Rohith Donthula

CYBER SECURITY ANALYST

Location: NJ, USA || **Mail:** Donthula.rohith04@gmail.com || **Ph.:** +19295347832 || **LinkedIn**

Professional Summary:

Cybersecurity Analyst with 3+ years of experience and a strong track record of utilizing industry-leading tools such as McAfee, CrowdStrike, SIEM, EDR, and XSOAR. Proven ability to enhance threat detection and response capabilities while significantly reducing phishing attempts through strategic analysis and proactive measures. Highly skilled in managing high-pressure environments, providing actionable insights that minimize security incidents, and strengthening organizational resilience. Committed to leveraging expertise to elevate and secure your cybersecurity framework.

Technical Skills:

SIEM Tools:	IBM QRadar, Splunk
Cloud Security:	AWS Security Hub, Azure Security Center
Endpoint Detection & Response:	CrowdStrike, Carbon Black, Microsoft Defender ATP
(IDS/IPS):	Snort, Suricata, Cisco Firepower, Mcafee
Encryption Solutions:	VeraCrypt, BitLocker, OpenSSL
Penetration Testing:	Kali Linux, Metasploit, Burp Suite
Forensics Tools:	EnCase, Volatility, FTK, Autopsy.
Vulnerability Scanning:	OpenVAS, Rapid7 Nexpose, Nessus
Firewalls:	Palo Alto Networks Firewalls, Fortinet, Cisco
Data Loss Prevention (DLP):	Forcepoint DLP, Symantec DLP
Compliance & Regulatory:	HIPAA, GDPR, PCI DSS, NIST, ISO 27001
Network Traffic Analysis:	Zeek (Bro), NetFlow
Security Protocols & Standards:	OWASP, MITRE attack framework
Network Access Compliance:	Forescout NAC
Certifications:	CompTIA Security+

Professional Experience:

Cyber Security Analyst | Cerner – MD — Jun 2025 - Current

- Led a **global SIEM optimization initiative** supporting Cerner's **EHR platforms and healthcare IT systems**, enhancing threat detection and incident response across clinical, administrative, and cloud-based healthcare environments while ensuring compliance with HIPAA, and healthcare security standards.
- Utilized **Splunk Enterprise** for centralized log management and advanced event correlation, ingesting logs from **EHR systems, clinical applications, databases, cloud infrastructure, IAM solutions, and network devices**, significantly improving threat visibility and early detection of suspicious activities.
- Conducted **continuous vulnerability assessments** using **Tenable.io** across Cerner-hosted healthcare applications, databases, and infrastructure, prioritizing remediation based on **CVSS scores and clinical risk impact**, reducing exposure to vulnerabilities affecting patient data and clinical workflows.
- Implemented **automated SIEM alerting and correlation use cases** for healthcare-specific threats, improving **Mean Time to Detect (MTTD) by 30%**, enabling faster identification of security incidents impacting EHR availability and integrity.
- Deployed and managed **Proofpoint email security** to protect healthcare communications, mitigating phishing, malware, and business email compromise (BEC) attacks targeting **clinical staff, administrators, and healthcare partners**.
- Customized **Forcepoint DLP policies** to safeguard **Electronic Health Records (EHR), PHI, and sensitive healthcare data** across endpoints, servers, and cloud environments, preventing data exfiltration via email, web uploads, removable media, and third-party integrations.
- Adopted **Agile cybersecurity practices** to improve collaboration between **security, application, and healthcare IT teams**, enabling faster threat response, continuous improvement of SIEM use cases, and minimal disruption to **clinical and patient-care services**.

Cyber Security Engineer | Capgemini – India — Jun 2021 – Jul 2024

- Integrated **IBM QRadar SIEM** with financial transaction logs, ATM switches, and online payment platforms, building custom correlation rules to detect fraud attempts & insider misuse. Enhanced SOC visibility with advanced dashboards, threat intelligence feeds, and real-time alerts for faster incident response.
- Conducted **vulnerability assessments** using **OpenVAS and Rapid7 Nexpose**, uncovering misconfigurations in payment gateways, APIs, and third-party vendor integrations. Partnered with **risk and compliance teams** to prioritize remediation within regulatory deadlines, reducing audit gaps significantly.
- Designed robust data protection strategies under **PCI DSS**, and **GDPR** by implementing **encryption**, **tokenization**, and **role-based access controls (RBAC)**. Delivered audit-ready compliance documentation, resulting in a **40%** audit pass rate across internal and external reviews, with zero non-compliance findings.
- Deployed **Palo Alto Next-Gen Firewalls** and **Cisco ASA Firewalls** to segment SWIFT, payment, and internet banking networks. Implemented **SSL/TLS inspection, intrusion prevention, and DoS/DDoS mitigation policies**, strengthening fraud-prevention and reducing attack surfaces.
- Implemented **Forcepoint DLP** across **email, cloud storage, and endpoints**, preventing unauthorized transfers of sensitive financial data. Automated regulatory compliance reporting workflows, improving monitoring efficiency and audit readiness.
- Performed **penetration testing** of online banking apps using **Burp Suite, Kali Linux, and OWASP Top 10** methodology. Identified SQL injection, XSS, session hijacking, and insecure API endpoints, and worked with developers to implement secure coding best practices.
- Utilized **EnCase** and **FTK Forensics** during fraud investigations involving rogue employees and compromised accounts. Extracted and analyzed digital evidence, and delivered litigation-ready forensic reports, contributing to **75%** increase in investigation turnaround speed and enabling timely action by compliance & legal teams.
- Configured **VeraCrypt** encryption for transaction databases and financial archives, ensuring compliance with cross-border data transfer regulations. Achieved a **50%** reduction in audit findings by standardizing encryption and access control across sensitive systems.
- Documented **NIST Cybersecurity Framework** policies and created **fraud-response playbooks, risk-control checklists, and** compliance workflows. Conducted quarterly fraud-awareness and security workshops for finance, audit, and compliance teams, strengthening the overall security culture.

Education:

Master of Science in Cybersecurity – Yeshiva University, New York, USA
Post Graduate Diploma in Cybersecurity – Indian Institute of Information Technology (IIIT), Bangalore, India
Bachelor of Technology in Computer Science – Malla Reddy Institute of Technology**,** Hyderabad, India