaylight and Cisco ACI to centralize network control and management.
* Worked with LDP to automate the creation and maintenance of label mappings, streamlining network operations.
* Conducted digital forensic investigations on compromised systems, identifying root cause and attack vectors.
* Utilized PCAP data to validate IDS/IPS alerts and improve detection accuracy.
* Configured and maintained SIEM solutions for centralized security monitoring.
* Integrated IDS/IPS with SIEM for centralized log management and alert correlation.
* Designed and implemented secure Azure environments using Azure AD, RBAC, and custom policy definitions.
* Collaborated with cross-functional teams to integrate RF systems with existing network infrastructure, enhancing overall performance.
* Utilized Infoblox IPAM for centralized management of IP address allocation, ensuring efficient use of IPv4/IPv6 subnets, and automated discovery of network devices to maintain an accurate inventory of IP resources.
* Implemented SSL offloading on F5 devices to reduce the encryption/decryption workload on backend servers, enhancing performance and security.
* Performed troubleshooting of OSPF Link-State Advertisements (LSAs) to resolve issues related to neighbor adjacency, stuck states (INIT/EXSTART), and route flapping in dynamic network environments.
* Experienced in setting up alerts within SolarWinds to notify of critical system or network component failures.
* Configured Fortinet’s VPN solutions to enable secure remote access and site-to-site communication.
* Implemented TCP/IP subnetting and address allocation strategies for optimizing network traffic flow.
* Implemented SNA for automated threat detection and response, reducing response time for incident management.
* Implemented TACACS+ policies to restrict and audit access to critical network infrastructure.
* Responded to alerts and incidents in the NOC, providing first-level diagnostics and troubleshooting.
* Implemented WPA2 and WPA3 protocols for secure WLAN access and user data protection.
* Managed ISE policy configurations to secure wireless and wired access across corporate networks.
* Configured RestConf APIs to enable RESTful communication with network devices.
* Deployed iEN hardware and software to optimize network performance and bandwidth utilization.
* Configured LDP on routers to enable label-switched paths (LSPs) for efficient MPLS traffic forwarding.
* Leveraged Arista's Extensible Operating System (EOS) for programmable network management and automation.
* Automated network provisioning and configurations using SDN, reducing manual processes by 40%.
* Led a team of technicians in the installation, configuration, and maintenance of network hardware, ensuring seamless connectivity across the enterprise.
* Integrated Fortinet Forti Analyzer for centralized log management and threat detection across the network.
* Monitored TCP/IP network traffic using tools like Wireshark and NetFlow for performance and security analysis.
* Used tools like Zeek and Wireshark to capture and analyze HTTP traffic for threat detection.
* Developed customized dashboards within SNA to report critical network security metrics to senior management.
* Integrated TACACS+ with existing authentication systems for unified user management and logging.
* Conducted site surveys and coverage analysis to optimize WLAN performance and connectivity.
* Integrated Cisco ISE with Active Directory to streamline user authentication and access management.
* Proficient in scripting and configuring network policies within SoundBound for operational efficiency.
* Configured and managed Nokia network equipment, including routers and switches.
* Integrated RestConf with SDN environments for flexible and scalable network management.
* Integrated Netconf with SDN controllers to enable programmatic control over network configurations.
* Troubleshot LDP sessions and label distribution issues, improving overall network stability.
* Deployed Ciena WaveLogic technology to support high-bandwidth applications in enterprise environments.
* Configured and managed Zeek for real-time network traffic analysis and intrusion detection.
* Configured and managed Check Point firewalls, including rule base creation and threat prevention tuning.
* Implemented Palo Alto Networks Prisma Access for secure remote access solutions.
* Conducted training sessions on SNA for team members to improve overall cybersecurity response and awareness.
* Configured and optimized Aruba wireless LAN solutions for large-scale deployments.
* Integrated Arista devices with cloud networking environments to support hybrid and multi-cloud infrastructures.
* Conducted regular audits of IDS/IPS rules and signatures for relevance.
* Created and maintained NOC documentation for processes, troubleshooting steps, and escalation paths.
* Configured and maintained VoIP telephony systems to streamline communications.
* Implemented wireless network solutions to enhance connectivity and coverage.
