

PROFESSIONAL SUMMARY:

I am a results-driven cybersecurity professional with expertise in IAM, Governance, Risk, and Compliance, SOC, and vulnerability remediation. Proven track record of implementing robust security controls, detecting threats, monitoring, and driving successful audits in alignment with global standards like SOC2, GDPR, HIPAA, and PCI-DSS.

SKILLS:

- **Frameworks and Standards:** HIPAA, PCI-DSS, NIST CSF, NIST SP 800-53, CIS benchmarks, ITIL, ISO 27001, and ISO 27002
- **Identity and Access Management:** Duo Security, Azure Entra ID, On-premises Active Directory, YubiKeys
- **Penetration Testing and Ethical Hacking:** Kali Linux, Metasploit, Nmap, Burp Suite, Wireshark, Hydra and John the Ripper
- **SIEM Tools:** SolarWinds, Microsoft Sentinel and Splunk
- **Vulnerability Scanning and Management:** Tenable Nessus, Microsoft Defender for Endpoint
- **Endpoint Detection and Response:** Forti EMS and Microsoft Defender ATP
- **Compliance and GRC Tools:** Service Now GRC, SAP GRC and Microsoft Purview
- **Data Loss Prevention:** Microsoft 365 DLP
- **Security Awareness and Training:** KnowBe4
- **Programming:** Python
- **Physical Security:** Alarm.com
- **Databases:** MySQL
- **Cloud:** Azure and AWS

PROFESSIONAL EXPERIENCE:**Liberty Software****Senior Information Security Analyst****March 2024-Present**

- Solely accountable for organization-wide cybersecurity strategy and execution, leveraging organizational skills to automate processes and collaborate cross-functionally for comprehensive protection and compliance.
- Scans web applications and networks with Tenable Nessus, cutting critical vulnerabilities by 70% through effective remediation.
- Manage end-to-end risk management including TPRM, due diligence, SQ, track metrics and holds meetings with stakeholders with reporting.
- Monitors 10,000+ monthly security events and proactive threat hunting with Microsoft Sentinel using AI enhancing threat detection capabilities.
- Conduct in-depth analysis and interpretation of HITRUST requirements, ensuring alignment with compliance evidence by reviewing documents
- Collaborate with SMEs to address gaps, delivering clear, concise findings to support regulatory compliance for SOC2, PCI-DSS and HITRUST
- Streamline audits with internal stakeholders and cross-functional teams streamlining evidence collection and assessment processes
- Implemented a comprehensive identity lifecycle management framework, reducing user onboarding time by 30% across 5 azure b2c tenants
- Manages 300+ endpoints and 100+ servers using Forti EMS for remote connection, blocking removable devices, virus and malware protection
- Implemented user federation in LastPass, KnowBe4 and with Microsoft Entra ID, reducing administrative overhead by 73%.
- Deployed MFA with YubiKeys and Cisco Duo across 100+ servers, reducing unauthorized access incidents by over 40%
- Revised all Information Security Policies to align with NIST CSF, HIPAA and PCI-DSS standards ensuring robust security posture.

Natsoft Corporation**Security Analyst****August 2023-March 2024**

- Analyzed security events in Splunk Enterprise, refining queries and rule sets to achieve 90% true positives and minimize false alarms.
- Ensured 100% compliance with GDPR, SOX, and PCI-DSS through Microsoft Defender, addressing all detected vulnerabilities.
- Revamped risk management SOPs and incident playbooks, driving consistency in security practices and enhancing organizational resilience
- Strengthened security posture by driving cross-departmental collaboration to resolve audit findings and ensure full regulatory compliance

University of Central Missouri**IT Support Specialist****December 2022 -June 2023**

- Configured and maintained antivirus and endpoint protection software on user devices, mitigating potential malware threats
- Created and updated documentation for IT support procedures, troubleshooting guides, and security configurations to streamline operations

Infosys – Novartis Pharmaceuticals**Cybersecurity Analyst (Acted as lead)****August 2021 - July 2022**

- Led a team of 15 for Vulnerability and risk management, access control and Onapsis SAP Cybersecurity team using shift left approach.
- Reviewed CVSS/CVE to triage vulnerabilities, maintained risk register and developed risk management plans using NIST SP 800-37.
- Conducted internal audits and acted as a liaison between business stakeholders and cross-functional teams to resolve audit findings.
- Integrated Splunk with Onapsis to enhance threat detection, streamline incident response, centralize visibility, improve risk management, enable advanced analytics, automate compliance reporting, and reduce MTTR for ERP security

Tata Consultancy Services**GRC Analyst – Ericsson IT****October 2019-August 2021**

- Achieved 100% GDPR compliance by implementing strict data security protocols and periodic user access reviews for internal audits.
- Reduced application code and system vulnerabilities by 63% with Virtual Forge, significantly improving security and compliance
- Implemented end-to-end GRC Access Control 12.0 and integrated with ERP Systems in accordance with SOX Standards and to ensure SOD

Security Administrator – Tata Motors**September 2018-October 2019**

- Architected, automated and managed SAP role/user administration, enforcing least privilege for secure access and privilege access management.
- Performed Internal audits and provided 24/7 on-call support during key updates, ensuring system security and operational continuity.

EDUCATION:

- Master of Science in Cybersecurity and Information Assurance - University of Central Missouri – December 2023
- Bachelor of Technology in Computer Science and Engineering – Vignan Institute of Science and Technology – May 2018

CERTIFICATIONS:

Microsoft Security Operations Center Analyst Associate | CompTIA Security+ | (ISC)2 CC | SANS AI for Business Leaders | AWS Cloud Quest Cloud practitioner| Google Cybersecurity