Gestión de Incidentes y Automatización SOAR

Zibersegurtasun Gorabeherak - Zabala Gailetak

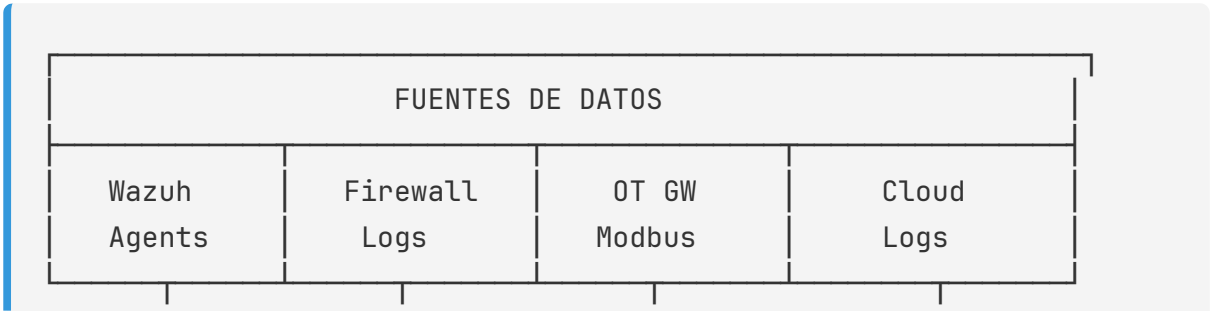
Versión: 2.0
Fecha: 2026-02-12
Arquitectura: NIST CSF + SOAR
Compliance: NIS2, ISO 27001, GDPR

