ot_incident_simulation_report

OT Intzidentzia Simulazio Txostena - Zabala Gailetak

1. Intzidentziaren Xehetasunak

- **Data:** 2024/05/20
- **Simulazio Mota:** OT Sarera baimenik gabeko sarbidea (Modbus manipulazioa).
- **Parte Hartzaileak:** IT Taldea, OT Mantentze Taldea, Zibersegurtasun Arduraduna.

2. Gertaeraren Deskribapena (Simulazioa)

Erasotzaile batek (Red Team) bulegoko saretik (IT) produkzio sarera (OT) jauzi egitea lortu zuen, gaizki konfiguratutako ingeniaritza-estazio bat erabiliz (Dual-homed PC: bi sareetara konektatuta zegoen ekipoa). Erasotzaileak Modbus komandoak bidali zizkion labeko PLCari tenperatura arriskutsu batera igotzeko.

3. Detekzioa

- **Ordua:** 10:15
- **Alerta:** SIEM sistemak “Modbus Write Coil” komando ezohikoak detektatu zituen PLC kritiko batean, baimendu gabeko IP helbide batetik.
- **Operadorea:** HMI pantailan tenperatura igotzen hasi zela ikusi zuen eta “Larrialdi Geldialdia” aktibatu zuen fisikoki.

4. Erantzuna eta Edukiera

1. **Isolamendua (10:20):** Firewall-ean IT-OT konexio guztiak moztu ziren “Panic Button” politikaren bidez.
2. **Identifikazioa (10:30):** Sareko trafikoa aztertuz, erasoaren jatorria “INGENIARITZA-PC-03” zela ikusi zen.
3. **Analisi Forentsea:** Ekipoa saretik deskonektatu eta diskaren irudia egin zen. Malwarea (RAT) aurkitu zen, USB kutsatu baten bidez sartutakoa.

5. Zuzenketa eta Ikasitakoa

- **Ahultasuna:** Sare segmentazioa saihestu zen bi saretara konektatutako PC baten bidez (Bridging).
- **Ekintza Zuzentzaileak:**
    - “Dual-homing” guztiz debekatu da. Ingeniaritza estazioak OT sarean bakarrik egongo dira.
    - USB gailuak blokeatu dira USB bidezko erasoak saihesteko.
    - PLCetan “Read-Only” modua aktibatu da urruneko konexioentzat, aldaketak fisikoki bakarrik baimenduz panel nagusitik.

6. Ondorioa

Simulazioak erakutsi du erantzun denborak onak izan direla (15 minutu), baina segmentazio fisikoa hobetu behar dela giza akatsak ekiditeko.