KESER SECURITY OPERATIONS

Security Assessment — Intake Questionnaire

■ ASSESSMENT INTAKE QUESTIONNAIRE

This questionnaire helps us design the right assessment scope for your environment. Complete as much as you can — nothing is required. We'll fill gaps on our first call.

■ ORGANIZATION INFORMATION

Organization / Company Name	**Industry / Sector**
Primary Contact Name	**Title / Role**
Email Address	**Phone (optional)**
City / Region	**Country**

■ ENVIRONMENT SIZE

Approximate number of employees	**Approximate number of managed devices**
Number of physical locations / sites	**Number of countries of operation**

Primary cloud environment(s):

■ AWS	■ Azure	■ Google Cloud	■ On-premise only	■ Hybrid / Mixed

Organization type:

■ For-profit business	■ Non-profit	■ Government / Public sector	■ Educational institution

■ CURRENT SECURITY ENVIRONMENT

Do you currently have a dedicated security team or person?

■ Yes, full-time security staff	■ Shared IT/security role	■ Outsourced / MSSP	■ No dedicated resource

Which of the following do you currently have in place? (check all that apply)

■ Endpoint detection (EDR)	■ Firewall / UTM	■ Email security / filtering
■ VPN / Remote access controls	■ Network monitoring / IDS	■ SIEM or log aggregation
■ Multi-factor authentication (MFA)	■ Vulnerability scanning	■ Incident response plan

How would you describe your current security monitoring coverage?

☐ Comprehensive	☐ Partial — some systems	☐ Minimal — mostly reactive	☐ Unknown / not sure

Do you operate in a regulated industry or have compliance requirements?

☐ HIPAA	☐ PCI-DSS	☐ SOC 2	☐ ISO 27001	☐ None / Not sure

Additional context on your current security environment:

■ MONITORING & DETECTION

Which types of traffic or activity are you currently monitoring? (check all that apply)

☐ Outbound internet traffic	☐ Internal network traffic	☐ Cloud API activity
☐ User authentication events	☐ Endpoint process / file activity	☐ DNS queries

How long are logs or security events currently retained?

☐ Less than 30 days	☐ 30–90 days	☐ 90 days – 1 year	☐ More than 1 year	☐ Unknown

Have you experienced any of the following in the past 24 months? (check all that apply)

☐ Ransomware or malware incident	☐ Phishing attack (successful)	☐ Unauthorized access
☐ Data loss or exfiltration	☐ Business email compromise (BEC)	☐ None of the above

Is there a specific concern or recent event that prompted this assessment?

■ AI & EMERGING RISK

Are employees using AI tools (ChatGPT, Copilot, Gemini, etc.) for work?

☐ Yes, officially approved	☐ Yes, unsanctioned / shadow AI	☐ Not sure	☐ No

Do you have a policy governing AI tool use and data handling?

☐ Yes, formal written policy	☐ Informal guidance only	☐ In progress	☐ No policy

■ ASSESSMENT GOALS

What are you hoping to get from this assessment? (check all that apply)

☐ Understand current risk posture	☐ Identify monitoring / detection gaps	☐ Meet a compliance requirement

☐ Prepare a board / leadership briefing	☐ Build a security roadmap	☐ Evaluate outsourcing SecOps

What is your preferred timeline to begin?

☐ Immediately	☐ Within 30 days	☐ 1–3 months	☐ Exploring / no fixed timeline

Is there an existing budget allocated for this engagement?

☐ Yes, budget approved	☐ Under discussion	☐ No formal budget yet	☐ Prefer not to say

Who else is involved in this decision?

☐ IT leadership	☐ C-suite / Executive team	☐ Board of directors	☐ External advisor / counsel

Anything else you'd like us to know before our first conversation?

Return this form by email: paul@keser.com | Or paste your answers into the contact form at keser.com/contact