Sorie Deen Sesay

ssdeen572@gmail.com • (571)-322-1402
LinkedIn URL • Stafford, VA

Cybersecurity Analyst Profile

Analytical and motivated professional with foundational knowledge in strengthening security measures, identifying cyber risks, and supporting the implementation of modern security solutions in enterprise settings.

Instrumental in security monitoring operations, threat intelligence, and vulnerability management, backed by hands-on experience in SOC environments, endpoint security, and project oversight. Adept at fortifying enterprise security by deploying, configuring, and fine-tuning SIEM solutions, intrusion detection systems, and advanced threat mitigation strategies. Proven ability to investigate, analyze, and remediate cyber threats through real-time monitoring, forensic analysis, and incident response frameworks. Skilled in designing cybersecurity policies, access controls, and security automation to enhance risk management. Creative problem-solver with competencies in managing security projects, aligning cybersecurity initiatives with business objectives, and improving network defense mechanisms.

Areas of Expertise

Cybersecurity Governance | Security Operations Management | Incident Response & Threat Hunting | Vulnerability Assessment

Cloud Azure Security Monitoring | Identity Access Management | Project Management | Critical Thinking & Problem-Solving

Technical Proficiencies

Security & Cloud:	Azure (Sentinel, Active Directory/Microsoft Entra ID, Defender for Cloud), Network Security Groups, Firewalls.
Virtualization:	Virtual Machines (VirtualBox, VMware, Hyper-V).
Cybersecurity Tools:	OpenVAS, Microsoft Sentinel, Log Analytics, KQL.
Administration:	Active Directory, Group Policy, Windows Server 2019, PowerShell.
Technical Support:	Helpdesk, IT Service Management (ISIM), ServiceNow, BMC Footprints.
Programming & Scripting:	Python, PowerShell
Operating System:	Windows 10, Linux

Education

Bachelor of Science in Cybersecurity Technology (In Progress), University of Maryland Global Campus

Licenses & Certifications

CompTIA CySA+ | CompTIA Security+ | CompTIA Network+ | Cisco Junior Cybersecurity Analyst | Cybersecurity Analyst (LeveldCareers)

Career Experience

Atrium Health, Charlotte, NC **2022 – 2024**

OSR Account Administrator

Optimized account management workflows by leveraging Microsoft Office Suite and advanced database applications to manage, track, and update customer information. Strengthened data security and compliance by implementing best practices for data handling and account management. Facilitated cross-functional collaboration by coordinating with teams to address account management challenges.

- Improved account accuracy and security up to 20% by leading customer account investigations and resolving discrepancies.

- Reduced data entry error rates up to 15% by streamlining processes through ServiceNow; ensured compliance with integrity standards.
- Decreased resolution time up to 30% by steering troubleshooting efforts for customer account issues / enhancing customer satisfaction.

CGI Federal, Fairfax, VA **2019**

Helpdesk Support Technician

Managed and resolved support tickets through ITSM tools, while escalating complex issues to higher-tier support teams. Installed, configured, and maintained operating systems, applications, and security updates across workstations and enterprise systems.

- Decreased average response time up to 40% by prioritizing and tracking service requests through BMC Footprints.
- Reduced technical support requests up to 35% by managing the migration of 100+ laptops per week to Windows 10.
- Streamlined asset tracking and reduced discrepancies by 20% by leading the development of an asset management module.
- Increased administrator efficiency by 25% by designing / managing internal Business Unit Directory integrated with Active Directory.
- Improved system uptime up to 30% by leveraging BCM for endpoint management and implementing software patching / installation.
- Achieved 100% customer satisfaction by delivering expert-level support for Windows 10 users, resolving technical issues both remotely and in-person, and improving system security across the organization.

Notable Projects

SOC Home Lab Project

- Enhanced cybersecurity skills by establishing a SOC Home Lab, deploying Pfsense firewall, Windows Server 2022 with Active Directory, and integrated threat detection tools.
- Investigated 40+ exploitation attempts, including Log4Shell (CVE-2021-44228), by leveraging Sysmon and CrowdSec for behavioral analysis and real-time threat detection.
- Strengthened network security by executing Windows Firewall Bouncer; automated malicious IP blocking / improved threat mitigation.

Cloud SOC Lab with Wazuh

- Improved threat visibility by deploying Wazuh for real-time security monitoring and integrating agents on Linux systems.
- Resolved WSL installation issues by troubleshooting agent deployment / ensuring seamless log collection across cloud environments.
- Enhanced compliance monitoring by configuring security alerts for virtualized infrastructure, reducing risk exposure.

Implementing a SOC and Honeynet in Azure

- Increased security event detection by configuring Azure Virtual Machines and Microsoft Sentinel to analyze threats in real time.
- Strengthened attack detection capabilities by fine-tuning SIEM rules for log analysis and suspicious activity correlation.
- Improved adversary analysis by simulating honeynet attacks, studying threat actor behaviors, and enhancing detection techniques.

Cybersecurity Vulnerability Management Project

- Improved cybersecurity readiness by simulating real-world threat mitigation scenarios and analyzing scan results.
- Identified and remediated critical security weaknesses by performing scans on a vulnerable Windows 10 VM using OpenVAS.
- Reduced potential attack vectors by developing vulnerability remediation framework; verified effectiveness through iterative scanning.

Sorie Deen Sesay

Active Directory Home Lab Project

- Improved threat detection by configuring Splunk SIEM to aggregate logs, generate security alerts, and analyze attack patterns.
- Enhanced security analytics by conducting adversarial simulations using Atomic Red Team and brute-force testing with Kali Linux.
- Strengthened enterprise network security by designing and deploying an Active Directory environment with Windows Server 2022, Windows 10, Kali Linux, and Ubuntu Server.