

GUIDE

Getting Started with SOC/SIEM

For organisations considering central log monitoring and a SOC: where to start, which questions to ask and how to measure success.



GUIDE

ABOUT 7 MIN READ

SOC / SIEM

IN THIS GUIDE

1. SIEM, SOC and EDR: what is the difference?
2. Questions to ask before you start
3. Project roadmap
4. Log source priority
5. Use cases and tuning
6. Success metrics

01

SIEM, SOC and EDR: what is the difference?

SIEM

A platform that collects and correlates logs from many sources and raises alerts. It is a tool.

SOC

The team and processes that continuously monitor, investigate and respond to alerts. It is people and process.

EDR / XDR

Detection and response on endpoints (and, for XDR, wider sources); it feeds data to the SIEM.

Managed service

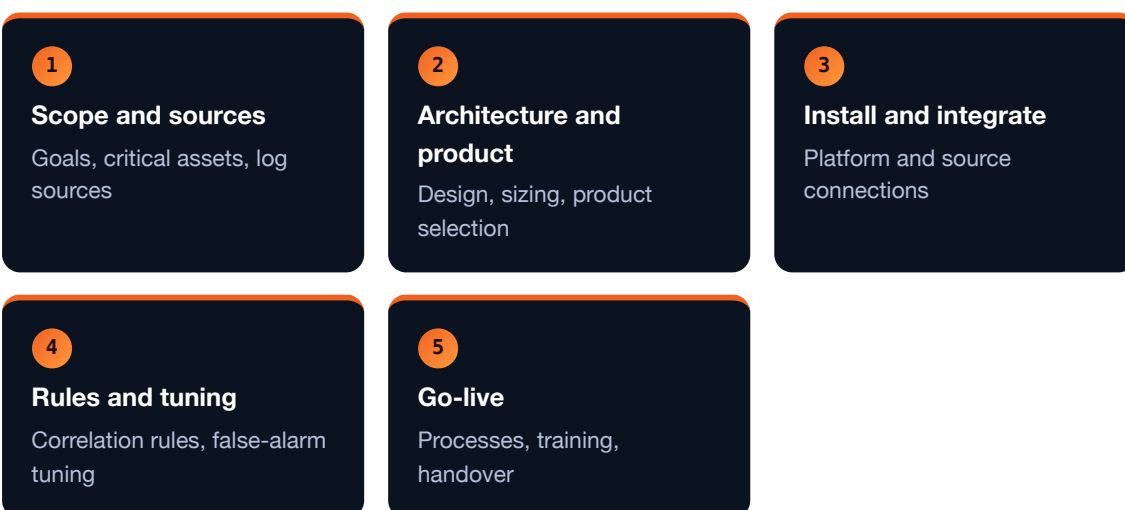
A provider runs part or all of the SIEM/SOC (MDR, managed SOC).

Important: Buying a SIEM is not building a SOC. Without people and process to watch the alerts, the tool creates no value.

02 Questions to ask before you start

- Which threats and which critical assets do we want visibility on?
- Which log sources exist and which must be enabled?
- What are the retention and compliance requirements?
- Do we have a team for 24/7 monitoring or will we buy a service?
- How will we measure success?

03 Project roadmap



04 Log source priority

Instead of connecting everything at once, start with the sources that create the most value:

- Identity systems (Active Directory, identity provider)
- Endpoints (EDR and server logs)
- Firewall, VPN and proxy
- E-mail security
- Cloud services
- Critical business applications

05 Use cases and tuning

Start rule writing with threat-driven scenarios, for example many failed logins followed by a successful one, sign-ins from unusual times or locations, and privilege escalation. Mapping to

MITRE ATT&CK makes coverage visible. Weeding out false alarms in the first weeks is critical to keep the team's trust in alerts.

06

Success metrics

- | | |
|--|--|
| ☐ Log source coverage (percentage of critical assets) | ☐ Mean time to detect (MTTD) and respond (MTTR) |
| ☐ False-alarm rate and time spent per alert | ☐ Rule coverage (mapping to ATT&CK techniques) |
| ☐ Number of incidents and resolution rate | |

Let's plan your SOC/SIEM project together We will define the architecture and roadmap that fit your needs.

// 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