Tools for Implementing Secure Backup & Restore

This document outlines the tools and recommended technologies to implement the Secure Backup & Restore feature into the Unified OT Ransomware Protection Platform. The tools below align with a Python-based microservice architecture using FastAPI and AWS S3 for secure cloud storage.

# 🔐 1. Encrypt Backup Data

• Tool: `cryptography` (Python library)  
 - Use AES-256 to encrypt all files before uploading to AWS.  
 - Supports encryption at rest ensuring data confidentiality.

Python from cryptography.fernet import Fernet

# 🔒 2. Secure Data in Transit

• Protocol: TLS 1.3  
 - AWS SDK (boto3) uses TLS 1.3 by default.  
 - FastAPI interface should be exposed over HTTPS (via Uvicorn or Nginx with certs).

# ✉️ 3. Verify Integrity

• Tool: `hmac` (Python) or `cryptography.hazmat.primitives.hmac`  
 - Generates HMAC-SHA256 to ensure file or log integrity.  
 - Verifies restored data hasn't been tampered with.

# 📋 4. Backup Schedules & Triggers

• Tools: `cron`, `Airflow`, `Kubernetes CronJobs`, or FastAPI scheduler.  
 - Users can choose full, incremental, or snapshot-based backups.  
 - Triggers include manual CLI, web interface, or SOAR signal.

# 📦 5. Immutable Storage

• Platform: Amazon S3 with Object Lock  
 - Enables Write Once Read Many (WORM) policy.  
 - Supports retention periods and legal holds.

# 🔍 6. Logging Backup Events

• Tools: Python `logging`, `ELK Stack`, or `Wazuh`  
 - Store backup/restore logs in append-only files.  
 - All logs include HMAC hash for verification.  
 - Forward logs to centralized visual dashboard.

# 🔑 7. Secret and Key Management

• Tools: HashiCorp Vault or `.env` files (for dev/test)  
 - Stores AES keys and HMAC secrets securely.  
 - Keys should rotate periodically and be access-controlled.

# 📊 Recommended Tool Stack

|  |  |
| --- | --- |
| Feature | Tool(s) |
| File encryption | `cryptography` (AES-256) |
| Secure transfer | TLS 1.3 via boto3/FastAPI |
| Logging + HMAC | Python `logging`, `hmac`, ELK |
| AWS storage | S3 with Object Lock |
| Scheduling | Cron, Airflow, SOAR |
| Secrets management | Vault / .env |
| Interface & API | FastAPI + HTTPS |

# 🔌 Summary

These tools support the end-to-end security lifecycle of the Backup and Restore feature. They ensure confidentiality, tamper-proof operation, and audit-friendly records while maintaining compliance with industry standards such as IEC 62443 and NERC CIP. With these technologies in place, your platform achieves robust ransomware resilience and operational reliability.