

SECURITY OPERATIONS · SELF-ASSESSMENT

Take the 5-Minute Security Assessment.

10 QUESTIONS
5 MINUTESSELF-SCORED
INSTANT RESULTSNO DATA
COLLECTED

LIMITED TIME OFFER

**Book a Free
Security Consultation****30% OFF** EARLY BIRDS

Get expert advice from our SOC team and learn how to strengthen your security — no obligation.

01

VISIBILITY

YES NO

- 1 Are security logs from firewalls, servers, endpoints and cloud services collected into a single location?
Separate consoles obscure activity that spans them. ☐ YES ☐ NO
- 2 Are those logs retained for at least 90 days?
An incident discovered in week six cannot be investigated without them. ☐ YES ☐ NO
- 3 Could you establish today whether an account authenticated from an unexpected location last night?
If this takes more than an hour to determine, record it as No. ☐ YES ☐ NO

02

COVERAGE

- 4 Is a named individual responsible for reviewing security alerts on each working day?
A team name is not an owner. ☐ YES ☐ NO
- 5 Outside office hours and at weekends, does a defined person or service receive and act on alerts?
Intrusions are commonly timed for precisely these windows. ☐ YES ☐ NO

03

ACCESS CONTROL

- 6 Are all administrative and privileged accounts protected by multi-factor authentication?
Including service accounts and remote access. ☐ YES ☐ NO
- 7 Is all access revoked within two working days of an employee's departure?
VPN, email, file shares and every third-party application. ☐ YES ☐ NO

04

RESPONSE & RECOVERY

- 8 Have you restored data from backup in the last six months to verify recoverability?
Confirming that a backup job completed is a different test. ☐ YES ☐ NO
- 9 Do you hold a written incident response plan naming who is contacted in the first hour?
Including who authorises disconnection and who informs customers. ☐ YES ☐ NO
- 10 Would an incident occurring overnight be identified by your own systems, rather than reported to you by a customer, partner or bank?
External notification remains the most common way breaches are discovered. ☐ YES ☐ NO

SCORING — COUNT YOUR " NO " RESPONSES

0-1**Established**

Visibility and ownership are in place. The remaining work is tuning and continuous improvement.

2-4**Partial coverage**

The most common result. Technology is largely in place; the gap is ownership and hours of cover.

5+**Requires attention**

Begin with questions 4, 5 and 8 — the fastest to remediate, and the largest reduction in exposure.

WANT TO UNDERSTAND YOUR RESULTS BETTER ?

Free Demo & Consultation

Contact MekongNet for a free demo and consultation with the MekongDefense SOC team, and explore how 24/7 security monitoring can support your business.



015 234 501 | 023 226 622



info.mekongnet.com.kh/soc

**Book Now!**

A self-assessment for internal use. It is not a security audit and does not certify compliance with any standard.