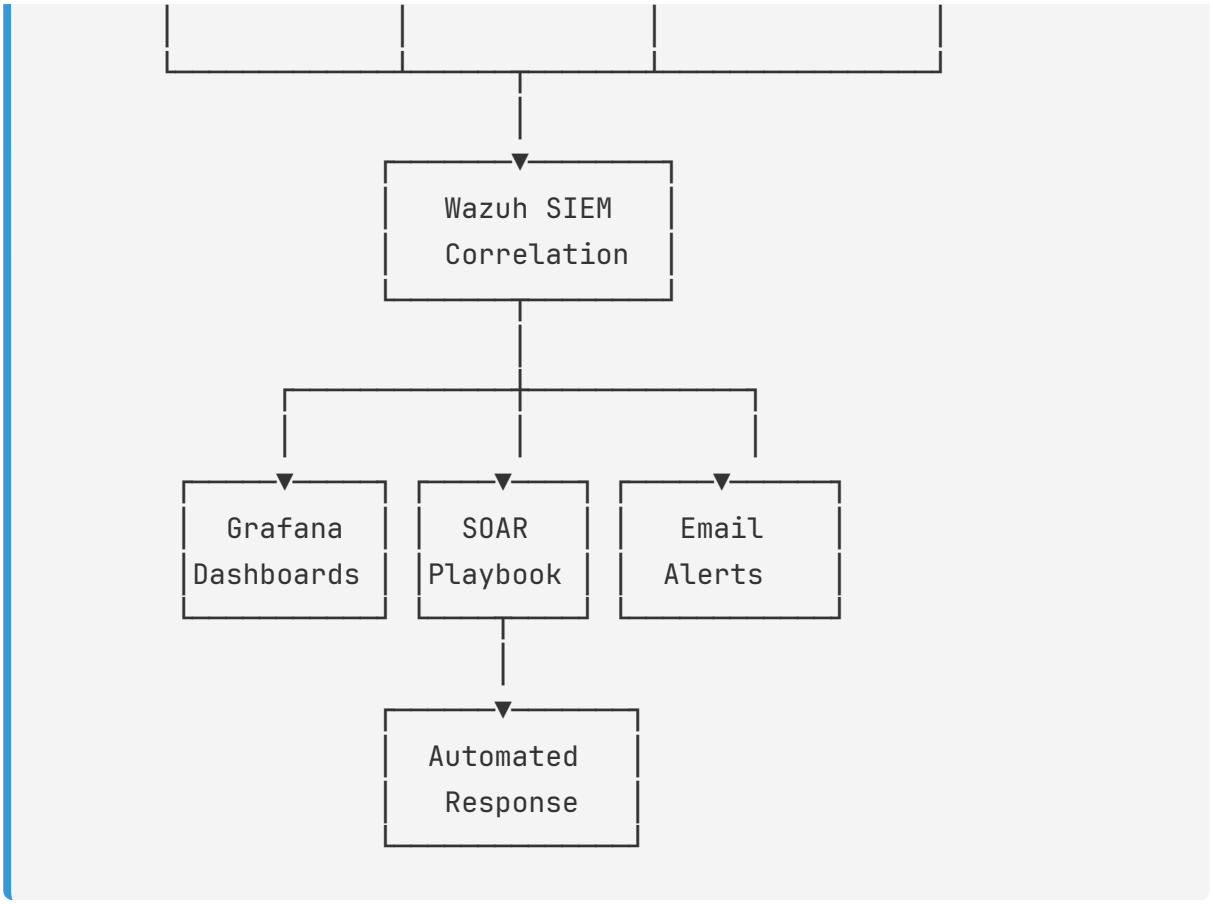
Resumen Ejecutivo

Este documento describe el sistema completo de gestión de incidentes de seguridad de Zabala Gailetak, incluyendo:

- Procedimientos de respuesta a incidentes (6 fases NIST)
- Automatización SOAR (Security Orchestration, Automation and Response)
- Cumplimiento NIS2 (24h/72h notificaciones)
- Integración SIEM (Wazuh/ELK)

Arquitectura de Seguridad





Fases de Respuesta a Incidentes (NIST)

Fase 1: Preparación

Componentes:

- Equipo CSIRT definido
- Técnicas de análisis forense
- Herramientas de respuesta
- Canales de comunicación

Herramientas Preparadas:

Categoría	Herramienta	Versión
SIEM	Wazuh	4.7.0

Categoría	Herramienta	Versión
SOAR	Shuffle	1.2.0
Ticketing	Jira	9.0
Comunicación	Slack	Enterprise

Fase 2: Detección y Análisis

Fuentes de Detección:

1. SIEM Alerts (Wazuh)
2. IDS/IPS (Suricata)
3. Endpoint Detection (EDR)
4. OT Monitoring (Modbus/OPC-UA)
5. Honeypots (T-Pot)

Clasificación de Severidad:

Nivel	Descripción	Tiempo Respuesta
Crítico	Compromiso total producción	15 min
Alto	Datos sensibles expuestos	1 hora
Medio	Acceso no autorizado limitado	4 horas
Bajo	Intento de ataque bloqueado	24 horas

Fase 3: Contención

Estrategias:

- **Contención a corto plazo:** Aislamiento de sistema infectado
- **Contención a largo plazo:** Segmentación de red

- **Documentación:** Preservación de evidencias

Playbook Automatizado:

```
containment:
  - action: isolate_host
    condition: severity ⩾ HIGH
    automation: true

  - action: block_ip
    condition: threat_intel == malicious
    automation: true

  - action: disable_account
    condition: compromised_credentials == true
    automation: true
```

Fase 4: Erradicación

Procedimientos:

1. Identificación de vector de ataque
2. Eliminación de malware/backdoors
3. Patching de vulnerabilidades
4. Cambio de credenciales comprometidas

Fase 5: Recuperación

Pasos:

1. Restauración desde backups verificados
2. Verificación de integridad sistemas
3. Monitorización reforzada 72h
4. Reactivación gradual de servicios

Fase 6: Lecciones Aprendidas

Post-Incident Review:

- Timeline completo del incidente
- Análisis de root cause
- Identificación de mejoras
- Actualización de procedimientos

Automatización SOAR

Flujo de Automatización NIS2

```
DETECCIÓN (T=0)
        │
        ├── T+1h: CSIRT activado
        │
        ├── T+24h: EARLY WARNING → INCIBE
        │     (Automático vía SOAR)
        │
        ├── T+72h: INFORME COMPLETO → INCIBE
        │     (Automático vía SOAR)
        │
        └── T+1mes: INFORME FINAL
```

