

PLAN_IMPLEMENTACION_PRESUPUESTO_ZABALA_GAILETAK

INIMPLEMENTAZIO PLANO OSOA - ZABALA GAILETAK SEGURTASUN INTEGRALAREN AURREKONTUA

PROIEKTUAREN IKUSPEGI OROKORRA

Bezeroa: Zabala Gailetak S.A. - Industria panifikadora (120 langile, Euskal Herria)

Esparrua: Segurtasuna OT/ICS + SIEM/SOC + Honeypot-ak + RRHH Ataria

Aurrekontu Totala: €733,950 1. Urtea + €129K/urte errepikakorra

Egitaraua: 10 hilabete implementazioa (Urtarrila-Abendua 2026)

ROI: %137.6 3 urtetan (€786K/urte onurak)

Emaitz espeora: IT/OT dokumentu profesional 35-40 orrialde estandarrak jarraituz, 3 zatitan banatuta hainbat publikorentzako.

DOKUMENTU FINALAREN EGITURA

PRESUPUESTO_ZABALA_GAILETAK_SEGURIDAD_INTEGRAL.md

- I. Atala: Laburpen Exekutiboa (6 orrialde) ⏳ EGITEKE
- II. Atala: Eskaintza Komertziala (8-10 orrialde) ⏳ EGITEKE
 - 7. Sekzioa: Zerbitzu Paketeak (3 maila)
 - 8. Sekzioa: Prezio Xeheak Hitoekin
 - 9. Sekzioa: Baldintza Komertzialak
 - 10. Sekzioa: Arrakasta Kasuak eta Erreferentziak
 - 11. Sekzioa: Zerbitzu Maila Akordioak
 - 12. Sekzioa: Balio Proposamena eta Diferentiazioa
- III. Atala: Espezifikazio Teknikoak (20-25 orrialde) ⏳ EGITEKE
 - 13. Sekzioa: IT/OT Arkitektura (Purdue Modeloa)
 - 14. Sekzioa: OT Segurtasun Implementazioa
 - 15. Sekzioa: SIEM & SOC (Wazuh vs ELK)
 - 16. Sekzioa: Honeypot Despliegue Arkitektura
 - 17. Sekzioa: HR Atari Espezifikazio Teknikoak
 - 18. Sekzioa: Betetze Mapeoa (ISO/IEC/GDPR)
 - 19. Sekzioa: Implementazio Plano Xehea
 - 20. Sekzioa: Arrisku Kudeaketa & FMEA
 - 21. Sekzioa: Eranskin Teknikoak

II. ATALA: ESKAINITZA KOMERTZIALA (7-16 orrialdeak)

7. Sekzioa: Zerbitzu Paketeak (7-9 orrialdeak)

Helburua: 3 zerbitzu maila behar eta aurrekontu desberdinatarako aurkeztea

Edukia xehea: 1. Pakete Oinarritzko - “OT Oinarria” (€180,000) - OT Segurtasun audit osoa - SIEM

oinarrizkoa (8x5 monitorizazioa) - Prestakuntza oinarrizkoa (40 ordu) - Email/telefono laguntza - Iraupena: 3 hilabete

2. Pakete Profesionala - “OT Aurreratua” (€324,000) ★ GOMENDATUA

- Oinarrizko guztia +
- Sare segmentazio osoa
- Honeypot-ak desplegatuta
- SIEM aurreratua OT alertekin
- Prestakuntza aurreratua (80 ordu)
- Lehentasunezko laguntza
- Iraupena: 5 hilabete

3. Pakete Empresariala - “OT Enterprise” (€733,950)

- Profesional guztia +
- HR Atari osoa
- SOC 24x7 6 hilabetez
- IT/OT integrazio osoa
- 24x7 laguntza
- Iraupena: 10 hilabete

4. Ezaugarrien Konparaketa Matrizea

Ezaugarria	Oinarrizkoa	Profesionala	Empresariala
OT Audit	✓	✓	✓
SIEM 8x5	✓	✓	✓
Sare Segmentazioa	✗	✓	✓
Honeypot-ak	✗	✓	✓
HR Ataria	✗	✗	✓
SOC 24x7	✗	✗	✓
Laguntza	Email	Lehentasunezko	24x7
Prestakuntza	40h	80h	120h

5. **Migrazio Bide-orria:** Nola hazi Oinarrizkoa → Profesionala → Empresariala eskuragarri den aurrekontuaren arabera

8. Sekzioa: Prezio Xeheak Hitoekin (10-11 orrialdeak)

Helburua: Kostuen eta ordainketen gardentasun desglosea

Edukia xehea: 1. **Pilarea Desglosea** (I. Atalean oinarrituta): - **1. Pilarea: OT Segurtasuna** €180,000 (%25) - Aktiboen inventarioa eta audit: €40K - Sare segmentazioa: €60K - PLC gotortzea: €35K - Jump host konfigurazioa: €25K - Dokumentazioa eta prestakuntza: €20K

- **2. Pilarea: SIEM & SOC** €120,000 (%16)
 - Plataforma konfigurazioa: €50K
 - Log integrazioa: €30K
 - Alerta garapena: €20K
 - SOC langileria (6 hilabete): €20K
- **3. Pilarea: Honeypot-ak** €24,000 (%3)
 - T-Pot plataforma: €8K
 - Conpot ICS: €10K
 - Integrazioa: €6K
- **4. Pilarea: HR Ataria** €300,000 (%41)
 - Backend garapena: €120K
 - Web frontend: €60K
 - Android app: €80K
 - Despliegua: €40K

- **PM & Audit** €110,000 (%15)
 - Proiektu kudeaketa: €50K
 - Betetze audit: €30K
 - Arrisku ebaluazioa: €30K

2. Ordainketa Hitoak (kontratu mailakatua):

Hito 1 (%30): Kontratuaren sinadura - €220,185
 Hito 2 (%20): OT Audit osoa + SIEM konfigurazioa - €146,790
 Hito 3 (%20): Segmentazioa + HR Atari 1. Fasea - €146,790
 Hito 4 (%20): Implementazio osoa - €146,790
 Hito 5 (%10): Go-live + onarpena - €73,395

3. 2. Urtea+ Kostu Errepikakorrak (€129,000/urte):

- SIEM monitorizazioa: €24K/urte
- SOC zerbitzuak (aukerakoa): €60K/urte
- HR Atari mantentzea: €30K/urte
- Segurtasun eguneraketak: €15K/urte

4. Aukerako Gehigarriak:

- Urteko penetrazio proba: €12K
- Gertaera erantzun kontratua: €15K
- Prestakuntza gehigarria: €1,500/egun
- Hiruhileko on-site auditoretza: €8K/urte

