HARI SHARMA

Security Engineer | Cloud Security | AWS & Azure | IAM | Network Security
Harisharma.net
sharma.hari1@proton.me / (248) 761-0319
linkedin.com/in/sharmahari25/
github.com/hsharma-cloud

SUMMARY

Security Engineer with hands-on experience securing hybrid and cloud environments across Azure and AWS. Skilled in network security, identity and access management, and security operations, with practical experience across both Cisco and Palo Alto security platforms, including firewall policy management, segmentation, and secure access controls. Proven ability to implement least-privilege access, monitor and respond to threats using SIEM and endpoint tools, and support vulnerability management initiatives. Experienced in leveraging automation and API-driven workflows to improve operational efficiency and consistency across environments. Adept at aligning security controls with enterprise standards and compliance frameworks including HIPAA and PCI DSS.

Skills:

- Security Engineering: IAM, RBAC, and least-privilege access across hybrid environments; firewall policy enforcement, segmentation, and vulnerability management.
- Cloud Security: Azure and AWS security controls including IAM, network security, and logging/monitoring for secure cloud and hybrid workloads.
- Security Operations and Automation: SIEM monitoring, incident response, and vulnerability scanning using Palo Alto and Cisco platforms; automation with APIs and scripting.

Experience:

Security Engineer / First National Bank of America – Lansing, Michigan - *Contract* *11/2025 – 04/2026*

- Detection and Monitoring: Implemented centralized logging, monitoring, and threat detection to improve visibility across cloud environments and enable timely incident response.
- Applied cloud security best practices including IAM, RBAC, and least-privilege access while contributing to security monitoring and incident response through analysis of centralized logs and telemetry.
- Assisted with vulnerability management and secure configuration reviews, validating security controls and supporting remediation efforts to improve overall security posture in shared-responsibility cloud environments.

Network Security Engineer / Trinity Health, St. Joseph's Health Hospital - Syracuse, NY *-Full Time* *04/2023 – 10/25*

- Implemented and supported enterprise security controls aligned with HIPAA and PCI DSS by configuring and validating policies across Cisco security platforms (ISE, Firepower Management Center), helping reduce data exposure risk and strengthen compliance posture.
- Performed vulnerability assessments and secure configuration reviews using tools such as Nessus, Wazuh EDR, SIEM, and DLP, supporting remediation efforts that reduced risk exposure and improved patch compliance.
- Designed and secured cloud and hybrid environments using identity and access controls, least-privilege principles, network segmentation, and secure connectivity patterns to protect enterprise workloads.
- Contributed to security monitoring and incident response by analyzing logs and alerts from SIEM and endpoint platforms, assisting with threat investigation, containment, and root-cause analysis.
- Supported security operations and risk assessments by documenting findings, validating controls, and assisting remediation tracking to improve overall security visibility and operational readiness.

Network Security Engineer / KDDI America - Livonia, MI - Contract *06/2022 - 03/2023*

- Configured and supported identity and access controls using Cisco ISE with 802.1X/MAB authentication and secure VPN access to reduce unauthorized access and improve secure connectivity.
- Supported security monitoring and incident response by analyzing logs and alerts in SIEM platforms, assisting with threat investigation, root-cause analysis, and remediation efforts.
- Installed, configured, and troubleshot network and security infrastructure (routers, switches, firewalls, load balancers), applying security best practices and supporting hybrid and cloud-connected environments.

Network Security Engineer / SAF-Holland - Muskegon, MI -Contract *08/2021 - 05/2022*

- Configured and supported network security controls including Cisco ASA firewalls and Site-to-Site, Remote-Access, and SSL VPNs to provide secure connectivity for a large remote user base and reduce unauthorized access risk.
- Applied secure routing and infrastructure hardening practices by implementing EIGRP authentication and route optimization techniques, helping protect network integrity and improve performance across enterprise environments.
- Integrated security operations controls such as multi-factor authentication, endpoint protection, email security, and data loss prevention to strengthen overall security posture across network and user environments.
- Streamlined security workflows using APIs and scripting for firewall validation, access reviews, and logging.

Network Security Engineer / Adient Global - Plymouth, MI -Contract *08/2019 - 08/2021*

- Delivered a security awareness effort by reinforcing security policies and user guidance, helping improve employee compliance and reduced policy violations across teams.
- Provided hands-on technical support for security operations, including SIEM platforms, wireless infrastructure, and DHCP configurations, contributing to improved operational efficiency and faster incident resolution.
- Configured and supported enterprise device and wireless security solutions, maintaining secure connectivity, high availability, and consistent service performance across multiple locations.
- Assisted with cloud security operations in Azure and AWS by supporting identity and access controls, reviewing resource configurations, and applying least privilege and RBAC best practices.
- Contributed to cloud and hybrid security monitoring by analyzing logs and security telemetry from Azure and AWS environments, supporting threat detection, investigation, and incident response activities

Network Security Engineer /WellCare/Meridian - Detroit, MI *Contract* *05/2019 - 07/2019*

- Contributed to a security awareness initiative by supporting user guidance and policy reinforcement efforts, helping improve adherence to security protocols and reduce policy violations.
- Provided hands-on technical support for security operations, including SIEM platforms, wireless infrastructure, and DHCP configurations, helping improve incident handling efficiency and reduce resolution times.
- Configured and supported enterprise wireless security solutions to maintain secure connectivity and high availability across multiple locations.

Network Security Engineer /LAN/WAN Professional - Irvine, CA -Contract *10/2018 - 04/2019*

- Supported secure enterprise network environments across multi-site infrastructures by configuring, maintaining, and troubleshooting LAN/WAN systems to ensure availability, performance, and controlled access for thousands of users.
- Managed and secured network and virtualization platforms, including routers, switches, firewalls, and virtual infrastructure, applying monitoring, access control, and troubleshooting practices to improve system stability and reduce incident resolution time.
- Assisted with infrastructure lifecycle activities such as hardware refreshes, license tracking, and vendor coordination, supporting cost efficiency, compliance requirements, and uninterrupted service delivery.

Network Analyst (SDA) / Care Tech Solutions - Troy, MI -Full Time *03/2016 - 09/2018*

- Handled high-volume service tickets to maintain secure system operations, ensuring availability, performance, and risk reduction.
- Enhanced network stability and secure access by troubleshooting routing, firewalls, and VPNs across hybrid environments.

EDUCATION AND TRAINING

Master of Science: Cybersecurity
Eastern Michigan University

Bachelor of Science: Information Assurance (Network Security)
Eastern Michigan University

Associates: CIS (Homeland Security/Computer Support)

Oakland Community College

CERTIFICATIONS

- CASP+ (CompTIA Advanced Security Practitioner)
- Systems Security Certified Practitioner (ISC2), Certified in Cybersecurity
- CEH (Certified Ethical Hacker)
- CompTIA PenTest+, Linux+
- CCNP Enterprise (Routing & Switching), CCNP Security Core
- AWS Certified Solutions Architect Associate
- ITIL Foundation