# Rujul Chaudhari

Bloomingdale, IL
Phone: (630) 624-7859
Email: rujul489@gmail.com
Socials: Github | Linkedin | Youtube


## Profile:

**Cybersecurity Analyst | IT Security & Compliance | PCI DSS & SOC Standards**

- Results-driven Cybersecurity Analyst with 4+ years of experience protecting enterprise environments through proactive threat detection, incident response, and vulnerability remediation. Proven expertise aligning with PCI DSS, SOC 2, and NIST standards to enhance security posture across cloud and on-prem infrastructure.
- Adept in leveraging advanced tools including SIEM platforms (Splunk, Sentinel), cloud-native security controls (Azure, AWS), and AI-driven automation tools like ChatGPT, Gemini, and Claude to streamline documentation, threat intelligence analysis, and report generation.
- Committed to continuous learning, hands-on experimentation, and building resilient, audit-ready systems.

## Core Skills & Competencies:

- Cybersecurity Analyst
- PCI DSS & SOC 2/3 Compliance
- IT Audit & Security Assessments
- Vulnerability Management
- Incident Response & Breach Investigation
- Cloud Security (AWS, Azure)
- Linux Administration
- Information Security Policies
- Risk Mitigation
- Network Security
- AI Tools (ChatGPT, Gemini, Claude)
- Security Documentation
- Threat Intelligence
- SIEM (Splunk, Azure Sentinel)
- Intrusion Detection
- Encryption
- Firewall Management
- Endpoint Security
- Data Privacy & Security Standards
- PowerShell Scripting

## Technical Skills:

- **Languages/Scripting:** Java, C#, Python, SQL (Oracle)
- **Security Tools/Frameworks:** PCI DSS Compliance, SOC 2, CIS, NIST framework, Security Systems, Sophos, BitDefender, Microsoft Defender
- **Networking/Access:** TCP/IP, DNS, Firewall Configs, VPN, SSO, MFA
- **Cloud Computing/IAM platforms:** MS Admin Center, AWS, Active Directory, Azure, Azure Active Directory (Entra), Azure DevOps, SaaS, IaaS, Haas, Cloud Infrastructure
- **Data Analytics:** SPSS, Tableau, PowerBI
- **Operating Systems:** Windows, Mac, Linux
- **Virtualization:** VMware, Hyper-V, VirtualBox

## Key Cybersecurity Projects:

- **Active Directory Home Lab:** Built and documented a virtual lab featuring a Domain Controller and Windows user machine; used to simulate AD group policies, user access control, and domain join scenarios.
- **Azure Sentinel Attack Map:** Deployed Azure Sentinel in a virtual lab to simulate real-time threat detection. Integrated third-party APIs, analyzed live attack data using KQL queries, and created interactive dashboards.
- **Nessus Vulnerability Management Lab:** Conducted internal vulnerability scans using Nessus on Windows Server instances. Documented vulnerabilities by CVSS score and tested remediation strategies in a controlled environment.
- **Wazuh SIEM Lab:** Installed and configured Wazuh on a Linux server with agent-based monitoring. Built rule-based alerts and practiced event correlation using built-in log analysis tools.
- **Network Mapper with GeoLite:** Developed and documented network mapping workflows using Nmap, GeoLite, and Wireshark to visualize topology and traffic patterns in segmented environments.

- **Automated System Recon Script:** Wrote a PowerShell script (with help from ChatGPT) to extract local system info and saved Wi-Fi credentials. Demonstrated secure transmission via Discord webhook for red-team testing use. Published full script and ethical use disclaimer on GitHub.

## Career History & Achievements:

---

**Celero Commerce, Rosemont, IL** **Aug 2022 - Present**
**Security Analyst**

- Manage, monitored, and analyzed security events and logs from various sources.
- Led incident response, ensuring that security protocols adhered to PCI DSS and SOC 2 standards.

**Key Highlights:**

- Successfully conducted PCI DSS and SOC 2 security audits, implementing actionable recommendations to achieve and maintain compliance.
- Developed and implemented cybersecurity measures that reduced security incidents by 40%, including encryption and advanced access controls.
- Led incident response efforts, quickly identifying vulnerabilities and leading remediation efforts that minimized downtime and data loss.
- Manage, monitor, and analyzed security events and logs from various sources.
- Mitigated potential security gaps by executing stringent user access management protocols that exposed critical security flaws, leading to fortification of the platforms against cyber-attacks.

**FortifyIT, Oakbrook, IL** **Dec 2021 - Aug 2022**
**Cybersecurity Engineer**

- Led incident response, ensuring that security protocols adhered to the NIST standards.
- Maintained SIEM integrations, leveraging distributed data processing for large-scale analytics.

**Key Highlights:**

- Lowered security incidents by 50% by introducing two-factor authentication, encryption, and access controls that strengthened systems against cyber threats and attacks.
- Minimized system vulnerabilities by conducting regular vulnerability scans on windows server environments to optimize system functionality and security.
- Fortified remote access capabilities across the entire organization by configuring VPN solutions to prevent unauthorized access and ensure compliance with cybersecurity standards.
- Reduced system downtime by streamlining threat intelligence and response protocols for maintenance of systems.

**Unisys, Chicago, IL** **Apr 2021 - Dec 2021**
**Security Support Specialist (Remote)**

- Supported configuration of security systems and tools, resolved cybersecurity issues and collaborated with technical teams to address security challenges affecting clients and company.
- Provided IT support and assisted in system administration operations.

**Key Highlights:**

- Diagnosed complex technical problems related to system/users using ServiceNow and remote access control tools.
- Cultivated a culture of compliance with security best practices by collaborating seamlessly with Tier II technicians.
- Performed troubleshooting, diagnosis, and resolution of hardware, software, and network-related technical issues.
- Implemented thorough documentation procedures for all security and technical issues, resulting in the development of an organized and efficient support system.

**Insight, Hanover Park, IL** **Aug 2020 - Apr 2021**
**Hardware Technician**

- Led efficient hardware configuration and deployments, conducted Quality Control, and ensured compliance with security best practices.
- Utilized SAP and Excel for order processing and timely fulfillment of hardware requests.

**Key Highlights:**

- Configured and deployed hardware and software in compliance with security best practices to strengthen systems.
- Improved product quality by conducting quality control inspections and providing diagnostic reports to the management.
- Utilized SAP and Excel for managing order processing, improving efficiency in hardware fulfillment.

## Early Career History:

**Itasca Country Club, Itasca, IL; Sep 2016 - May 2017**
**Web Design Intern**

**Carol Stream Library, Carol Stream, IL; Mar 2014 - Jun 2014**
**Library Volunteer**

## Education:

- DePaul University, College of Computing and Digital Media; Jun 2019
  **B.S in Computer Science**

## Certifications:

- Splunk Certification – Ongoing
- CompTIA Security+ - Sept 2025
- SOC Fundamentals – April 2025
- Essentials in Cybersecurity – LinkedIn – Sep 2024
- Essentials in System Administration – Linkedin – Sep 2024
- Palo Alto Networks Cybersecurity Certificate – Coursera – Mar 2024
- SOC1 Certificate – TryHackMe – Jun 2024
- DevSec Ops Certificate – TryHackMe – Jun 2024
- Google Cybersecurity Professional Certificate – Coursera – Oct 2023
- Quantum Security Certificate – Cyber Now – Jan 2025