Ditikrushna Routray

Cyber Risk & Compliance Analyst

ditikrushnaroutray@gmail.com Cuttack,Odisha ditikrushnaroutray.netlify.app

linkedin.com/in/ditikrushnaroutray github.com/ditikrushnaroutray

PROFILE

GRC Analyst with **3+ years** of freelance experience bridging **IT operations** and **security governance**. Experienced in **auditing access controls**, **dissecting network protocols**, and **identifying compliance violations**. Specializes in documenting **threat models** and **remediation strategies** to protect corporate assets.

SKILLS

- **Compliance & Risk: NIST 800-53**, **PCI DSS v4.0**, ISO 27001 , SOC2 , **control assessment**, **gap analysis**, remediation tracking, audit evidence collection, **risk register management**
- **Control Testing: Control design review**, **operating effectiveness testing**, findings documentation, evidence sufficiency
- **Security & Forensics: Incident Response Planning**, Network Traffic Analysis (Wireshark/tshark), **Access Control Auditing**, PAM log analysis, **MITRE ATT&CK**
- **Operating Systems: Enterprise Linux Administration** (Ubuntu, Arch,Kali), Windows Security Basics, Bash scripting
- **Development: Python** (Security & Compliance Automation), Git, GitHub

PROJECTS

Access Control & Policy Audit (Project Nighthawk) 04/2026 – 04/2026

- Executed an **access control audit** on a Linux (Ubuntu) environment to test resilience against brute-force authentication bypass.
- Documented findings in a **Risk Register**, mapping the technical vulnerabilities to standard control frameworks (e.g., **NIST 800-53**).
- Authored a **mock remediation policy** requiring the implementation of account lockout controls (Fail2Ban).

Incident Response Simulation (HawkEye Lab) 04/2026 – 04/2026

- Analyzed network traffic and extracted malicious payloads to simulate a **post-breach forensic review**.
- Drafted a technical **Incident Report** detailing the threat actor's TTPs using the **MITRE ATT&CK** framework.
- Outlined **preventative controls** and policy updates required to prevent recurrence of data exfiltration.

Automated Compliance & Integrity Monitoring (Sentinel-FIM) 01/2026 – 03/2026

- **Engineered an automated File Integrity Monitoring (FIM)** solution to satisfy mandatory regulatory controls (e.g., **PCI-DSS Requirement 11.5, SOC 2**) regarding the detection of unauthorized system modifications.
- **Designed cryptographic baseline comparisons** that generate **structured, immutable audit logs**, providing verifiable evidence of continuous system integrity for external regulatory reviews.
- **Enforced least-privilege execution principles** and authored clear operational documentation, aligning technical endpoint defense directly with **IT risk mitigation and access governance frameworks**.

CERTIFICATES

- Google CyberSecurity

EDUCATION

B.Sc. Computer Science | Utkal University | 2023 – 2026
*Class 12 (Science) | **CHSE Odisha** | 2021 – 2023*