

incident_log_template

Intzidentzien Erregistroa

Txantiloi hau segurtasun intzidentziak erregistratzeko erabiliko da.

Intzidentziaren Xehetasunak

- ID:** [INC-Urtea-Zbk] (adib. INC-2024-001)
- Data eta Ordua:** [YYYY-MM-DD HH:MM]
- Detektatzailea:** [Izena/Sistema]
- Mota:** [Malware / Phishing / DDoS / Baimenik gabeko sarbidea / Datu Ihesa / Bestelakoak]
- Larritasuna:** [Baxua / Ertaina / Altua / Kritikoa]

Deskribapena

- Zer gertatu da?** (Laburpen teknikoa)
- Kaltetutako Sistemak:** [IPak, Izenak, Zerbitzuak]
- Eragina:** [Produkzioa geldituta, Datuak galdu, Webgunea erorita...]

Erantzuna

- Hasierako Ekintzak:** (adib. Sarea isolatu, erabiltzailea blokeatu)
- Arduraduna:** [Izena]
- Egoera:** [Ireki / Aztertzen / Konponduta / Itxita]

Analisia eta Konponbidea

- Erro-kausa (Root Cause):**
- Hartutako neurriak:**
- Froga / Ebidentziak:** (Logs, Pantaila-argazkiak - Erantsi erreferentzia)

Ikasitako Lezioak

- Zer egin zitekeen hobeto?
- Beharrezko al da Segurtasun Plana egunearatzea?