9. Sekzioa: Baldintza Komertzialak (12-13 orrialdeak)

Helburua: Baldintza kontratu argi eta profesionalak

Edukia xehea: 1. **Bermeak:** - Softwarea (HR Ataria): 12 hilabete akats bermea - Aholkularitza: 6 hilabete entregagarrien bermea - Hardwarea: 3 urte fabrikatzailaren bermea - Segurtasun konfigurazioak: 90 egun egokitzeko epea

2. Ordainketa Baldintzak:

- 30 egun fakturaz geroztik
- Atzerapen penalizazioa: %1.5 hileko
- Ordainketa azkarreko deskontua: %3 10 egunetan ordaintzen bada
- Onartutako metodoak: Banku transferentzia, txeke korporatiboa

3. Kontratu Iraupena:

- **1. Urtea:** Implementazio kontratua (10 hilabete)
- **2-3. Urteak:** Mantentze kontratua (aukerakoa)
- **Berritze deskontua:** %10 deskontua 3 urteko konpromiso aurreratuagatik

4. Bertan Behera Utzi Klautsulak:

- Bezeroaren bertan behera: Hito osatuetan oinarritutako itzulketak, eginiko lana kenduta
- Indar nagusia: Bi aldeak salbuetsita
- Errendimendu ezak: 30 eguneko konponketa epea

5. Erantzukizun Mugak:

- Kap orokorra: €733,950 (kontratuaren balioa)
- Ondoriozko kalteak: Baztertuta (negligentzia larria salbu)
- Ziber asegurua: €2M estaldura mantendu

6. Jabetza Intelektuala:

- HR Atari kodea: Zabala Gaietak-en jabetza ordainketa osoa ondoren
- Segurtasun konfigurazioak: Zabala-rako erabilera lizentzia
- Prestakuntza materialak: Lizentzia iraunkorra

10. Sekzioa: Arrakasta Kasuak eta Erreferentziak (14 orrialdea)

Helburua: Fideltasuna antzeko kasu anonimoen bidez

Edukia xehea: 1. **Kasu Ikaskuntza: Industria Esnegaia (Nafarroa)** (Anonimoa) - **Profilak:** 200 langile, ekoizpen automatizazioa - **Erronka:** OT segurtasunik gabe, ransomware mehatxu gertaera - **Soluzioa:** Antzeko OT audit + SIEM + segmentazioa - **Emaitzak:** 0 gertaera 24 hilabetean, ISO 27001 ziurtagiria, %180 ROI

2. 2. Kasu Ikaskuntza: Industria Panifikadora (Zabala antzekoa)

- **Profilak:** 80 langile, robotizatutako ekoizpen lerroak
- **Erronka:** SCADA legacy, auditoria trail-ik gabe
- **Soluzioa:** Purdue Modeloa + jump host-ak
- **Emaitzak:** IEC 62443 SL2 audit onartua, €300K ekoizpen gelditzea ekidinda

3. 3. Kasu Ikaskuntza: RRHH Digitalizazioa SME

- **Profilak:** 150 langile, fabrikatzaile industriala
- **Erronka:** RRHH prozesu paperezkoak, GDPR betetze gaps-ak
- **Soluzioa:** HR Atari pertsonalizatua app mugikorrarekin
- **Emaitzak:** %60 admin RRHH denbora murriztua, €50K urteko aurrezpenak

4. Erreferentziak (baimenarekin):

- Kontaktu informazioa: Izena, enpresa, telefonoa
- LinkedIn gomendioak
- Ziurtagiriak: ISO 27001 Lead Auditor, CISSP, IEC 62443 Certified

11. Sekzioa: Zerbitzu Maila Akordioak (15 orrialdea)

Helburua: Neur daitezkeen errendimendu konpromisoak

Edukia xehea: 1. **SIEM/SOC Erantzun Denborak:** | Larritasuna | Detekzioa | Erantzuna | Konponketa | -----|-----|-----|-----| | Kritikoa | 5 min | 15 min | 4 ordu | | Altua | 15 min | 1 ordu | 24 ordu | | Ertaina | 1 ordu | 4 ordu | 5 egun | | Baxua | 4 ordu | 24 ordu | 30 egun |

2. Sistemaren Eskuragarritasuna:

- SIEM: %99.5 uptime (gehienez 3.65h downtime/hile)
- HR Ataria: %99.0 uptime (negoziotako orduak 7am-11pm)
- Honeypot-ak: %95 uptime (sistemas isolatuak)
- OT Sarea: %99.9 uptime (gehienez 43 min/hile)

3. Laguntza Kanalak:

- **24x7 Hotline:** +34 XXX XXX XXX (Enpresarial paketea)
- **Sistema Ticketing:** Erantzuna <2h negozio
- **Email Laguntza:** Erantzuna <8h negozio
- **On-site Laguntza:** <4h gertaera kritikoetarako (Euskal Herria)

4. Pata Kudeaketa:

- Kritikoak: <72h
- Altua: <7 egun
- Arruntak: Hilabeteko mantentze leihoa

5. SLA Kredituak (SLA betetzen ez bada):

- %99.5-%99.0: %10 kreditu hileko
- %99.0-%95.0: %25 kreditu hileko
- <%95: %50 kreditua + konponketa plana

12. Sekzioa: Balio Proposamena eta Diferentziajazioa (16 orrialdea)

Helburua: Zergatik aukeratu gaituzten lehiakideen aurka

Edukia xehea: 1. Gako Diferentziatzaileak: - OT/ICS Espezializazioa: IEC 62443 gaitasuna duten enpresa gutxi Euskal Herrian - Elikadura Sektoruko Esperientzia: HACCP + zibersegurtasun integrazioaren ulermena - Tokiko Presentzia: Bilboko taldea, <2 ordu on-site eskuragarritasuna - Betetze Bikotza: ISO 27001 + IEC 62443 konbinatutako ikuspegia (kostu aurrezpena) - Euskarazko Laguntza: Dokumentazio eta prestakuntza euskara hizkuntza natiboan

2. Abantaila Teknikoak:

- Factory I/O + OpenPLC simulazioa (produkzioa probatu aurretik probak seguruak)
- Elikadura protokoloetarako Conpot honeypot espezializatuak
- GDPR Art. 88-rako (langileen datu babesa) eraikitako HR Atari pertsonalizatua
- PostgreSQL + Redis stack-a (enpresa maila, kode irekia kostu eraginkorra)

3. Negozio Balioa:

- **Arrisku Murrizketa:** Batez besteko €1.2M ransomware kostua ekiditea
- **Eragiketa Jarraitutasuna:** €500K/urteko ekoizpen gelditzea ekiditea
- **Betetzea:** GDPR €20M isunak ekiditeko, ISO 27001 eskatzen duten B2B kontratuak mantentzeko
- **RRHH Eraginkortasuna:** %60 admin overhead murrizketa (€44K/urteko aurrezpenak)