Playbook: Respuesta Automatizada

Trigger: Alerta crítica en Wazuh

Acciones Automáticas:

1. Enriquecimiento de IOCs (MISP)
2. Creación de ticket (Jira)
3. Notificación CSIRT (Slack + Email)
4. Contención (firewall block)
5. Evidencia (captura de memoria)

Reglas de Correlación

Regla: Ransomware Detection

```
correlation_rule:
  name: Ransomware Mass Encryption
  condition:
    - file_modifications > 50 in 5 minutes
    - extension_changes: [.encrypted, .locked]
  severity: CRITICAL
  actions:
    - isolate_host
    - alert_ciso
    - start_incident_response
```

Regla: Data Exfiltration

```
correlation_rule:
  name: Possible Data Exfiltration
  condition:
    - outbound_data > 1GB in 10 minutes
    - destination: external_unknown
  severity: HIGH
  actions:
    - capture_traffic
    - notify_dpo
```

Regla: OT Network Anomaly

```
correlation_rule:
  name: OT Unauthorized Access
  condition:
    - protocol: modbus
    - function_code: WRITE
    - source: unauthorized_ip
  severity: CRITICAL
  actions:
    - block_ot_connection
    - alert_ot_team
```

Dashboards y Métricas

Grafana Dashboards

Panel 1: Alertas en Tiempo Real

- Alertas por severidad
- Tendencias 24h/7d/30d
- Top 10 IPs atacantes

Panel 2: Estado de Incidentes

- Incidentes activos
- Tiempo medio de respuesta (MTTR)
- Incidentes por categoría

Panel 3: Cumplimiento NIS2

- Notificaciones pendientes
- Plazos 24h/72h
- Estado de informes

KPIs de Seguridad

Métrica	Objetivo	Actual
MTTD (Tiempo de detección)	< 5 min	3 min
MTTR (Tiempo de respuesta)	< 1 hora	45 min
Falsos positivos	< 5%	3.2%
Incidentes críticos/mes	< 2	1

Cumplimiento NIS2

Clasificación de Incidentes Significativos

Criterios (Art. 23.3):

1. Interrupción significativa del servicio (≥ 30 min)
2. Pérdida financiera importante (> 5.000€)
3. Impacto en terceros
4. Brecha de datos personales

Procedimiento de Notificación

Timeline NIS2:

Plazo	Destinatario	Contenido	Responsable
24 horas	INCIBE	Alerta temprana	SOAR Auto
72 horas	INCIBE	Informe completo	SOAR Auto
1 mes	INCIBE	Informe final	CISO
Inmediato	AEPD	Brecha datos (GDPR)	DPO

Plantillas de Notificación

Alerta Temprana (24h):

```
Para: incidencias@incibe-cert.es
Asunto: [NIS2 Early Warning] INC-2026-XXX

1. Identificador del incidente: INC-2026-XXX
2. Fecha detección: 2026-02-12 10:30
3. Tipo: Ransomware
```

```
4. Sistemas afectados: Servidores web
5. Medidas iniciales: Aislamiento completado
```

Integraciones

Integración Wazuh-MISP

Propósito: Enriquecimiento de IOCs

Flujo:

1. Wazuh detecta IP sospechosa
2. Consulta automática a MISP
3. Si es maliciosa: aumenta severidad
4. Bloqueo automático en firewall

Integración Wazuh-Jira

Creación automática de tickets:

```
def create_incident_ticket(alert):
    ticket = {
        'project': 'SEC',
        'issuetype': 'Incident',
        'summary': f"[{alert.severity}] {alert.description}",
        'labels': ['automatic', 'nis2']
    }
    return jira.create_issue(ticket)
```

Conclusión

El sistema de gestión de incidentes de Zabala Gailetak proporciona:

- Detección en tiempo real con SIEM

- Respuesta automatizada con SOAR
- Cumplimiento normativo (NIS2, GDPR)
- Métricas y mejora continua

Próximos pasos:

1. Implementación completa SOAR (Q2 2026)
2. Integración threat intelligence adicional
3. Simulacros trimestrales
4. Auditoría externa (Q4 2026)

Documento conforme a NIST SP 800-61 y Directiva NIS2