

SOFTWARE & READINESS

Incident Response Readiness

We help you plan in advance what will be done when a security incident occurs, who is responsible and how communication will work, so you minimise the impact.

**6**

scope areas

5

step method

6

deliverables

// WHY IT MATTERS

Why it matters

The moment of an incident is the worst time to decide.



A ready plan, clear roles and rehearsed scenarios significantly reduce the time from detection to recovery and the cost of the incident.

// WHO IS IT FOR?

Who is this service for?



Organisations without a written response plan



Teams building or planning SOC/SIEM



Those working on ISO 27001 and ISO 22301



Those who want to rehearse incident scenarios with senior management

// SCOPE

What does it cover?

**Incident response plan**

We define roles, authorities, the communication chain and decision points.

**Classification and escalation**

We determine incident severity levels and who is informed and when.

**Scenario-based playbooks**

We prepare step-by-step guides for scenarios such as ransomware, account takeover and data leakage.

**Tabletop exercises**

We run realistic scenario exercises with management and technical teams.

**Evidence preservation and communication**

We plan evidence preservation, internal and external communication and KVKK breach notification.

**Post-incident review**

We design the post-incident evaluation and improvement process.

Think like an attacker, build like a defender.

// METHOD

How we work

1

Current state and risks

We assess your existing plans, team and most likely scenarios.

2

Defining the plan and roles

We write the response plan, responsibilities and communication flow.

3

Preparing playbooks

We develop actionable steps for priority scenarios.

4

Exercise

We test the plan with tabletop exercises and identify gaps.

5

Improvement

We update the plans from findings and set a regular review calendar.

// DELIVERABLES

What do we deliver?



Incident response plan and procedures



Classification and escalation matrix



Exercise report and improvement recommendations



Role and communication matrix



Scenario-based playbooks



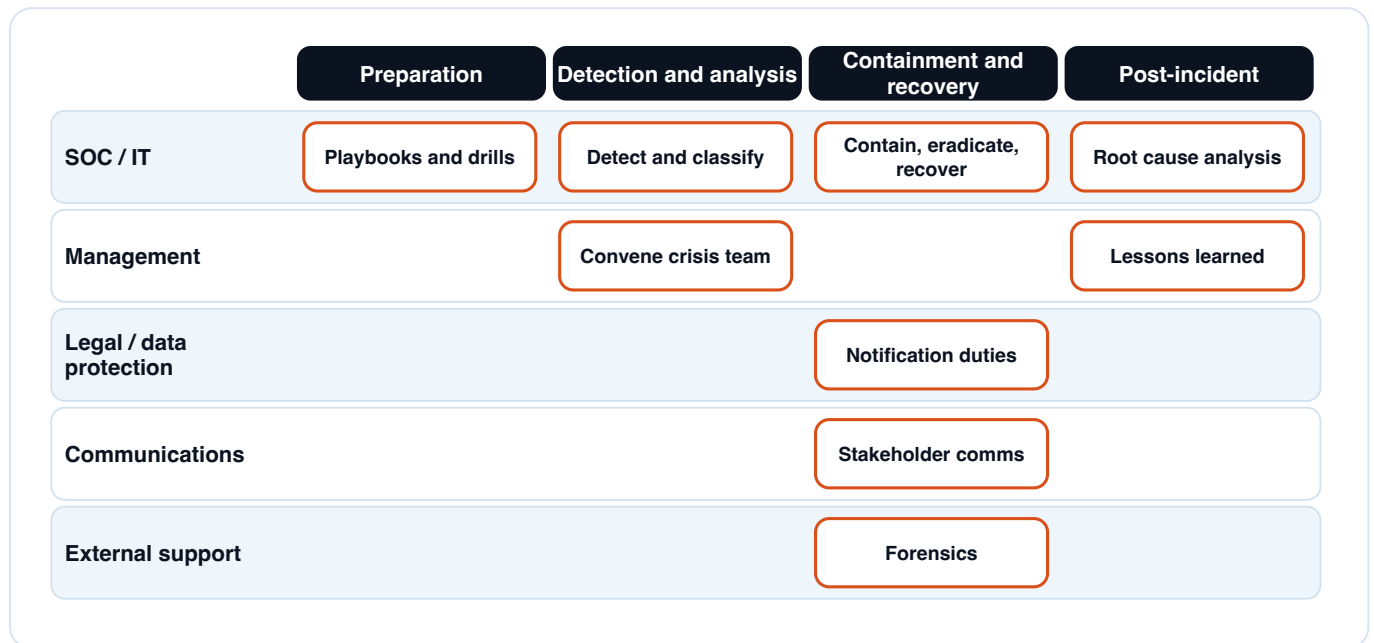
Post-incident review template

// VISUAL GUIDE

Service-specific visuals

Roles and phases in incident response

Who does what, and when? Agreeing this flow in advance saves time during a crisis.