* Developed comprehensive network diagrams and flowcharts using Microsoft Visio for system architecture representation.
* Designed and implemented efficient IP addressing schemes using subnets to optimize network performance and scalability.
* Supported the deployment of Aruba ClearPass, helping to streamline user onboarding and enhance network security.
* Using AirMagnet WiFi Planning for Importing Floor Plans, Antenna Selection, Area Maps, Defining the environment, Scaling, Floor Attenuation and AP spot.
* Configured and synchronized DNS and DHCP services using Infoblox Grid Manager, ensuring seamless integration, high availability, and improved network reliability across distributed environments.
* Integrated Nokia equipment with SDN solutions for centralized network management.
* Developed scripts for Netconf sessions, reducing manual configurations by 50%.
* Conducted troubleshooting and maintenance on Ciena network elements to ensure optimal performance and uptime.
* Used forensic tools (e.g., EnCase, Autopsy) to recover and analyze evidence from computers, networks, and storage media.
* Developed custom detection signatures and scripts to identify known APT behavior in network and endpoint logs.
* Monitored SSH login attempts for brute force or unusual access patterns.
* Configured RSVP for traffic engineering in MPLS networks to ensure optimal path selection.
* Monitored FTP traffic for unauthorized access and suspicious transfers.
* Monitored DNS traffic for signs of malicious activity, such as DNS tunneling.
* Configured firewalls and web application firewalls (WAFs) to secure HTTP/HTTPS communications.
* Analyzed network activity logs generated by Zeek to identify potential security threats.
* Managed virtual networks, subnets, and NSGs to secure Azure resources and control traffic flow.
* Configured Palo Alto firewalls with Layer 7 application inspection and policy enforcement.
* Designed and implemented Wi-Fi networks in high-density environments for optimal connectivity.
* Configured VTP (VLAN Trunking Protocol) on Cisco switches to manage VLAN information consistently across the network.
* Configured and optimized STP (Spanning Tree Protocol) to prevent network loops and ensure redundancy in switched networks.
* Developed custom SDN applications to enhance network monitoring and performance tracking.
* Oversaw network hardware lifecycle management, including procurement, inventory, and replacement of outdated equipment, improving network reliability.
* Developed automation scripts using RestConf to streamline configuration tasks.
* Maintained chain-of-custody procedures to ensure evidence integrity during forensic investigations.
* Analyzed HTTP, DNS, and FTP traffic in PCAP files to identify attack vectors and vulnerabilities.
* Conducted post-incident analyses of APT incidents to strengthen defenses against similar attacks.
* Integrated various log sources into SIEM, including firewalls, IDS/IPS, and servers.
* Used IDS/IPS data to identify and respond to emerging threats in the network.
* Set up multi-factor authentication (MFA) to secure SSH access to critical systems.
* Configured and managed HPE switches for enterprise-level networking environments.
* Implemented WPA2 and WPA3 encryption protocols to secure wireless networks.
* Designed and deployed SD-WAN solutions to optimize network traffic flow and reduce costs.
* Installed and configured fiber optic cabling for high-speed data transmission.
* Performed regular software upgrades and patches on Check Point appliances to ensure optimal security performance.
* Managed intranet site content to facilitate internal communication and resource sharing.
* Deployed and configured RADIUS servers for centralized authentication, authorization, and accounting (AAA) of network devices.
* Configured Ciena MCP (Manage, Control, Plan) for centralized management and control of optical networks.
* Configured secure FTP servers with TLS to protect file transfer communications.
* Analyzed HTTP request and response headers for vulnerabilities and security gaps.
* Wrote custom Zeek scripts to enhance detection capabilities and tailor monitoring to network needs.
* Implemented and maintained Palo Alto Next-Generation Firewall features, including URL filtering and WildFire threat analysis.
* Implemented DNS security extensions (DNSSEC) to protect against spoofing attacks.
* Automated infrastructure deployment using Azure Resource Manager (ARM) templates and Bicep.
* Configured secure VPN connections using Prisma Access for distributed workforces.
* Proficient in troubleshooting and maintaining Aruba wireless infrastructures.
* Integrated multi-vendor equipment to create a cohesive network infrastructure.
* Developed custom filtering scripts for PCAP files to expedite incident response and analysis.
* Configured and optimized BGP routing across enterprise networks to ensure efficient path selection and failover.
* In order to collect, filter, and aggregate data for business analysis, sophisticated SQL queries were developed.