4. Lehiaketa Posizionamendua:

Faktorea Zabala Segurtasun Projektua IT Enpresa Generikoa Aholkularitza Handia
----- ----- ----- -----
OT Gaitasuna <input checked="" type="checkbox"/> IEC 62443 ziurtagiria <input checked="" type="checkbox"/> IT soilik <input checked="" type="checkbox"/> Bainan garestia
Elikadura Sektorua <input checked="" type="checkbox"/> Espezializatua <input checked="" type="checkbox"/> Generikoa <input checked="" type="checkbox"/> Generikoa
Tokiko Eskuragarritasuna <input checked="" type="checkbox"/> <2h <input checked="" type="checkbox"/> Urrutikoa soilik <input checked="" type="checkbox"/> HQ Madril
Kostua €733K 1. Urtea €500K (IT soilik) €1.2M+
Euskarazko Laguntza <input checked="" type="checkbox"/> Hizkuntza natiboa <input checked="" type="checkbox"/> Gaztelania soilik <input checked="" type="checkbox"/> Gaztelania soilik
HR Atari Barne <input checked="" type="checkbox"/> Pertsonalizatua <input checked="" type="checkbox"/> Esparrua kanpo <input checked="" type="checkbox"/> Bainan COTS

5. Arrakasta Metrikak (dashboard-ean jarraituta):

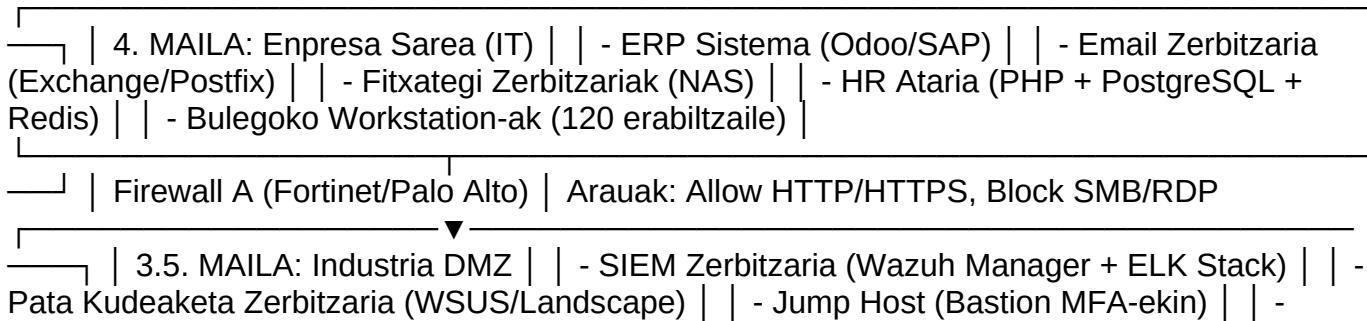
- 0 produkzioa kaltetzen duten gertaerak
- <%5 false positive tasa SIEM-ean 90 egunen ondoren
 - %95 HR Atari adopzioa 6 hilabetean
- ISO 27001 + IEC 62443 ziurtagiria 12 hilabetean

III. ATALA: ESPEZIFIKAZIO TEKNIKOAK (17-42 orrialdeak)

13. Sekzioa: IT/OT Arkitektura (Purdue Modeloa) (17-19 orrialdeak)

Helburua: Arkitektura seguruaren diseinu teknikoa

Edukia xehea: 1. Implementatutako Purdue Eredua (ASCII diagrama):



Historian DB (InfluxDB/TimescaleDB) | | - Honeypot Sarea (T-Pot, Conpot, Cowrie) -
ISOLATUA |

— | Firewall B (Industria Firewall) | Arauak: Whitelist soilik, Modbus/Profinet inspektiona

— | 3. MAILA: Eragiketak (OT) | | - SCADA Zerbitzaria (Ignition/WinCC) | | - HMI
Panelak (3x Siemens TP1200) | | - Ingeniaritza Workstation (TIA Portal, Factory I/O) | | -
OpenPLC Runtime (Simulazioa)

— | Switch Kudeatua (VLAN Segmentazioa)

— | 2. MAILA: Kontrol Sarea | | - PLC-ak (5x Siemens S7-1500, 3x Allen-Bradley
CompactLogix) | | - RTU-ak (Remote Terminal Units) |

— | Ethernet Industriala (Profinet/EtherNet/IP)

— | 1/0. MAILA: Eremuko Gailuak | | - Nahasketak (3x VFD-ekin) | | - Labeak (4x
industriak PID-ekin) | | - Enbalatze Robotak (2x ABB IRB 1200) | | - Sentsoreak
(Temperatura, Presioa, Fluxua - 50+ I/O puntu) | | - Aktuadoreak (Balbulak, Motorrak,
Garraiatzaileak) |

—

2. VLAN Diseinua:

VLAN 10: Bulego IT Sarea (192.168.10.0/24)

VLAN 20: Industria DMZ (10.10.20.0/24)

VLAN 30: SCADA/HMI Sarea (10.10.30.0/24)

VLAN 40: PLC Kontrol Sarea (10.10.40.0/24)

VLAN 50: Eremuko Gailuak (10.10.50.0/24)

VLAN 99: Honeypot Sarea (172.16.99.0/24) - ISOLATUA

3. Firewall Arauen Laburpena (Firewall B - IT/OT muga):

Allow: Jump Host (DMZ) → SCADA (port 135 RDP, MFA beharrezko)

Allow: SIEM (DMZ) → PLC (port 102 S7Comm, irakurketa-soilik)

Allow: Historian (DMZ) ← SCADA (port 8088 InfluxDB idazketa)

Deny: VLAN IT → VLAN OT (trafiko zuzena)

Deny: VLAN OT → Internet (irteera guztia)

Alert: Modbus trafiko edozein VLAN 40/50-etatik kanpo

4. Diagrama Placeholder-ak:

- [DIAGRAMA A]: Topologia fisikoa (rack-ak, switch-ak, firewall-ak)
- [DIAGRAMA B]: Arkitektura logikoa VLAN
- [DIAGRAMA C]: Datu fluxu diagrama (SCADA → Historian → SIEM)

14. Sekzioa: OT Segurtasun Implementazioa (20-22 orrialdeak)

Helburua: OT implementazioaren xehetasun teknikoak

Edukia xehea: 1. **Aktiboen Inbentario Metodologia:** - **Tresnak:** Nmap 7.94, Nessus Industrial Edition, Claroty CTD - **Prozesua:** Pasiboko discovery (core switch span port-a), eskaner aktiboa (mantentze leihoa), eskuzko berrikuspena (ingeniaritza marrazkiak) - **Entregagarria:** Excel/CSV MAC, IP, vendor, firmware, kritikotasun puntuazioarekin

2. PLC Gotortze Prozedurak:

Siemens S7-1500:

