Security Monitoring: Key Aspects & Security Requirements

The following table highlights Key Aspects security monitoring to consider, and a relevant Security Monitoring Requirement for each. It also recommends examples of what your organisation can do to meet each of the requirements.

Key Aspects	Security Monitoring Requirement	Recommended steps to meet the Security Monitoring Requirements
 Business traffic crossing a boundary	Traffic exchanges are authorised and conform to security policy. Transport of malicious content and other forms of attack by manipulation of business traffic are detected and alerted.	• Collect details of imports and exports executed by internal users. • Track cross-boundary information exchange operations. • Collect information on the use of any externally visible interfaces. • Collect information and alerts from content checking and quarantining services.
 Activity at a boundary	Detect suspect activity indicative of the actions of an attacker attempting to breach the system boundary, or other deviation from normal business behaviour.	• Collect information from firewalls and other network devices for traffic and traffic-trend. • Collect information from any Intrusion Detection Service (IDS) at the boundary with any un-trusted network.
 Internal workstation, server or device	Detect changes to device status and configuration from accidental or deliberate acts by a user, or by malware.	• Record changes to device configuration. • Record indications that could be attributed to accidental or malicious activity (eg system restarts or undefined system processes). • Record indications of unauthorised actions in tightly controlled environments such as the attachment of USB storage devices. • Collect information relating to access to any business critical file areas.
 Internal network activity	Detect suspicious activity that may indicate attacks by internal users, or external attackers who have penetrated the internal network.	• Monitor critical internal boundaries and resources within internal networks. Possible candidates for heightened internal monitoring include: ▪ core electronic messaging infrastructure (eg email servers & directory servers) ▪ sensitive databases (eg HR databases, finance, procurement/contracts, etc.) ▪ project servers and file stores with restricted access requirements
 Network connections	Prevent unauthorised connections to the network made by remote access, VPN, wireless or any other transient means of network connection.	• Monitor network access points that are open to connection attempts by anyone (eg WiFi access points). • Monitor mobile users and remote working solutions. • Monitor restrictive environments in which the attachment of modems and wireless access points are prohibited. • Monitor network ports of the wired network environment.
 Session activity by user & work station	Detect unauthorised activity and access that is suspicious or violates security policy requirements.	• Monitor user activity and sensitive data accesses to ensure they can be made accountable for their actions. • Monitor workstation connectivity, connected peripherals and data ports. • Profile normal user activity to enable detection of abnormal behaviour. • Tightly control and monitor administration and service accounts.
 Alerting on events	Be able to respond to security incidents in a time frame appropriate to the perceived criticality of the incident.	• Ensure events classed as critical are notified in as close to real-time as is achievable. • Ensure automation and filtering is sufficient to bring events to the attention of the right people using the right mechanism. • Establish the correct level of monitoring for the organisation, ranging from simple monitoring to integrated solutions using enterprise level centralised security. • Consider combining functions such as security and network management, taking into account maintaining segregation requirements. • Implement secondary alerting channels (eg SNMP, email, SMS, etc.) using in-hours or out-of-hours services when continuous console manning cannot be provided
 Accurate time in logs	Be able to correlate event data collected from disparate sources.	• Provide a master clock system component which is synchronised to an atomic clock • Update device clocks from the master clock using the Network Time Protocol (NTP) • Record time in logs in a consistent format - Universal Co-ordinated Time (UTC) is recommended • Provide a process to check and update device clocks on a regular basis (eg weekly) • Define the error margin for time accuracy according to business requirements • Provide manual maintenance for devices that do not support clock synchronisation • Provide support for local time on human interfaces • Provide a process to correct clock drift on mobile devices upon reconnection
 Data backup status	Be able to recover from an event that compromises the integrity or availability of information assets.	• Provide an audit trail of backup and recovery to enable identification of the last known good state of the information assets. • Alert storage failure events.