

# NIS2 SOAR Playbook-ak / Automated Response Playbooks

---

## NIS2 Art. 21.2.b, Art. 23 — Incident Handling & Notification

---

**Dokumentu Kodea:** NIS2-SOAR-001

**Bertsioa:** 1.0

**Data:** 2026-02-06

**Jabea:** CISO + SOC

---

### 1. SARRERA

---

Dokumentu honek SOAR (Security Orchestration, Automation and Response) playbook-ak definitzen

ditu NIS2 Direktibarekin lotutako segurtasun intzidentziei automatikoki erantzuteko.

Playbook hauek SIEM (Wazuh/ELK) alerta arau espezifikoekin loturik daude (nis2\_correlation\_rules.json).

---

### 2. PLAYBOOK KATALOGOA

---

#### PB-NIS2-001: Datu Ihesa / Data Breach Response

**Trigger:** nis2-inc-001 (Data Breach Detected)

**Larritasuna:** KRITIKOA

**NIS2 Artikulua:** Art. 23.3, Art. 23.4

#### Urrats Automatikoak (Automated Steps)

```
playbook: PB-NIS2-001
name: "NIS2 Data Breach Response"
trigger: nis2-inc-001
severity: critical

steps:
  - id: 1
    action: create_incident_ticket
```

```

params:
  type: NIS2_SIGNIFICANT
  severity: critical
  assign_to: ciso
  title: "[NIS2] Data Breach Detected - ${alert.source}"

- id: 2
  action: start_timer
  params:
    timer_name: nis2_24h_early_warning
    duration: 24h
    escalation_at: 20h

- id: 3
  action: start_timer
  params:
    timer_name: nis2_72h_full_report
    duration: 72h
    escalation_at: 64h

- id: 4
  action: collect_evidence
  params:
    - capture_siem_logs: last_48h
    - capture_affected_system_state: true
    - preserve_network_flows: true
    - screenshot_dashboards: true
    destination: compliance/nis2/evidence-pack/INC-${incident.id}/

- id: 5
  action: notify_csirt
  params:
    channels: [phone, signal, email]
    recipients: [ciso, dpo, it_lead, legal]
    priority: emergency
    message: >
      🚨 NIS2 SIGNIFICANT INCIDENT: Data breach detected.
      System: ${alert.source}
      Time: ${alert.timestamp}
      NIS2 24h timer started. War room activation required.

- id: 6
  action: prepare_notification_draft
  params:
    template: notifications/early_warning_24h_template.md
    auto_fill:
      incident_id: ${incident.id}
      detection_time: ${alert.timestamp}
      incident_type: "Datu ihesa"
      severity: "KRITIKOA"
      affected_systems: ${alert.affected_systems}
    save_to: evidence-pack/INC-${incident.id}/early_warning_draft.md

```

```
- id: 7
  action: containment_assessment
  params:
    check_data_scope: true
    check_gdpr_applicability: true
    if_gdpr: trigger_gdpr_breach_workflow
```

### Urrats Manualak (Manual Steps — Human Required)

#	Ekintza	Arduraduna	Epemuga
M1	War Room aktibatu eta bilakaera ebaluatu	CISO	≤ 1h
M2	Early Warning txantiloia berrikusi eta osatu	CISO + DPO	≤ 20h
M3	Early Warning bidali INCIBE-CERT-era	CISO	≤ 24h
M4	GDPR Art.33 jakinarazpena AEPD-ra (beharrezkoa bada)	DPO	≤ 72h
M5	Full Report txantiloia osatu	CISO + IT Lead	≤ 68h
M6	Full Report bidali INCIBE-CERT-era	CISO	≤ 72h

## PB-NIS2-002: Ransomware Response

**Trigger:** nis2-inc-002 (Ransomware Detected)

**Larritasuna:** KRITIKOA

**NIS2 Artikulua:** Art. 23.3

```
playbook: PB-NIS2-002
name: "NIS2 Ransomware Response"
trigger: nis2-inc-002
severity: critical

steps:
  - id: 1
    action: auto_isolate_host
    params:
      method: edr_network_isolation
      fallback: firewall_block
      preserve_evidence: true

  - id: 2
    action: disable_compromised_accounts
    params:
      scope: affected_users
      force_password_reset: true
```

```

    revoke_active_sessions: true

- id: 3
  action: create_incident_ticket
  params:
    type: NIS2_SIGNIFICANT
    severity: critical
    assign_to: ciso

- id: 4
  action: start_nis2_timers
  params:
    early_warning: 24h
    full_report: 72h

- id: 5
  action: capture_forensic_evidence
  params:
    - ram_dump: true
    - disk_image: true
    - network_pcap: last_24h
    - malware_sample: quarantine_and_hash
  destination: evidence-pack/INC-`${incident.id}/

- id: 6
  action: threat_intel_enrichment
  params:
    check_iocs: [file_hashes, c2_domains, ransomware_family]
    sources: [virustotal, abuse_ch, misp]

- id: 7
  action: notify_csirt_emergency
  params:
    message: "🚨 RANSOMWARE: Host `${alert.hostname}` isolated. CSIRT activation requ

- id: 8
  action: check_backup_integrity
  params:
    verify_last_clean_backup: true
    test_restore_capability: true

- id: 9
  action: prepare_notification_draft
  params:
    template: notifications/early_warning_24h_template.md
    auto_fill:
      incident_type: "Ransomware"

