

TESTING & MONITORING

Regular Vulnerability Scanning and Management

We set up and help run a sustainable vulnerability management process that scans your systems at regular intervals and helps you prioritise, fix and track vulnerabilities.

**6**

scope areas

5

step method

6

deliverables

// WHY IT MATTERS

Why it matters

New vulnerabilities are published every day; a scan done once becomes outdated quickly.



Regular scanning and prioritisation tell you which weakness to close first, so you spend limited resources on the highest risk.

// WHO IS IT FOR?

Who is this service for?



Those who need regular vulnerability management under ISO 27001



Teams without capacity to track new vulnerabilities



Organisations running many servers and applications



Those who want to establish basic hygiene before a penetration test

// SCOPE

What does it cover?

**Asset inventory**

We identify the systems, applications and owners to be scanned and keep the inventory current.

**Infrastructure scanning**

We regularly scan servers, network devices and operating-system vulnerabilities.

**Web application scanning**

We regularly detect common web vulnerabilities with automated tools.

**Cloud and configuration**

We review security settings of cloud resources and system configurations.

**Risk-based prioritisation**

We rank vulnerabilities by business impact and exploitability as well as technical severity.

**Remediation tracking**

We assign fixes, track them and verify through rescanning.

**Think like an attacker,
build like a defender.**

// METHOD

How we work

1

Scope and inventory

We determine the assets to scan and their criticality.

2

Policy and schedule

We define scan frequency, method and rules that limit impact on production.

3

Regular scanning

We run scans at the planned intervals.

4

Prioritisation and reporting

We prioritise findings and present them in clear reports.

5

Remediation tracking and validation

We verify closed vulnerabilities by rescanning and follow the trend.

// DELIVERABLES

What do we deliver?



Asset and scope inventory



Regular vulnerability reports



Vulnerability management process document



Scanning policy and schedule



Prioritised remediation list



Trend and executive summary reports

// VISUAL GUIDE

Service-specific visuals

From thousands of findings to the ones to fix first

Scan output is turned from a raw list into a risk-based priority order.

**Cuts the noise**

False positives are removed so the team focuses on real issues.

Adds context

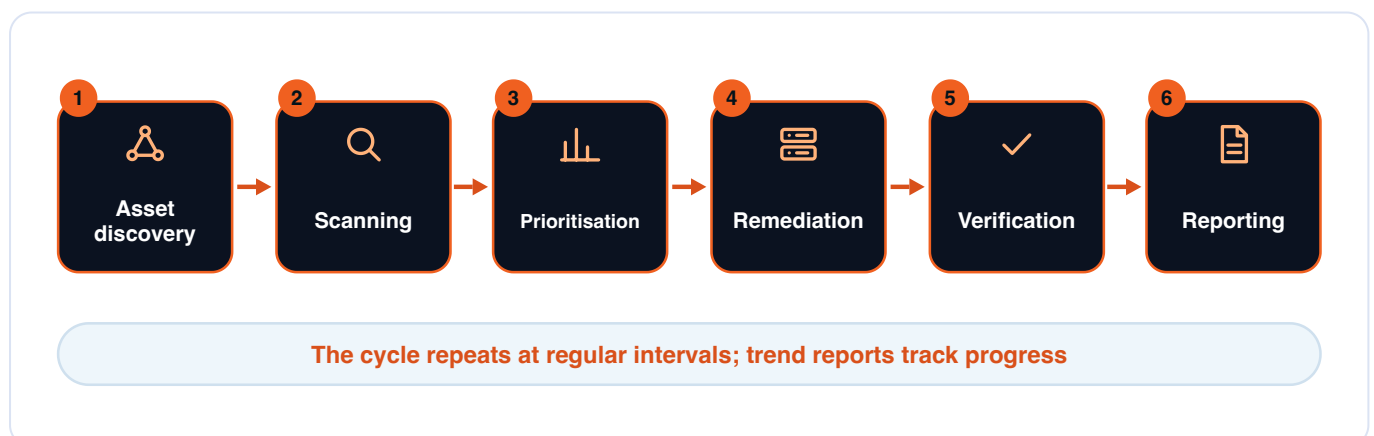
Severity reflects asset value and exposure, not just a score.

A closable list

The output is a short fix list with owners and target dates.

The recurring vulnerability management cycle

A regular, measurable process rather than a one-off scan.

**Inventory first**

An unknown asset cannot be scanned; discovery is the first step.

Regular repetition

New vulnerabilities appear constantly, so scanning must be periodic.

Trends tracked

Reports show trends in open findings and time to fix.

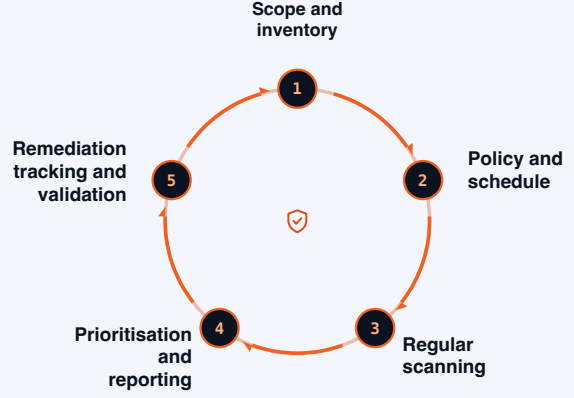
// AT A GLANCE

Service overview

SCOPE MAP



OUR DELIVERY LOOP



// UNDER ONE ROOF

Our other services

- | | | |
|--|--|--|
|  ISO 27001 Consulting |  ISO 22301 Consulting |  ISO 14298 Consulting |
|  KVKK Compliance Consulting |  Cyber Security Consulting |  Risk Management Consulting |
|  Penetration Testing |  DoS, DDoS Testing and Protection |  SOC / SIEM Implementation |
|  Endpoint Security Monitoring |  Secure Software Development |  Information Security Awareness Program |
|  Incident Response Readiness | | |

// 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@troybilgiteknolojileri.com

Scan the QR code for the service page and information form