- Desgaitu beharrezkoak ez diren zerbitzuak (FTP, HTTP zerbitzaria)
- Gaitu pasahitz babesia (sarbiak maila 3+ PLC)
- Konfiguratu IP sarbiak zerrendak (ingeniaritzako workstation whitelist)
- Desgaitu PUT/GET eragiketak baimendutako IP-eraketa salbu
- Gaitu audit log-ak (syslog → SIEM)
- Firmware eguneraketa: TIA Portal v18 → 2024ko ekaineko patak aplikatu

Allen-Bradley CompactLogix:

- Segurtasun modua "Enhanced"-era ezarri (CIP Security)
- Erabiltzaile kontuak sortu pribilegio minimokoekin
- Gaitu CIP Security TLS 1.2+ekoak
- Desgaitu HTTP/Telnet (HTTPS/SSH soilik erabili)
- Konfiguratu FactoryTalk Security politikak

3. Sare Segmentazioa:

- **Fisikoa:** IT/OT-rako switch bereiziak
- **Logikoa:** ACL-ak dituzten VLAN-ak
- **Firewall kokapena:** 3.5/3 eta 3/2 mailen artean
- **IDS/IPS:** Industria protokoloaren kontzientea (Claroty/Nozomi kokapena)

4. Jump Host Konfigurazioa:

Hardware: Zerbitzari espezializatua (Dell PowerEdge R250 edo baliokidea)

SO: Ubuntu 24.04 LTS Server (CIS benchmark-ekoan gotortua)

Sarbidea: OpenSSH MFA-ekoan (Google Authenticator/Duo)

Saio Grabazioa: Auditd + Teleport pantaila grabaziorako

Baimendutako Irteera: RDP → SCADA, S7Comm → PLC-ak (logeatuta)

Erabiltzaile kudeaketa: Active Directory-rekin LDAP integrazioa

5. ICS Protokolo Segurtasuna:

Modbus TCP (502 Portua):

- Firewall-ean pakete sakon inspezkioa
- SIEM-erak irakurketa-soilik funtzio kodeak (0x01-0x04)
- Idazteko komandoak (0x05, 0x06, 0x0F, 0x10) blokeatu ingeniaritzako IP-eraketa salbu

Profinet (Ethernet geruza):

- 802.1X segurtasuna switch-eten
- VLAN isolamendua ekoizpen gune bakotzea
- Siemens Scalance switch-ak NAT/firewall gaitasunekin

6. Babespenea & Disaster Recovery:

- PLC programak: Asteko babespena TIA Portal bidez (NAS-en enkriptatua biltegiratua)
- SCADA DB: Eguneko inkrementala, asteko osoa (atxikipena: 90 egun)
- Recovery Time Objective (RTO): 4h SCADA, 8h PLC-ak
- Recovery Point Objective (RPO): 24h gehienezko datu galera

15. Sekzioa: SIEM & SOC (Wazuh vs ELK) (23-25 orrialdeak)

Helburua: SIEM/SOC plataforma espezifikazioak

Edukia xehea: 1. Plataforma Konparaketa Matrizea:

Irizpidea	Wazuh (Gomendatua)	ELK Stack (Aukera)	AlienVault OSSIM
Kostua	€0 (kode irekia)	€0 (oinarria)	€0 (kode irekia)
OT/ICS Laguntza	Modbus/S7Comm parser-ak	Logstash plugin-ak beharrezkoak	OT mugatua
Eskalagarritasuna	10K+ agente	Bikaina (Elasticsearch)	1 nodo muga
Ikasketa Kurba	Ertaina	Altua	Ertaina
Komunitatea	Aktiboa	Oso aktiboa	Beherakorra
EDR Gaitasuna	Built-in	Add-on-ak beharrezkoak	EDR gabe
RBAC	Granularra	X-Pack-ekin (ordainduta)	Oinarrizkoa
Betetzea	PCI-DSS, GDPR txostenak	Pertsonalizatua	Pre-built

ERABAKIA: Wazuh OT laguntzagatik + sinpletasunagatik + EDR + kostua = €0 lizenziak

2. Log Iturrien Integrazioa (30 guztira):

IT Iturriak (15):

- Firewall-ak: FortiGate/Palo Alto (syslog UDP/514)
- Domeinu Kontrolatzaila: Windows Event Logs (Wazuh agentea)
- Web Zerbitzariak: Apache/Nginx access/error log-ak (Filebeat)
- Linux Zerbitzariak: auditd, syslog (Wazuh agentea)
- Email Gateway: Postfix log-ak (Filebeat)

OT Iturriak (10):

- Industria Firewall: Syslog (Claroty/Nozomi alertak)
- SCADA Zerbitzaria: Aplikazio log-ak + DB audit trail
- HMI Panelak: Saio hasiera gertaerak (syslog)
- PLC-ak: S7Comm log-ak OPC UA gateway bidez
- Jump Host: SSH saio log-ak + auditoretzak

Aplikazio Iturriak (5):

- HR Ataria: PHP aplikazio log-ak + PostgreSQL audit
- Autentikazioa: LDAP/AD saio hasiera gertaerak
- VPN Konzentratzailea: OpenVPN/IPSec log-ak
- Babespen Sistema: Veeam/Bacula job log-ak
- Honeypot-ak: T-Pot JSON log-ak (Cowrie, Conpot, Dionaea)

3. Alerta Arauak & Kasu Erabilera (50+ eszenario):

Kategoria: Autentikazioa (10 arau):

- Huts egindako login >5 5 minututan IP-tik → Alerta
- Saio hasiera arrakastatsua geolocation desberdinak → Alerta
- Saio hasiera negozio orduetatik kanpo (admin kontuak) → Alerta

- MFA saiakera saihestea → Alerta Kritikoa
- Kontu blokeoa aktibatua → Alerta

Kategoria: OT-Espezifikoak (15 arau):

- Modbus idazketa komando baimenik gabe → Alerta Kritikoa
- PLC firmware aldaketa detektatua → Alerta Kritikoa
- SCADA → PLC konexioa IP ezezagunetik → Alerta
- Modbus eskanerra detektatua (funtzio kode anitzak) → Alerta
- PLC CPU gelditze komandoa → Alerta Kritikoa
- HMI saio hasiera kreditzialetan lehenetsiak → Alerta

Kategoria: Malware (8 arau):

- Fitxategi osotasun monitorizazioa /bin, /sbin aldaketa → Alerta
- Prozesua PHP-tik sortua (webshell) → Alerta Kritikoa
- Ezagutzen den malware hash-a (VirusTotal API) → Alerta Kritikoa
- Mugimendu lateralua (PSEexec, WMI abusua) → Alerta

Kategoria: Datu Exfiltrazioa (7 arau):

- Irteera transferentzia handia (>1GB) → Alerta
- DB dump komandoa exekutatua → Alerta
- HR Atari langileen datu bulk export → Alerta
- USB gailua OT workstation-era konektatua → Alerta Kritikoa

4. Dashboard Diseinuak:

Panel Exekutiboa (CEO/CFO-rako):