**Roles agreed in advance**

Debating authority and duties during a crisis wastes time.

Not only technical

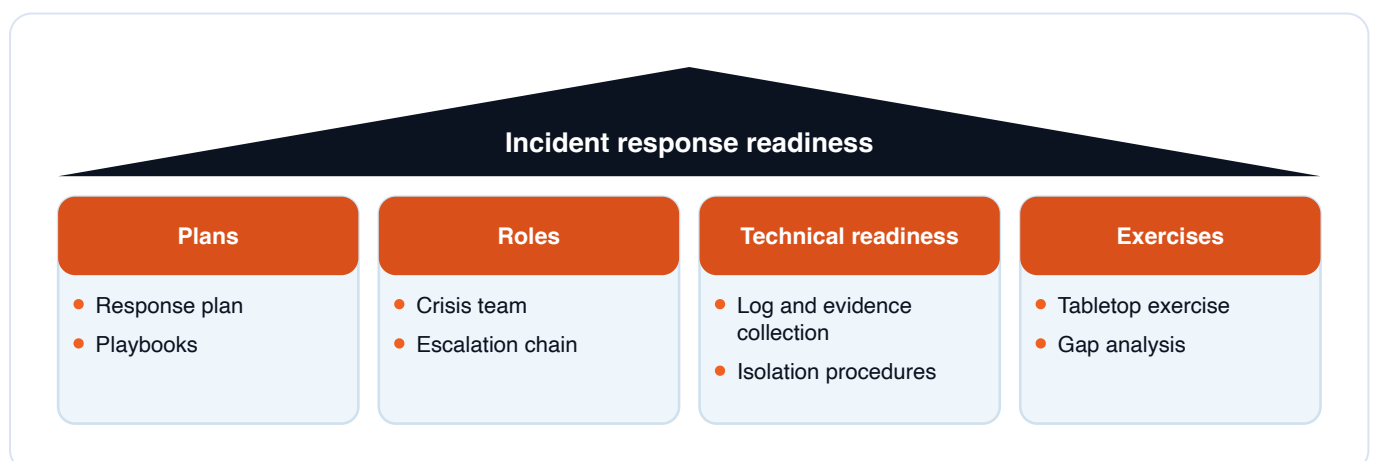
Legal, communications and management are part of the response.

The aftermath matters

Root cause analysis and lessons prevent the next incident.

Outputs of the preparation phase

These pieces, prepared before an incident, determine response time.

**Plan and playbooks**

Ready step-by-step procedures for common scenarios.

Evidence preserved

Log and evidence collection serve both analysis and legal processes.

Tested by exercise

A tabletop exercise reveals plan gaps before a real incident does.

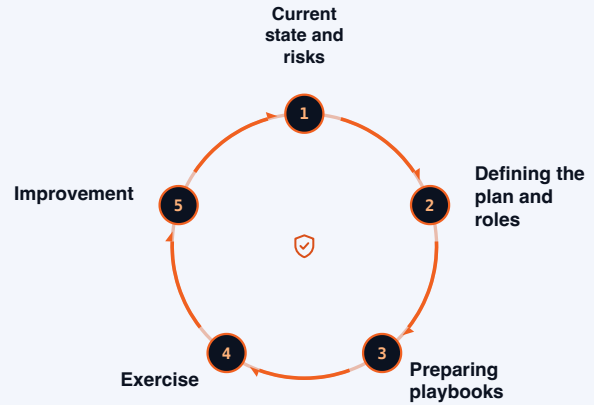
// AT A GLANCE

Service overview

SCOPE MAP



OUR DELIVERY LOOP



// UNDER ONE ROOF

Our other services



ISO 27001 Consulting

**KVKK Compliance Consulting**

Penetration Testing



SOC / SIEM Implementation



Information Security Awareness Program



ISO 22301 Consulting



Cyber Security Consulting



Regular Vulnerability Scanning and Management



Endpoint Security Monitoring



ISO 14298 Consulting



Risk Management Consulting



DoS, DDoS Testing and Protection



Secure Software Development

// CONTACT

Get in touch

Share your needs and current situation and we will define the right scope and roadmap together. Fill in our information form or contact us directly.

Troy Bilgi Teknolojileri Ticaret Limited Şirketi

Atatürk Mah. Vedat Günyol Cad. 44M/2

Ataşehir / İstanbul, Türkiye

T 0-216-575 5222 **E** info@troybilgiteknojileri.com



Scan the QR code for the
service page and information
form