**MCKesson, New York Jul 2019 - Sep 2021**

**Network Security Engineer**

**Responsibilities:**

* Tuned BGP internal and external peers with manipulation of attributes such as metric, origin and local preference.
* Worked on FTP, HTTP, DNS, DHCP servers in windows server-client environment with resource allocation to desired Virtual LANs in the network.
* Applied UTM (Unified Threat Management) features on Fortinet devices, including IPS, antivirus, and web filtering.
* Configured and managed VPNs leveraging IPsec and SSL within TCP/IP networks for secure remote access.
* Deployed TACACS+ to enhance security and auditing capabilities for network administration.
* Conducted root cause analysis in NOC for recurring incidents to improve long-term stability.
* Deployed access point (AP) configurations and monitored WLAN traffic for optimal network performance.
* Set up guest access and BYOD policies within Cisco ISE for secure, managed user access.
* Conducted firmware and software upgrades on Nokia devices, ensuring compatibility and security.
* Troubleshot RestConf communication issues, ensuring consistent device connectivity.
* Configured iEN with SDN platforms for centralized control of edge devices and services.
* Integrated RSVP with other protocols like OSPF-TE to support dynamic and reliable network routing.
* Integrated Ciena solutions with existing SDN platforms to enable dynamic bandwidth allocation.
* Deployed and configured IDS/IPS systems for real-time threat detection.
* Implemented HTTP security headers (HSTS, Content-Security-Policy) to enhance web security.
* Integrated Zeek with SIEM platforms for centralized alerting and reporting.
* Configured and maintained Azure Firewall and DDoS Protection for enhanced cloud security.
* Deployed Arista CloudVision for centralized network visibility, improving monitoring and management.
* Coordinated with cross-functional teams to plan and execute network hardware installations, ensuring minimal disruption to daily operations.
* Utilized SolarWinds NetFlow Traffic Analyzer to analyze network traffic patterns and ensure bandwidth efficiency.
* Implemented Fortinet SD-WAN to optimize WAN connectivity and reduce MPLS dependencies.
* Diagnosed and resolved connectivity issues at each layer of the OSI model to ensure reliable TCP/IP communication.
* Conducted periodic access reviews using TACACS+ logs to verify adherence to access control policies.
* Prepared and distributed network performance reports to stakeholders from NOC analytics.
* Developed WLAN policies to support secure guest access and prevent unauthorized network access.
* Conducted capacity planning and trend analysis with SolarWinds to optimize network resources.
* Customized endpoint profiling in Cisco ISE to classify devices and enforce policy-based access control.
* Configured automated reports in SolarWinds to track uptime, device availability, and network performance KPIs.
* Skilled in integrating Sound Bound with network management systems for streamlined network automation.
* Troubleshot Nokia device connectivity issues, minimizing network downtime.
* Configured XML-based APIs in Netconf to automate device management tasks.
* Managed Forti Manager for streamlined firewall policy deployment across multiple Fortinet appliances.
* Applied QoS policies on TCP/IP traffic to prioritize critical applications and reduce latency.
* Monitored iEN performance metrics to ensure reliability and detect potential issues early.
* Integrated LDP with MPLS VPNs to support scalable, multi-tenant networks in enterprise environments.
* Worked on Ciena's Adaptive IP solutions, improving resilience and adaptability in multi-domain networks.
* Integrated SDN with network function virtualization (NFV) to optimize resource utilization and support virtual services.
* Used PCAP files to reconstruct incidents for forensic analysis and evidence gathering.
* Leveraged ISE to improve network security through context-aware access and user identity management.
* Monitored IDS/IPS alerts and logs to investigate potential security incidents.
* Applied SolarWinds Network Configuration Manager (NCM) for centralized management of device configurations.
* Developed incident response workflows within the NOC to streamline troubleshooting and resolution.
* Used Zeek to monitor SSH traffic and generate alerts for suspicious activity.
* Worked with IT security teams to configure TACACS+ for role-based access to network resources.
* Logged and reviewed FTP activities as part of regular security auditing.
* Conducted network traffic analysis to identify and mitigate potential risks using Stealthwatch’s behavioral analysis capabilities.
* Conducted regular firmware updates and patch management for Fortinet appliances to maintain security.
* Conducted performance tuning on TCP/IP stacks for high availability and load balancing in enterprise networks.
* Monitored WLAN traffic and analyzed logs to troubleshoot and resolve connectivity issues.
* Conducted regular updates and audits of ISE configurations to maintain security compliance.
* Analyzed DNS logs for anomalous queries indicative of malware or phishing.
* Conducted threat intelligence research on APT groups, TTPs (tactics, techniques, and procedures), and indicators of compromise (IOCs).
* Collaborated with stakeholders to validate and sign off on network automation tools during UAT.
* Configured QoS on Nokia routers to prioritize traffic and maintain service levels.
* Configured network policies through RestConf for simplified and remote administration.
* Developed automation scripts for iEN configuration, reducing setup time and human error.
* Analyzed RSVP reservation requests to ensure bandwidth availability for prioritized traffic.
* Conducted configuration and testing of LDP for traffic engineering and enhanced bandwidth management.