- Segurtasun jarrera puntuazioa (1-100)
- Azken 7 egunetako alerta kritikoak (joera)
- Betetze egoera (implementatutako ISO 27001 kontrolen %)
- Top 5 mehatxu aktoreak (honeypot datuak)

Panel SOC Analistarentzat:

- Alerta ilara (lehentasunaren arabera ordenatua)
- Top erasotzaileak IP-ka (GeoIP mapa)
- Aktibo kritisitate heat map
- Gertaera erantzun workflow egoera

Panel OT Ingeniariarentzat:

- PLC osasun egoera (CPU, memoria, comm erroreak)
- SCADA uptime metrikak
- Sarbide saiakera baimenik gabeak (OT sarea)
- Protokolo anomaliak (Modbus/Profinet)

5. Mehatzu Inteligentzia Feed-ak:

- AlienVault OTX (mehatzu truke irekia)
- MISP (Malware Info Sharing Plataforma)
- ICS-CERT oharrak (US-CERT)
- Barne honeypot inteligentzia (eraso sinadurak)
- VirusTotal API (fitxategi hash ospea)

6. SOC Langileria Eredua:

Aukera A: SOC 8x5 (€20K/6 hilabete, aurrekontuan barne):

- Estaldura: A-L 8am-5pm
- Langileria: 1 L1 analista + 1 L2 (part-time estaldura)
- Eskalatzea: On-call ingeniarria alerta kritikoetarako

Aukera B: SOC 24x7 (+€60K/urte, Enpresarial paketea):

- Estaldura: 24h, 7 egun, 365 egun
- Langileria: 3 txanda x 2 analista = 6 FTE
- Eskalatzea: Gertaera erantzun talde espezializatua

16. Sekzioa: Honeypot Hedapen Arkitektura (26-27 orrialdeak)

Helburua: Honeypot-ak diseinatzeko teknika

Edukia xehea: 1. **T-Pot All-in-One Plataforma:** Hardware: Zerbitzari espezializatua (bare-metal edo VM) Specs: 8 vCPU, 16GB RAM, 500GB SSD SO: Debian 12 (T-Pot instalatzailaileak auto-konfiguratzen du) Barnean Honeypot-ak: - Cowrie: SSH/Telnet honeypot (22, 23 portuak) - Dionaea: Multi-protokoloa (SMB, FTP, MySQL, MSSQL) - Conpot: ICS/SCADA (Modbus, S7Comm, BACnet) - Honeytrap: Low-interaction (portu guztiak) - Glutton: TCP/UDP portu guztiak

2. ICS Honeypot-ak Conpot:

Txantiloia 1: Siemens S7-300 PLC

- Protokoloa: S7Comm (ISO-TSAP)
- Datu espostuak: Fake temperatura sentsoreak, motor egoerak
- Helburua: ICS eskaner automatizatuak detektatzea (Shodan, ZoomEye)

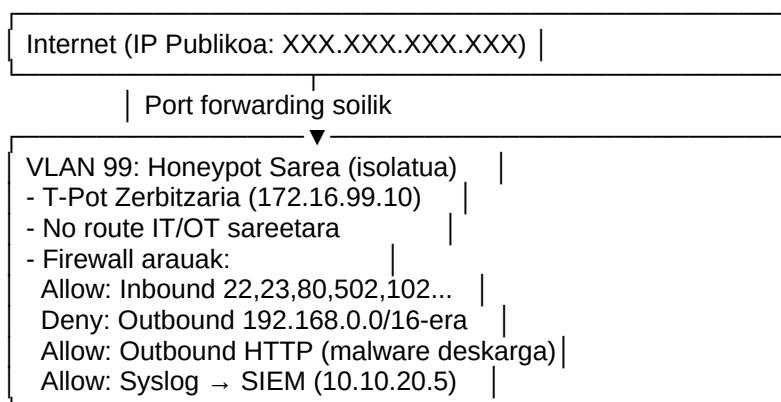
Txantiloia 2: Modbus RTU Gateway

- Protokoloa: Modbus TCP (502 portua)
- Erregistroak: 100 fake coils/holding registers
- Helburua: Modbus eskaner tresnak harrapatzea

Txantiloia 3: Guardian AST Tank Gauging

- Protokoloa: Guardian AST (10001 portua)
- Helburua: Oil/gas sektoreko erasotzaileak erakartzea

3. Sare Isolamendu Diseinua:



4. Datu Bilduma & Analisi Pipeline-a:

Honeypot Erasoa → ELK Stack T-Pot (Kibana panela)

↓
JSON Log-ak → Logstash → Wazuh SIEM (korrelazioa)

↓
 Mehatzu Inteligentzia → Firewall blocklists eguneratu
 ↓
 Malware laginak → VirusTotal Submission → IOC DB

5. SIEM Integrazioa:

- T-Pot-eko Logstash forwarder-a → Wazuh manager
- Alerta: SSH brute force ereduak, Modbus idazteko saiakerak, malware deskarga
- Aberastea: GeoIP (erasotzailearen kokapena), ASN (hosting hornitzalea), ospea (VirusTotal)

