Shivam Patel

Sayreville, NJ • 603-785-2259 • shivamp9816@gmail.com

PROFESSIONAL SUMMARY

Junior IT Administrator with 2 years of experience supporting Microsoft 365, Entra ID, Windows systems, and network troubleshooting. I am developing strong security foundations through Security+ studies and hands-on SOC lab work focused on alert triage, log analysis, and threat identification. Through this experience I have become skilled in onboarding, device configuration, VPN support, and monitoring system activity for anomalies. Also known for fast, accurate problem solving, clear documentation, and growing expertise in security operations.

SKILLS

Security skills

Basic security log analysis (Windows Event Logs), understanding of authentication events, and early exposure to incident-response concepts through real-world ransomware containment.

Familiar with Microsoft Defender alerts, Microsoft 365/Entra ID security features (MFA, conditional access basics), and identity-related investigations.

Actively studying Security+ with growing knowledge of threats, vulnerabilities, access control, and foundational security principles.

Beginning hands-on SOC lab work focused on collecting endpoint logs (Sysmon), understanding SIEM concepts, and building core investigation habits**.**

Core IT skills

Microsoft 365: Outlook, Exchange, Teams, SharePoint, OneDrive, migrations
Identity & Access: Entra ID (Azure AD), provisioning, resets, license assignments
Systems: Windows, Linux (basic)
Networking: DNS, DHCP, VPN, IP addressing, LAN/WAN, Wi-Fi, firewalls
Tools: Remote desktop, Cisco Packet Tracer, antivirus tools, backup utilities
Hardware: Laptops, desktops, printers, peripherals, component replacement

Soft Skills: Customer service, communication, problem-solving, time management, adaptability, teamwork, documentation, attention to detail, user training

WORK EXPERIENCE

Junior IT Administrator

BestBet Computer 2024–Present

- Assisted in containment and triage during a ransomware incident by isolating compromised systems, analyzing event logs (4624/Type 3), and identifying lateral-movement patterns used against the client's Windows domain.
- Monitored **system, application, and security logs** across Microsoft 365 and endpoint environments to identify anomalies, investigate issues early, and escalate potential security events.
- Investigated **suspicious sign-ins, MFA failures, email anomalies, and access-related incidents**, determining root cause and documenting findings for escalation.
- Responded to user-reported incidents through the ticketing system, performing initial triage, gathering evidence, and following incident handling procedures.

- Assisted with endpoint security by reviewing **Microsoft Defender alerts**, performing basic remediation, and ensuring devices remained compliant and up to date.
- Supported **Microsoft 365 and Entra ID** operations including group assignments, access troubleshooting, conditional access checks, and mailbox configuration.
- Followed runbooks to perform secure provisioning, deprovisioning, and configuration changes while maintaining identity hygiene and reducing access-related incidents.
- Troubleshot and resolved issues involving **DNS/DHCP conflicts, VPN failures, IP conflicts, and firewall access requests**, restoring secure connectivity under time-sensitive conditions.
- Executed documented procedures during **three Microsoft 365 migrations (~100 users each)**, ensuring smooth deployment, validating security configurations, and resolving post-migration issues quickly.

Projects

Home SOC Lab — Elastic SIEM, Wazuh XDR, Suricata IDS, Sysmon, Microsoft Sentinel (Ongoing)

- Building a full SOC lab to gain hands-on experience with SIEM, XDR, IDS, and endpoint telemetry.
- Currently deploying core components (Elastic SIEM + Wazuh) and configuring Windows endpoints with Sysmon for telemetry collection.
- Beginning to analyze authentication logs, process creation events, and basic alert triage workflows.
- Practicing foundational SOC skills: identifying suspicious activity, correlating events, and mapping behaviors to MITRE ATT&CK techniques.
- Expanding the lab step-by-step to include Suricata IDS, detection rules, and simulated attack scenarios as part of ongoing learning.
- Documenting each phase of the build, including configurations, detections, and investigation notes to strengthen incident-response skills.

EDUCATION

MS – IT Administration & Security
New Jersey Institute of Technology | 2024–2026

BS – IT Administration & Security
New Jersey Institute of Technology | 2019–2022

CERTIFICATIONS

CompTIA Security+ (In Progress)