

TESTING & MONITORING

SOC / SIEM Implementation

We support you in building a monitoring infrastructure that collects network, system and application logs centrally, correlates them and turns them into meaningful alerts.

**6**

scope areas

5

step method

6

deliverables

// WHY IT MATTERS

Why it matters

Most attacks leave traces first, but those traces get lost among scattered logs. A SIEM and SOC approach lets you see events from one place and respond in time.



We work vendor-neutral: we choose the right solution with you based on your needs, budget and existing infrastructure.

// WHO IS IT FOR?

Who is this service for?



Organisations without central log and event monitoring



Those not getting enough value from an existing SIEM



Organisations with logging and monitoring obligations under regulation



Organisations that want to build their own SOC

// SCOPE

What does it cover?

**Identifying log sources**

We prioritise which systems' logs should be monitored.

**SIEM implementation**

We support platform selection, set-up and log integrations.

**Correlation rules**

We develop detection rules by mapping use cases to MITRE ATT&CK.

**Alert tuning**

We reduce false positives and bring real threats to the surface.

**Dashboards and reporting**

We build meaningful dashboards and regular reports for operations and management.

**SOC processes**

We define incident classification, escalation and response workflows.



Think like an attacker, build like a defender.

// METHOD

How we work

1

Needs and source analysis

We identify goals, critical assets and existing log sources.

2

Architecture and product selection

We determine the right architecture and solution for you, vendor-neutrally.

3

Installation and integration

We install the platform and connect log sources.

4

Rule development and tuning

We deploy use cases and tune alerts for your environment.

5

Go-live and handover

We train your team and hand over operational processes.

// DELIVERABLES

What do we deliver?

- ✓ Monitoring architecture document
- ✓ Correlation rules and use-case list
- ✓ SOC process and incident response workflows

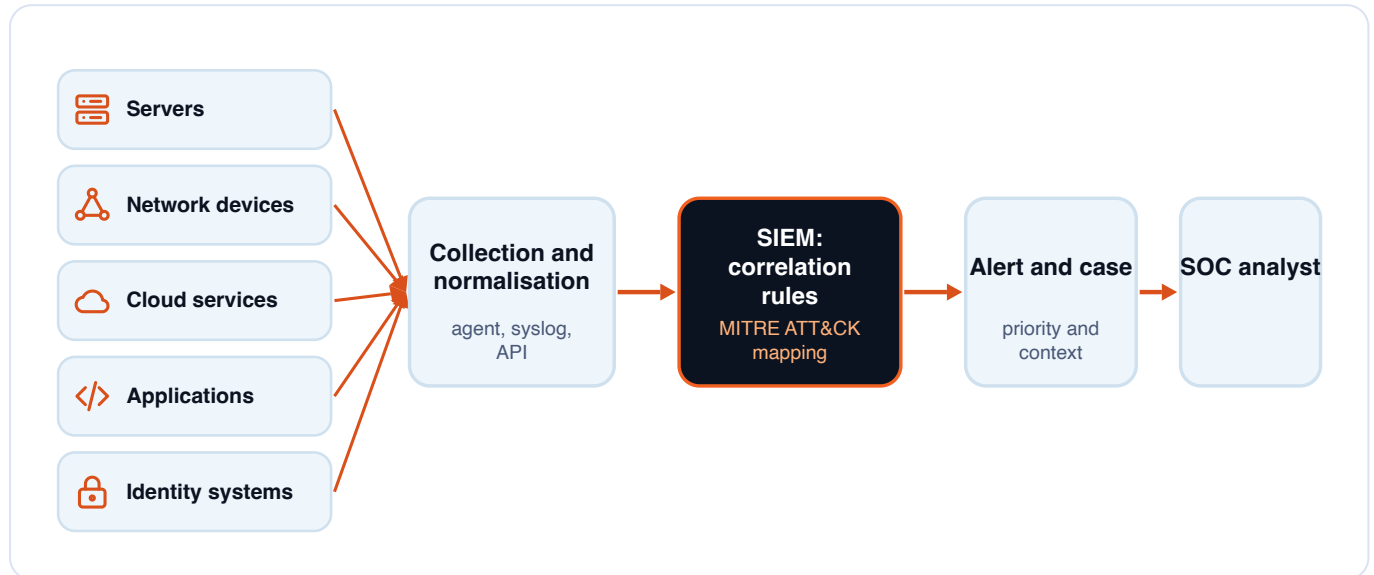
- ✓ Log source inventory
- ✓ Operations and management dashboards
- ✓ Training and handover documents

// VISUAL GUIDE

Service-specific visuals

From log sources to response: the SOC/SIEM data flow

Scattered logs are collected centrally, correlated by rules and reach the analyst as meaningful alerts.