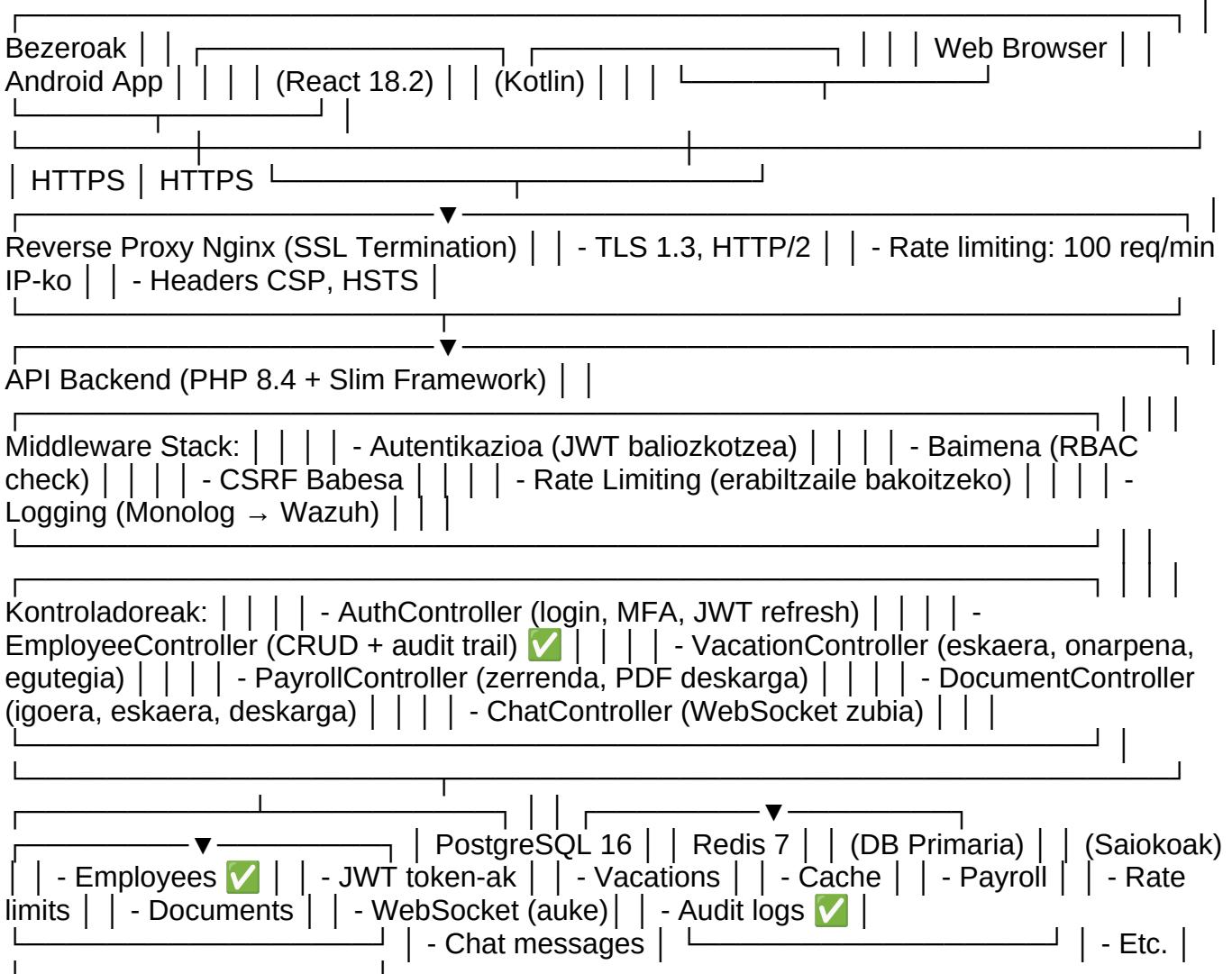
6. Legezko eta Etika Konsiderazioak:

- **Jakinarazpena:** Honeypot-aren existentzia EZ da argitaratzen (Euskal Herrian segurtasun ikerketarako legala)
- **Datu atxikipena:** Eraso log-ak 90 egunetan mantentzen dira (GDPR Art. 6(1)(f) interes legitimoa)
- **Malware kudeaketa:** Sandbox-ed analisia soilik, ez birbanaketa
- **Zuzenbidearen betearazpena:** INCIBE-rekin koordinatu mehatxu esanguratsuak

17. Sekzioa: HR Atari Espezifikazio Teknikoak (28-31 orrialdeak)

Helburua: HR atariaren xehetasun teknikoak

Edukia xehea: 1. Sistema Arkitektura:



2. Datu-base Eskeema (migrations/001_init_schema.sql-tik):

Taula Nagusiak (7 3. Fasea + 15+ planifikatuak):

- users (autentikazioa, MFA, rolak) - ✓ Osoa
- employees (profil datuak, NIF, IBAN, kontaktua) - ✓ Osoa
- departments (jerarkia, manager esleipena)
- vacations (eskaerak, onarpenak, balantzea) - Eskeema prest
- documents (fitxategi metadatuak, upload jarraipena)
- payroll (soldata kalkuluak, dedukzioak, ordainketa garbia)
- complaints (kanal anonimoa whistleblower-rako)
- chat_messages (denbora errealeko mezularitza)
- audit_logs (aldaketa jarraipen ez-aldaezina) - ✓ Osoa
- notifications (alertak, oroigarriak)

Eskeema Laburpena:

```
CREATE TABLE employees (
    id UUID PRIMARY KEY DEFAULT uuid_generate_v4(),
    user_id UUID REFERENCES users(id),
    employee_number VARCHAR(20) UNIQUE NOT NULL,
    first_name VARCHAR(100) NOT NULL,
    last_name VARCHAR(100) NOT NULL,
    nif_nie VARCHAR(10) UNIQUE NOT NULL, -- Checksum-ekin baliozkotua
    iban VARCHAR(24), -- mod-97-ekin baliozkotua
    phone VARCHAR(15), -- Spainiako formatua +34XXXXXXXXX
    hire_date DATE NOT NULL,
    department_id UUID REFERENCES departments(id),
    position VARCHAR(100),
    is_active BOOLEAN DEFAULT TRUE,
    created_at TIMESTAMP DEFAULT NOW(),
    updated_at TIMESTAMP DEFAULT NOW()
);
```

3. API Endpoint Dokumentazioa:

Autentikazioa (3 endpoint):

```
POST /api/auth/login
Body: { "email": "user@zabala.eus", "password": "...", "mfa_code": "123456" }
Response: { "token": "JWT...", "refresh_token": "...", "user": {...} }
```

```
POST /api/auth/refresh
Body: { "refresh_token": "..." }
Response: { "token": "new_JWT..." }
```

```
POST /api/auth/logout
Headers: Authorization: Bearer {token}
Response: 204 No Content
```

Langileak (8 endpoint) - ✓ 3. FASEAN OSATUA:

GET /api/employees	→ Zerrenda (orrikatua, 10/orria)
GET /api/employees/{id}	→ Xehetasuna auditoria historialarekin
POST /api/employees	→ Sortu (RBAC: admin, hr_manager)
PUT /api/employees/{id}	→ Eguneratu (audit log-ekin)
DELETE /api/employees/{id}	→ Soft delete (is_active=false)
POST /api/employees/{id}/restore	→ Ezabatutako langilea berreskuratu
GET /api/employees/{id}/history	→ Audit trail (denbora-lerroa)
GET /api/audit/user/{userId}	→ Erabiltzaile jarduera log-a

Oporrak (6 endpoint) - ⏳ PLANIFIKATUA:

```
GET /api/vacations      → Zerrenda (egoera, urtea filtratu)
```

```
GET /api/vacations/{id}           → Xehetasuna  
POST /api/vacations            → Opor eskaera  
PUT /api/vacations/{id}/approve → Onartu (RBAC: manager+)  
PUT /api/vacations/{id}/reject  → Baztertu arrazoairekin  
GET /api/vacations/calendar/{year} → Egutegi ikuspegia
```

Nóminak (3 endpoint) - PLANIFIKATUA:

```
GET /api/payroll                → Nire nóminak zerrendatu (edo guztiak hr_manager bada)  
GET /api/payroll/{id}           → Xehetasuna  
GET /api/payroll/{id}/download → PDF deskarga
```

4. Segurtasun Kontrolak:

Autentikazioa:

- JWT access token-ak: 1 ordu iraungitzea
- Refresh token-ak: 7 egun iraungitzea, Redis-en biltegiratua
- MFA/TOTP: Google Authenticator bateragarria (30 segunduko kodeak)
- Pasahitz politika: 8+ karaktere, maiuskula, minuskula, zenbaki, karaktere berezi

