Monitoring activities

ISO 27002 Control 8.16

Control

Networks, systems and applications should be monitored for anomalous behaviour and appropriate actions taken to evaluate potential information security incidents

Purpose

To detect anomalous behaviour and potential information security incidents

Why is it important?

- Establishing a baseline helps accurately identify true anomalies and minimizes false positives
- It ensures quick response to positive indicators from the monitoring system

To what is it applicable ?

- Monitoring outbound and inbound network, system, and application traffic
- Establishing a baseline of normal utilization and access patterns for users
- Configuring automated monitoring software to generate alerts based on predefined thresholds

How is it evidenced ?

- Documented monitoring scope and level
- Documentation defining the established baseline of normal behaviour and utilization
- Configuration settings of monitoring tools showing alerts based on predefined thresholds
- Records of alerts generated and the corresponding response actions
- Records of monitoring maintained for defined retention periods

Link with other frameworks

- NIST 800-53 rev5 : AC-2(12), AC-17(1), AU-13*, IR-4(13)*, MA-4(1)*, PE-6*, PE-6(3)*, SI-4, SI-4(4)*, SI-4(13)*, SI-4(16)*
- NIST CSF 2.0 : ID.AM-03, ID.RA-02, DE.CM-01, DE.CM-03, DE.CM-06, DE.CM-09, RS.MA-02

Renaud Dardenne
Asphalia Consulting