* Automated network tasks using Arista’s eAPI, reducing manual configurations and operational errors.
* Worked with protocols such as OpenFlow to facilitate SDN deployment in multi-vendor environments.
* Generated forensic reports detailing findings, evidence, and recommended corrective actions.
* Integrated PCAP analysis with SIEM systems to improve alert context and enrich threat detection.
* Optimized VPN configurations using Check Point to enhance secure remote access capabilities.
* Troubleshot Wi-Fi issues using tools like Wireshark and NetSpot for packet analysis.
* Coordinated with cross-functional teams to integrate Aruba wireless networks into existing systems.
* Analyzed call traffic to optimize telephony system performance.
* Established and enforced best practices for network security and hardware installation, improving the overall security posture.
* Documented RestConf usage guidelines and training materials for the IT team.
* Troubleshot Netconf sessions to ensure successful device communication and configuration.
* Monitored RSVP sessions to maintain QoS and prevent congestion in high-demand network segments.
* Configured VXLAN on Arista devices to support overlay networking for scalable data center deployments.
* Monitored network health and performance using Ciena analytics tools, proactively addressing potential issues.
* Conducted testing and validation of SDN policies to ensure security and compliance with enterprise standards.
* Designed and implemented multicast networks for efficient delivery of video, voice, and other real-time applications.
* Monitored OSPF neighbors and ensured stable adjacency formation, preventing issues like stuck in INIT/EXSTART states.
* Configured and managed security controls at each level of the Purdue Model, from Level 0 (field devices) to Level 5 (enterprise network), enhancing overall ICS security.
* Leveraged Netconf for real-time device monitoring and data retrieval.
* Monitored LDP signaling and session states to ensure robust and resilient network connectivity.
* Generated PCAP reports to provide insights into network security incidents and patterns.
* Implemented countermeasures to prevent APTs from escalating privileges or moving laterally within the network.
* Created custom SIEM correlation rules to detect advanced threats.
* Assisted in capacity planning and upgrades on Ciena network infrastructure to support organizational growth.
* Tuned IDS/IPS rules to reduce false positives and enhance detection accuracy.
* Used Zeek to monitor and analyze FTP connections, identifying potential threats.
* Integrated Azure Monitor and Log Analytics for proactive infrastructure monitoring and alerting.
* Supported RF testing and troubleshooting, ensuring compliance with industry standards.
* Integrated HPE switches into multi-vendor network setups for seamless interoperability.
* Implemented VLSM (Variable Length Subnet Mask) to efficiently utilize IP address space in large network deployments.
* Integrated Prisma Access with existing cybersecurity frameworks to ensure data protection.Provided end-user support and training for Aruba wireless network usage and troubleshooting.
* Provided hands-on training and mentorship to junior technicians, enhancing their skills in network hardware setup and troubleshooting.
* Configured fail2ban or similar tools to automatically block failed SSH login attempts.
* Used Zeek to generate detailed logs for HTTP, DNS, SSH, and other protocols.
* Blocked access to known malicious domains via DNS filtering.
* Conducted memory forensics to identify in-memory malware and advanced persistent threats.
* Limited SSH access to specific IP addresses for enhanced security.
* Monitored SIEM alerts for suspicious activities, escalating incidents as needed.
* Performed in-depth analysis and remediation of incidents using Palo Alto threat logs and traffic analysis tools.
* Conducted detailed troubleshooting and resolution of issues related to Check Point firewalls and network traffic.
* Upgraded existing cabling systems to support increased bandwidth requirements.
* Troubleshot telephony issues to minimize downtime and service interruptions.
* Troubleshot SD-WAN issues to ensure high availability and minimal latency.
* Designed fiber optic networks to meet organizational data transmission needs.
* Developed best practices for managing a multi-vendor environment.
* Deployed network monitoring to detect and prevent brute force attacks on FTP accounts.
* Managed Aruba ClearPass for network access control (NAC), enforcing 802.1x and guest authentication policies.
* Designed wireless networks using predictive modeling tools for optimal layout.
* Integrated third-party tools into the intranet for increased functionality.
* Deployed Azure Key Vault to manage and secure keys, secrets, and certificates.
* Configured DNS records (A, MX, TXT) for network and email security.
* Collaborated with incident response teams to investigate and mitigate APT-related incidents.
* Integrated Check Point with SIEM solutions to enhance centralized threat monitoring.
* Troubleshot Layer 2 and Layer 3 connectivity issues on HPE switch networks.
* Conducted root cause analysis on incidents detected by SIEM.
* Implemented security measures in SD-WAN to protect data and manage traffic.
* Implemented feedback from UAT to enhance network automation scripts and tools for optimal performance.
* Wrote custom scripts to monitor HTTP logs for indicators of compromise.
* Standardized Visio templates for recurring diagramming tasks, increasing team efficiency.
* Optimized Wi-Fi performance by tuning signal strength, channel selection, and interference mitigation.
* Configured root bridge and backup root bridge in STP to control network traffic and ensure optimal path selection.