Baimena (RBAC):

Rolak:

```
- admin:      43 baimen (sarbide osoa)  
- hr_manager: 31 baimen (HR eragiketak)  
- department_head: 15 baimen (nire taldea)  
- employee:   7 baimen (auto-zerbitzua)
```

Baimen check adibidea:

```
if (!$user->hasPermission('employees.create')) {  
    return $response->withStatus(403);  
}
```

Sarrera Baliozkotzea (3. Fasetik):

- NIF/NIE: Spainiako ID checksum-ekin baliozkotzea
- IBAN: mod-97 checksum baliozkotzea
- Telefonoa: Spainiako formatua +34XXXXXXXXX (9 digitu)
- Posta kodea: 00000-52999 tartea
- Email: RFC5322 betetzen du
- XSS garbiketa: DOMPurify (bezero-aldera), htmlspecialchars() (zerbitzari-aldera)

Datu-base Babesa:

- PDO prepared statements (SQL injekzio prebentzia)
- Soft deletes (langileen ezabaketa fisikoa gabe)
- Audit trail (CUD eragiketa guztiak logeatuta user_id, timestamp, JSON aldaketak)

5. Modulu Espezifikazioak:

Langileen Modulua (3. Fasea - OSATUA):

- Kode lerroak: ~5,500 (backend + web + mugikorra)
- Probak: 82/82 pasatzen (PHPUnit)
- Ezaugarriak: CRUD, baliozkotzea, audit trail, orrikatzea, soft delete, berresprena

Nóminal Modulua (Planifikatua - 5. Fasea):

- Kalkulu motorra: Oinarritzko soldata + ordu gehigarri + bonus-ak - dedukzioak - zergak

- Zerga atxikipena: 2024ko Spainiako IRPF taulak
- Gizarte segurtasuna: Kalkulu automatikoa (enpresa + langile ekarpenak)
- PDF sortzea: TCPDF liburutegia nómina txantiloi ofizialarekin
- Estimatutako LOC: ~3,000

Opor Modulua (Planifikatua - 4. Fasea):

- Urteko balantze kalkulua: 22 egun lanegun/urte (Spainiako legea)
- Eskaera workflow-a: Langilea → Manager → HR (aukerakoa)
- Egutegi integrazioa: iCal export Google Calendar/Outlook-erako
- Gatazka detekzioa: Saihestu opor gainjartzeak departamentu berean
- Estimatutako LOC: ~2,500

Dokumentu Modulua (Planifikatua - 6. Fasea):

- Fitxategi biltegiratzea: Egonkorrean enkriptatua (AES-256), employee_id-ka antolatua
- Onartutako motak: PDF, JPG, PNG (gehienetarikoa 10MB fitxategiko)
- Dokumentu eskaerak: HR → Langilea (adib. “Eguneratutako NIF eskaneatua igo”)
- Sarbide kontrola: Langileek beren dokumentuak soilik ikusten dituzte, HR-ak guztiak ikusten ditu
- Estimatutako LOC: ~2,000

Txat Modulua (Planifikatua - 7. Fasea):

- Denbora errealean: WebSocket Ratchet PHP liburutegiaren bidez
- Kanalak: HR Txata (1-on-1 HR sailarekin), Sail Txata (taldea)
- Mezu motak: Testua, emoji, fitxategi eranskinak
- Atxikipena: 90 egun (GDPR datu minimizazioa)
- Estimatutako LOC: ~3,500

Kexa Modulua (Planifikatua - 8. Fasea):

- Anonimatoa: Aukerako aurkezpen anonimoa (GDPR Art. 88 betetzea)
- Kategoriak: Jazarpena, diskriminazioa, segurtasuna, etika
- Workflow-a: Ireki → Prozesuan → Konponduta → Itxita
- Sarbidea: HR Manager + Admin soilik
- Estimatutako LOC: ~1,500

6. Hedapen Arkitektura:

Docker Compose Stack:

services:

```
nginx:
  image: nginx:alpine
  ports: 8080:80, 8443:443
  volumes: SSL Ziurtagiriak, nginx.conf
```

```
php:
  image: php:8.4-fpm-alpine
  volumes: /app/src
  depends_on: postgres, redis
```

```
postgres:
  image: postgres:16-alpine
  volumes: /var/lib/postgresql/data
  healthcheck: pg_isready
```

```
redis:
  image: redis:7-alpine
  healthcheck: redis-cli ping
```

Hosting:

- On-premise: 3x Dell PowerEdge R250 zerbitzari (nginx, php, postgres)
- Cloud aukera: AWS (EC2 t3.medium x3 + RDS PostgreSQL + ElastiCache Redis)

7. Babespen & DR Estrategia:

- PostgreSQL: Eguneko babespen osoa + WAL artxibatze jarraitua (PITR gaitasuna)
- Atxikipena: 30 egun on-site, 90 egun off-site (enkriptatua S3/Azure Blob)
- Dokumentu upload-ak: Eguneko rsync NAS-era + asteko zinta babespena
- RTO: 2 ordu (standby zerbitzaritik babespena berresprena)
- RPO: 15 minutu (WAL bidalketa tarte)

18. Sekzioa: Betetze Mapeoa (ISO/IEC/GDPR) (32-34 orrialdeak)

Helburua: Nola betetzen ditu proiektuak eskakizunak

Edukia xehea: 1. ISO 27001:2022 Kontrolen Implementazioa:

Kontrola	Izenburua	Implementazioa	Egoera
A.5.1	Informazio segurtasun politikak	SGSI politikak dokumentatuta	Egina
A.8.1	Aktiboen inventarioa	OT aktiboen DB (machinery_inventory.md)	Aurrerapenak
A.8.9	Konfigurazio kudeaketa	PLC gotortze prozedurak, aldaketa kontrolak	1. Fasea
A.12.4	Log-ak eta monitorizazioa	SIEM zentralizatua (Wazuh)	2. Fasea
A.13.1	Sare segurtasuna	Purdue segmentazioa, firewall-ak	1. Fasea
A.14.2	Garapenean segurtasuna	HR Ataria: SDLC segurua, kode berrikuspena, probak	3. Fasea
A.17.1	Negozio jarraitutasuna	SCADA-rako DR plana, babespen prozedurak	1. Fasea
A.18.1	Legezko eskakizunen betetzea	GDPR, LOPD-GDD, lan legea	Aurrerapenak

Gap Analisi Laburpena: - Annex A kontrol totala: 93 - Oraingoz implementatuak: 28 (%30) - Implementazio planifikatua (proiektu hau): +45 (%48 → %78) - Geratzen direnak (proiektu ostean): 20 (ekintza bereziak behar dituzte)

2. IEC 62443 Segurtasun Mailak:

Oraingo Egoera Ebaluazioa: SL0 (segurtasun neurririk gabe)

