Remote Data Storage, Mitigation M1029 - Enterprise

Archived: 2026-04-05 17:54:34 UTC

Remote Data Storage focuses on moving critical data, such as security logs and sensitive files, to secure, off-host locations to minimize unauthorized access, tampering, or destruction by adversaries. By leveraging remote storage solutions, organizations enhance the protection of forensic evidence, sensitive information, and monitoring data. This mitigation can be implemented through the following measures:

Centralized Log Management:

- Configure endpoints to forward security logs to a centralized log collector or SIEM.
- Use tools like Splunk Graylog, or Security Onion to aggregate and store logs.
- Example command (Linux): `sudo auditd | tee /var/log/audit/audit.log | nc <remote-log-server> 514`

Remote File Storage Solutions:

- Utilize cloud storage solutions like AWS S3, Google Cloud Storage, or Azure Blob Storage for sensitive data.
- Ensure proper encryption at rest and access control policies (IAM roles, ACLs).

Intrusion Detection Log Forwarding:

- Forward logs from IDS/IPS systems (e.g., Zeek/Suricata) to a remote security information system.
- Example for Suricata log forwarding:
  `outputs:
- type: syslog
  protocol: tls
  address: `

Immutable Backup Configurations:

- Enable immutable storage settings for backups to prevent adversaries from modifying or deleting data.
- Example: AWS S3 Object Lock.

Data Encryption:

- Ensure encryption for sensitive data using AES-256 at rest and TLS 1.2+ for data in transit.
  Tools: OpenSSL, BitLocker, LUKS for Linux.

Source: https://attack.mitre.org/mitigations/M1029