Secure Backup and Restore Implementation in Our Platform

Our platform includes Secure Backup and Restore as a critical feature to ensure data survivability, business continuity, and ransomware recovery.  
  
Within the Unified OT Ransomware Protection Platform, Secure Backup and Restore protects critical data such as system configurations, firmware, logs, and operational files. This module integrates seamlessly with the SOAR engine, logging infrastructure, and AWS-based immutable storage to enable fast, secure, and tamper-proof recovery processes.

# 🔗 How It Links to Other Modules

Each module works in coordination with the Secure Backup and Restore component:  
  
- Real-Time Monitoring → Triggers backup pre-checks when anomalies arise.  
- Ransomware Detection Engine → Initiates snapshot or full backup prior to potential compromise.  
- SOAR Engine → Automates backup and restore procedures through playbooks.  
- Secure Logging → All backup/restore actions logged with AES-256 + HMAC.  
- Admin Dashboard → Shows current status of all backups and restore operations.

# 🔐 Key Functions of This Feature

- Provides three backup types: Full, Incremental, and Snapshot-based backups. (user can choose and configure)  
- Integrates with AWS S3 Object Lock for immutable, versioned storage.  
- Encrypts data before backup using AES-256, and transfers via TLS 1.3.  
- Appends HMAC to all backup/restore logs for verification.  
- Enables scheduled or triggered backups via user choice or SOAR events.  
- Ensures all actions are logged and audit-ready.

# 🧠 When It Becomes Useful

This module is essential during:  
  
- Pre-incident preparation – scheduled backups  
- During an incident – triggered backups or snapshots  
- Post-incident – fast, secure restore without paying ransom  
- Recovery testing – validating sandbox restore scenarios

# ✅ Summary

Secure Backup and Restore acts as the backbone of operational resiliency within our platform. The module works silently in the background but plays a vital role when disaster strikes. It combines encrypted backup storage, automated recovery, and verified logging to provide a trustworthy, ransomware-resilient protection framework.  
  
Our architecture empowers users to recover with confidence, meet audit and compliance needs, and maintain 24/7 operations even under attack.