Single view

Events from all sources are examined centrally in a common format.

Meaningful alerts

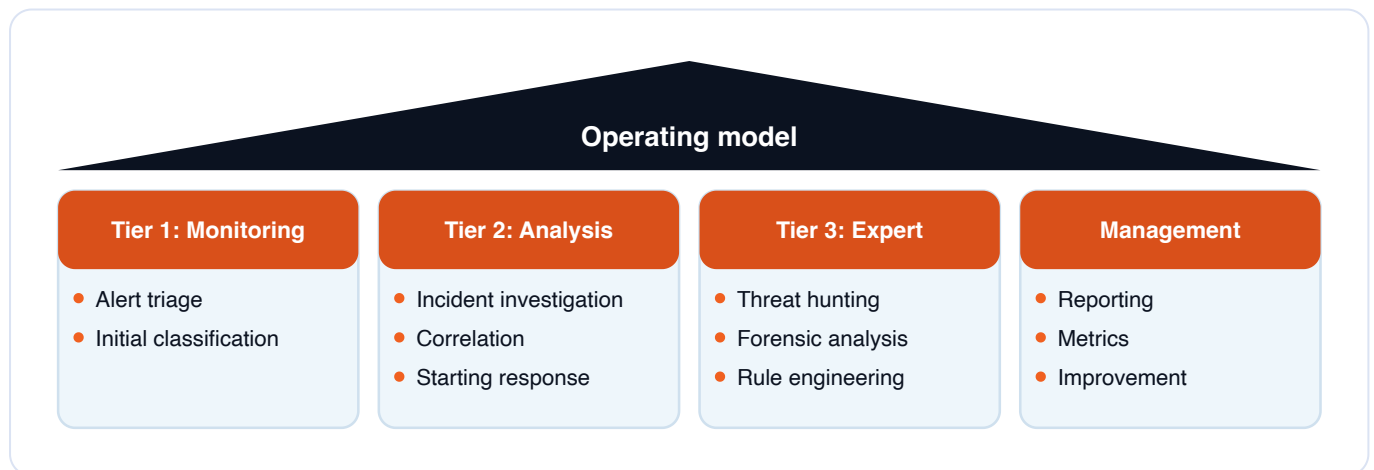
Correlation rules link single events to real threat scenarios.

Noise tuning

Rule tuning reduces false alarms and protects analyst time.

SOC tiers and responsibilities

A tiered structure routes alerts to the right person at the right depth.



Right depth

Simple alerts close at tier 1; complex incidents are escalated.

Proactive hunting

Tier 3 looks for threats without waiting for alerts.

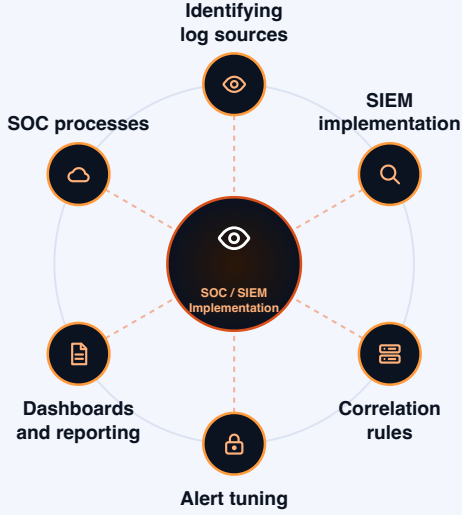
Measurable operations

Metrics show SOC performance and improvement.

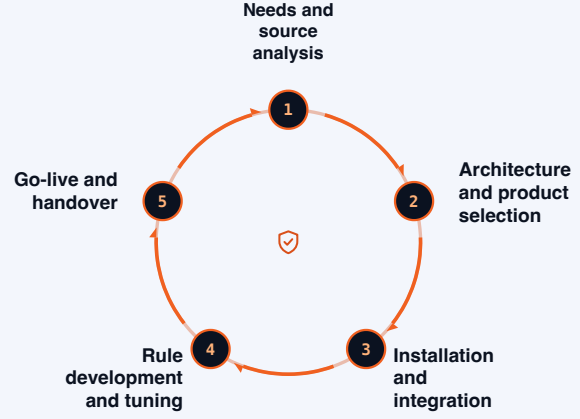
// AT A GLANCE

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 |  Regular Vulnerability Scanning and Management |  DoS, DDoS Testing and Protection |
|  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@troybilgiteknojileri.com



Scan the QR code for the service page and information form