Helburu Egoera: SL2 (asmo oneko haustea metodo simpleekiko babesra)

Oinarrizko Eskakizuna	SL2 Eskakizunak	Implementazioa
FR1: Identifikazioa & Auth	Erabiltzaile kontuak, pasahitz	Jump host, LDAP, MFA

Oinarrizko Eskakizuna

SL2 Eskakizunak

Implementazioa

FR2: Erabilera Kontrola

politika, MFA

FR3: Sistema Osotasuna

Rol bidezko sarbidea, pribilegio SCADA-rako RBAC, PLC sarbide minimoa

zerrendak

FR4: Datu Konfidentzialtasuna

Software whitelist, aldaketa detekzioa

Fitxategi osotasun monitorizazioa (Wazuh FIM)

FR5: Datu Fluxu Murritzua

Sare segmentazioa, firewall-ak

Purdue Modeloa, VLAN-ak, firewall arauak

FR6: Erantzun Goiztiarra

Gertaera log-ak, alertak

OT espezifiko alertak dituen SIEM

FR7: Baliabide Eskuragarritasuna

Aniztasuna, babespena

SCADA failover, eguneko babespenak

SL3 Konsiderazioak (etorkizuneko hobekuntza):

- Autentikazio aurreratua (biometriak, txartel adimendunak)
- Gailu eremu mailan enkriptatzea (unean ez dute gailu guztiekin onartzen)
- Estimatutako kostu gehigarria: +€80K

3. GDPR Betetzea:

32. Artikula: Prozesamendu Segurtasuna:

- ✓ Enkriptatzea: HTTPS, DB at-rest enkriptatzea (pgcrypto)
- ✓ Pseudonimizazioa: Langile ID-ak (UUID-ak), aukerako kexa anonimoa
- ✓ Konfidentzialtasuna: RBAC, beharrezkoan oinarritutako sarbidea
- ✓ Osotasuna: Audit trail, log ez-aldaezinak
- ✓ Eskuragarritasuna: Eguneko babespenak, %99 uptime SLA
- ✓ Probak: Penetrazio probak (urterokoa), DR drill-ak (erdi-urterokoa)

33. Artikula: Gertaera Jakinarazpena:

- SIEM alertak datu exfiltrazio saiakeretarako konfiguratuta
- Gertaera erantzun plana (compliance/gdpr/data_breach_notification_template.md txantiloia)
- 72 orduko erlojua detekzioan hasten da

35. Artikula: Datu Babesaren Inpaktu Ebaluazioa (DPIA):

- HR Atariaren DPIA osatua (compliance/gdpr/dpia_template.md txantiloia)
- Arrisku handiko prozesamendua: Langileen datu pertsonalak, nómina (finantza sensiblea)
- Murrizketa: Enkriptatzea, sarbide kontrola, audit log-ak

88. Artikula: Langileen Datu Babesa:

- HR Atariaren betetze espezifikoak:
 - Prozesamendu gardena (pribatasun oharra lehen saio-hasieran erakusten da)

- Datu minimizazioa (beharrezko eremuak soilik bildu)
- Atxikipen egitaraua (langileak: kontratua amaitu eta 10 urtera, nómima: 6 urte)
- Kexa kanal anonimoa (whistleblower-ak babesten ditu)

4. NIS2 Zuzentaraaua Eskakizunak:

Esparrua: Zabala Gailetak “**entitate funtsezkoa**” gisa kualifikatzen da (elikadura ekoizpena, >50 langile)

Oinarritzko Betebeharrak:

- Arrisku kudeaketa neurriak (proiektu honek ebaluazio integrala implemetatzen du)
- Gertaera kudeaketa (SIEM + SOC + gertaera erantzun plana)
- Negozio jarraitutasuna (SCADA-rako DR, babespen prozedurak)
- Hornidura kate segurtasuna (PLC/SCADA hornitzairen ebaluazioa)
- Segurtasun prestakuntza (120 ordu langile guztiaren planifikatua)
- Kriptografiaren erabilera (TLS, SSH, babespen enkriptatuak)
- Ahultasun kudeaketa (Nessus eskanerak hilero)

Betetze Ezaren Zigorak: €10M arte edo mundu mailako fakturazioaren %2 **Betearazpen Data:** 2024ko urriaren 17a (Espainiako transposizioa 2024ko abendua)

19. Sekzioa: Implementazio Plano Xehea (35-36 orrialdeak)

Helburua: Dependentziak dituzten egitarau xehea

Edukia xehea: 1. **10 Hilabete Egitaraua** (8 fasea: Discovery → Go-live → Laguntza) - **1. Fasea (1-2.**

Hilabeteak: Discovery & Plangintza - OT aktiboen inventario osoa - Arkitektura diseinua (Purdue Modeloa) - Arrisku ebaluazioa eta gap analisia - HR Atari 1. Fasea (oinarria)

- **2. Fasea (2-4. Hilabeteak):** Oinarri Konfigurazioa
 - SIEM desplieguea eta log iturrien integrazioa
 - Sare segmentazioa (firewall-ak, VLAN-ak)
 - Jump host konfigurazioa eta MFA implementazioa
 - HR Atari 2. Fasea (auth + CRUD oinarrizko)
- **3. Fasea (4-6. Hilabeteak):** OT Segurtasun Implementazioa
 - PLC gotortze prozedurak
 - Honeypot desplieguea
 - SOC konfigurazioa eta alerta doikuntza
 - HR Atari 3. Fasea (langile CRUD osoa)
- **4. Fasea (6-8. Hilabeteak):** Aplikazio Garapena
 - HR Atari 4. Fasea (oporen modulu)
 - HR Atari 5. Fasea (nómima modulu)
 - IT/OT integracio proba
 - Erabiltzaile onarpen proba
- **5. Fasea (8-9. Hilabeteak):** Probak eta Gotortzea
 - Penetrazio probak
 - Errendimendu probak
 - Segurtasun probak (ISO/IEC betetzea)
 - Prestakuntza entrega
- **6. Fasea (9-10. Hilabeteak):** Hedapena eta Go-live
 - Produkzio desplieguea
 - Datu migrazioa
 - Parallel run (beharrezko bada)
 - Go-live laguntza
- **7. Fasea (10-12. Hilabeteak):** Go-live Osteko Laguntza
 - 2 hilabeteko bermea

- SOC monitorizazioa
 - Gertaera erantzuna
 - Errendimendu optimizazioa
 - **8. Fasea (12+ Hilabeteak):** Etengabeko Eragiketak
 - Hiruhileko segurtasun auditoretza
 - Urteroko penetrazio probak
 - SOC zerbitzuak (kontratatuta badago)
 - HR Atari mantentze eguneraketak
2. **Gantt Diagramma** (placeholder dependentziekin)
- **Hito 1 (2. Hilabetea):** Oinarri azpiegitura osoa
 - **Hito 2 (4. Hilabetea):** OT Segurtasuna implementatua