**Delta Airlines, Atlanta, GA Feb 2017– Jun 2019**

**Network Engineer**

**Responsibilities:**

* Daily analysed network traffic looking for trends and or malicious activities, created vulnerability report with action plans.
* Configured HSRP, VLAN Trunking 802.1Q encapsulation, VLAN Routing on Catalyst 6500 switches
* Maintain, install and upgrade/downgrade Cisco hardware including routers, switches, firewalls, and data center switches like Catalyst 3560/3750/6500’s, ASA 5505-5550 firewalls, and Cisco UCS 6100/B-series blade servers.
* Implemented IPsec Site-to-Site VPNs over the internet utilizing 3DES, AES/AES-256 with Cisco PIX and Cisco ASA Firewalls.
* Troubleshot network connectivity issues related to Prisma Access deployments.
* Trained teams on using Cisco Stealth watch for proactive threat detection and security incident investigation.
* Collaborated with cross-functional teams to transition legacy networks to SDN-enabled infrastructure.
* Designed subnetting structures for multi-branch offices to ensure clear separation of network traffic and resources.
* Performed regular updates and upgrades to Nutanix software and firmware, maintaining system stability and security.
* Migrating Cisco ASA firewall AnyConnect with secured VPN Users Group, including deployment of Two-Factor Authentication (LDAP+Soft Token) for VPN Clients.
* Utilized Stealth watch for detecting lateral movement and insider threats within complex network environments.
* Utilized SDN for enhanced traffic engineering, optimizing data paths based on network demand.
* Managed vendor relationships for network hardware, including negotiating contracts and coordinating on-site support to ensure efficient issue resolution.
* Optimized Zeek’s performance to handle high-throughput network environments.
* Analyzed security incidents and threat intelligence, utilizing Firepower's threat analytics and response capabilities to mitigate risks.
* Developed custom alerts and reports in Cisco Stealth watch to streamline security monitoring and auditing processes.
* Design antenna system for 802.11g specifications.
* Deployed and managed AWS Lambda functions to implement serverless architecture for event-driven processing.
* Developed and enforced data flow and communication protocols between different Purdue levels, ensuring secure and efficient data exchange while minimizing risk.
* Conducted incident response drills and tabletop exercises, preparing teams for potential cyber incidents affecting ICS/SCADA systems.
* Conducted root cause analysis and troubleshooting of network hardware issues, reducing resolution time and enhancing system stability.
* Conducted threat hunting and forensic investigations using Zeek logs.
* Collaborated with cross-functional teams to ensure seamless integration of ClearPass with existing network infrastructure, including firewalls, switches, and wireless controllers.

**Qualcom , India Aug 2013 – Jan 2017**

**Network Support Engineer**

**Responsibilities:**

* Worked with Cisco Catalyst 3500, 4500 switches and Cisco 2800, 3600, 3800 series and 2500, 3550 series Routers.
* Performed tasks that include Configuring and constant administration of Static routing, Default Routing & dynamic Routing Protocols.
* Configured new WAN links and monitored network performance
* Worked to set up the TFTP server for backing up the IOS images and configuration files of Cisco Routers and Switches and troubleshooting the file servers.
* Performed network evaluations, troubleshooting a variety of network problems, and implementing various software and hardware upgrades.
* Troubleshoot Cisco hardware: Inspected devices, Read device LEDs, loose connections, cards, OS upgrade, switch configuration usage of Visual Switch Manager, Switch port configuration, Port monitoring.
* Performed configuration of LAN\WAN technologies such as Ethernet, Fast Ethernet, & Gigabit Ethernet.
* Trained operational and security teams on the Purdue Model's principles and best practices, enhancing their understanding of secure ICS network architecture.