Logging

ISO 27002 Control 8.15

Control

Logs that record activities, exceptions, faults and other relevant events should be produced, stored, protected and analysed

Purpose

To record events, generate evidence, ensure the integrity of log information, prevent against unauthorized access, identify information security events that can lead to an information security incident and to support investigations

Why is it important?

- Logs are crucial for correlation, alerting, and investigation - especially when time sources are synchronized
- They help maintain accountability for privileged users (who might manipulate logs)
- Protection ensures log integrity for legal/disciplinary evidence
- Log analysis identifies indicators of compromise and anomalous behaviour

How to implement ?

- Document a topic-specific policy on logging detailing purpose and protection requirements
- Collect logs including user IDs, system activities, dates, device identity, and network addresses
- Protect logs by restricting delete/de-activate permissions (especially for privileged users) and using techniques like cryptographic hashing
- Perform log analysis using specific monitoring tools (e.g., SIEM, UEBA) and threat intelligence

What are the related concepts ?

- Logging
- Log integrity
- Clock synchronization
- SIEM (Security Information and Event Management)
- UEBA (User and Entity Behaviour Analytics)
- PII protection

Link with other frameworks

- NIST 800-53 rev5 : AU-3, AU-6, AU-9, AU-11, AU-12, AU-14
- NIST CSF 2.0 : PR.PS-04, DE.CM-03, RS.MA-02

Renaud Dardenne
Asphalia Consulting