```

## Urrats Manualak

#	Ekintza	Arduraduna	Epemuga
M1	Ordainketa EZ egin — Politika korporatiboa bete	CEO + CISO	Berehala
M2	Ransomware familia identifikatu (No More Ransom kontsultatu)	Security	≤ 4h
M3	Babeskopietatik berrezarri (backup garbia baieztatu ondoren)	IT Lead	≤ RTO
M4	Early Warning INCIBE-CERT-era	CISO	≤ 24h
M5	Full Report INCIBE-CERT-era	CISO	≤ 72h

**PB-NIS2-003: OT/SCADA Compromise Response**

**Trigger:** nis2-inc-003 (OT/SCADA Compromise)

**Larritasuna:** KRITIKOA

**NIS2 + IEC 62443 Artikuluak:** Art. 23.3, SR 5.1

```
playbook: PB-NIS2-003
name: "NIS2 OT/SCADA Incident Response"
trigger: nis2-inc-003
severity: critical

steps:
  - id: 1
    action: activate_ot_isolation
    params:
      block_it_ot_gateway: true
      method: firewall_rule_override
      preserve_ot_operations: true # Safety first

  - id: 2
    action: alert_plant_operators
    params:
      method: [phone, physical_alarm]
      message: "⚠️ OT segurtasun alerta. Manual mode-ra pasatu prozesu kritikoak."

  - id: 3
    action: create_incident_ticket
    params:
      type: NIS2_SIGNIFICANT_OT
      severity: critical
      assign_to: [ciso, ot_specialist]
      tags: [iec62443, ot_safety]

  - id: 4
    action: start_nis2_timers
    params:
      early_warning: 24h
```

```
    full_report: 72h

- id: 5
  action: capture_ot_evidence
  params:
    - plc_state_snapshot: true
    - hmi_screenshots: true
    - modbus_traffic_capture: true
    - historian_data_export: last_24h
  destination: evidence-pack/INC-`${incident.id}/ot/

- id: 6
  action: notify_csirt_emergency
  params:
    include_ot_specialist: true
    message: "🚨 OT/SCADA COMPROMISE: IT-OT gateway blocked. Plant ops notified."
```

---

## PB-NIS2-004: DDoS Response

**Trigger:** nis2-inc-004 (DDoS Service Disruption)

```
playbook: PB-NIS2-004
name: "NIS2 DDoS Response"
trigger: nis2-inc-004
severity: high

steps:
- id: 1
  action: enable_ddos_mitigation
  params:
    cloudflare_under_attack_mode: true
    rate_limiting_strict: true
    geo_blocking: optional

- id: 2
  action: monitor_service_availability
  params:
    check_interval: 1m
    services: [web, api, email]
    threshold_recovery: 95%

- id: 3
  action: assess_nis2_significance
  params:
    criteria:
      - service_downtime_exceeds: 30m
      - affected_users_exceed: 100
      - financial_impact_exceeds: 5000
    if_significant: start_nis2_timers
```

```
- id: 4
  action: create_incident_ticket
  params:
    type: NIS2_SIGNIFICANT
    severity: high
```

---

## PB-NIS2-005: Supply Chain Compromise Response

**Trigger:** nis2-inc-005 (Supply Chain Compromise)

```
playbook: PB-NIS2-005
name: "NIS2 Supply Chain Response"
trigger: nis2-inc-005
severity: critical

steps:
  - id: 1
    action: quarantine_affected_package
    params:
      block_registry_pull: true
      pin_known_good_version: true

  - id: 2
    action: scan_all_deployments
    params:
      check_iocs: true
      verify_signatures: true
      scan_containers: true

  - id: 3
    action: rollback_if_compromised
    params:
      auto_rollback: false # Requires human approval
      prepare_rollback_plan: true

  - id: 4
    action: notify_supplier
    params:
      method: email
      include_iocs: true
      request_acknowledgment: true

  - id: 5
    action: start_nis2_timers
    params:
      early_warning: 24h
      full_report: 72h
```

---






### 3. PLAYBOOK TESTING

Playbook	Azken Proba Data	Emaita	Hurrengo Proba
PB-NIS2-001	—	Pendiente	2026-Q2
PB-NIS2-002	—	Pendiente	2026-Q2
PB-NIS2-003	—	Pendiente	2026-Q2
PB-NIS2-004	—	Pendiente	2026-Q2
PB-NIS2-005	—	Pendiente	2026-Q2

**Simulakro plana:** Hiruhilekoa — Tabletop + Live exercise

**Katalogoaren berrikusketa:** Seihilekoa

### 4. INTEGRAZIOAK

Sistema	Integrazioa	Egoera
Wazuh SIEM	Alerta arauak → Playbook trigger	
CrowdStrike EDR	Auto-isolation, IOC feed	
Cloudflare	DDoS mode, WAF rules	
Email (PGP)	Notification templates	
PagerDuty	Guardia alertak	
Ticketing (Jira/GitLab)	Intzidentzia kudeaketa	