

Checklist

8.16 – Monitoring van activiteiten

Thema: Technisch | ISO 27002: 8.16 | Gerelateerd: 8.15, 8.17

Doelstelling

Aantonen dat netwerken, systemen en applicaties actief worden gemonitord op afwijkend gedrag en beveiligingsgebeurtenissen, zodat dreigingen tijdig worden gedetecteerd.

Monitoringstrategie en -beleid

- ☐ Is er een vastgestelde monitoringstrategie voor netwerken, systemen en applicaties?
- ☐ Zijn monitoringsdoelstellingen en te detecteren scenario's beschreven?
- ☐ Is vastgelegd wie verantwoordelijk is voor monitoring en opvolging van meldingen?
- ☐ Is monitoring ingericht op basis van een risicoafweging (kritieke systemen prioriteit)?

Technische monitoringsmaatregelen

- ☐ Is een SIEM (Security Information and Event Management) systeem ingericht?
- ☐ Zijn detectieregels en use cases geïmplementeerd in de SIEM?
- ☐ Is IDS/IPS (Intrusion Detection/Prevention System) ingericht op het netwerk?
- ☐ Worden netwerkverbindingen gemonitord op ongebruikelijk dataverkeer?
- ☐ Is endpoint detection and response (EDR) geïmplementeerd op endpoints?

Alerting en respons

- ☐ Worden alerts automatisch gegenereerd bij detectie van afwijkingen?
- ☐ Is er een proces voor triage en opvolging van beveiligingsalerts?
- ☐ Zijn drempelwaarden voor alerts afgestemd op het acceptabele risico (minimaliseer false positives)?
- ☐ Is er 24/7 monitoring ingericht voor kritieke systemen of is dit uitbesteed?

Rapportage en verbetering

- ☐ Worden monitoringbevindingen periodiek gerapporteerd aan management of CISO?
- ☐ Worden detectieregels regelmatig bijgewerkt op basis van actuele dreigingen?
- ☐ Worden false positives geanalyseerd en gebruikt om detectieregels te verbeteren?



Worden trends in beveiligingsgebeurtenissen gebruikt als input voor risicoanalyse?

Verantwoordelijke:	_____	Datum controle:	_____
Afdeling:	_____	Score:	___ / 21
Reviewcyclus:	☐ Jaarlijks ☐ Na wijziging ☐ Na incident		Status: ☐ Voldoet ☐ Actiepunt ☐ N.v.t.