Penetration Testing Client Intake & Scoping Form

Help us understand your environment so we can recommend the right testing and give you an accurate fixed-fee proposal.

How to complete this form

- Fill in what you know. **"Don't know" is a perfectly good answer**; we'll help fill the gaps.
- On a computer: click any box and type, tick the check boxes, then save and email the PDF back.
- Tick **one** box for questions with a single answer; tick **all that apply** for lists.
- On paper: print, write in the boxes, and scan or photograph it.
- **Please do not write passwords, keys or secrets on this form.** We'll arrange a secure way to share access details later.
- Completing this form is **not** authorization to test. Testing starts only after a signed agreement and Rules of Engagement.

Please return to (name / email) | Requested return date

Date completed | Completed by (name) | Title

1 ORGANIZATION & CONTACTS

Company legal name | Doing business as (if different)

Street address | City | State | ZIP

Website | Industry / sector | Number of employees

Number of office / facility locations | Countries where you operate | Parent company / subsidiaries

People we should know about

	Title	Email	Phone
Primary contact			
Executive sponsor / decision-maker			
Technical contact (IT / security)			
24/7 emergency contact			Mobile
Billing / procurement contact			

2 GOALS & DRIVERS

What is prompting this assessment? (check all that apply)

- ☐ Compliance / audit requirement
- ☐ Cyber-insurance application or renewal
- ☐ Board / executive request
- ☐ Annual / routine testing
- ☐ Customer or partner requirement
- ☐ Recent security incident
- ☐ New system, app or acquisition
- ☐ Proactive improvement
- ☐ Other:

Which standards or regulations apply to you?

- ☐ PCI DSS
- ☐ ISO 27001
- ☐ NYDFS 500
- ☐ HIPAA
- ☐ NIST CSF / 800-53
- ☐ GLBA / FFIEC
- ☐ SOC 2
- ☐ CMMC / NIST 800-171
- ☐ GDPR / CCPA
- ☐ None / not sure
- ☐ Other:

What do you need from the results?

- ☐ Compliance evidence / report for auditor
- ☐ Prioritized fix list for IT
- ☐ Test our detection & response
- ☐ Proof for customers or insurer
- ☐ Board-level risk summary
- ☐ Security awareness baseline
- ☐ Other:

Who will read the report? (e.g., IT team, CISO, board, auditor, customers)

What are you most worried about, or what data / systems can you least afford to lose or expose?

Any specific attack scenarios you want us to try? (e.g., ransomware, stolen laptop, phishing, insider, customer-data theft)

3 SERVICES OF INTEREST

Tick everything you'd like us to consider. Not sure? Tick the last box and we will recommend.

Services

- ☐ A Vulnerability Assessment (scan + manual validation)
- ☐ B External Penetration Test (internet-facing)
- ☐ C Internal Penetration Test (inside the network)
- ☐ D Web Application / API Assessment
- ☐ E Wireless Security Assessment
- ☐ F Social Engineering (phishing / vishing / physical)
- ☐ G Red Team Exercise (full-scope, tests detection)
- ☐ H Cloud Security Review (AWS / Azure / GCP / M365)
- ☐ Mobile application assessment
- ☐ Purple-team workshop / IR tabletop exercise
- ☐ Quarterly recurring program (retests + trend reporting)
- ☐ Not sure: please recommend

Do you want retesting after fixes are made? ☐ Yes ☐ No ☐ Not sure

Are you interested in an ongoing (quarterly) program? ☐ Yes ☐ No ☐ Maybe, tell us more

4 EXTERNAL (INTERNET-FACING) ENVIRONMENT

Approx. number of public IP addresses

Approx. number of domains / hostnames

Number of locations with internet links

List public IP ranges and domains in scope (or attach a list). Do not include any you do not own or control.

Which internet-facing services do you run?

- ☐ Websites / web apps
- ☐ Customer / partner portals
- ☐ APIs
- ☐ Email servers
- ☐ VPN / remote access
- ☐ Remote Desktop / SSH exposed
- ☐ File transfer (SFTP/FTP)
- ☐ VoIP / phone systems
- ☐ IoT / OT / building systems
- ☐ Other:

Where are they hosted? ☐ On-premises ☐ Cloud (AWS / Azure / GCP) ☐ Colocation ☐ Hosting provider / MSP

Is a WAF, CDN or DDoS service in front of them? ☐ Yes ☐ No ☐ Don't know

Do any systems belong to a vendor/host who must approve testing? ☐ Yes ☐ No ☐ Don't know

5 INTERNAL NETWORK

Number of sites / offices

Approx. number of subnets / VLANs

Approx. number of servers

Approx. workstations / laptops

Approx. number of users / staff

Number of Active Directory domains / forests

Number of domain controllers

Operating systems and platforms in use

- ☐ Windows Server
- ☐ Windows 10/11
- ☐ macOS
- ☐ Linux
- ☐ VMware / Hyper-V
- ☐ Network / security appliances
- ☐ Databases (SQL, Oracle, etc.)
- ☐ Legacy / end-of-life systems
- ☐ Other:

Identity platform: ☐ On-prem Active Directory ☐ Entra ID / Azure AD ☐ Okta / other SSO ☐ Local accounts only

Do you use multi-factor authentication (MFA)? ☐ All users ☐ Some users ☐ No ☐ Don't know

Is the network segmented (e.g., guest, servers, PCI, OT)? ☐ Yes ☐ Partly ☐ No ☐ Don't know

Endpoint protection / EDR in place? ☐ Yes, managed 24/7 ☐ Yes, unmanaged ☐ Antivirus only ☐ No

Security monitoring (SIEM / SOC / MDR)? ☐ In-house ☐ Outsourced ☐ None ☐ Don't know

Is IT managed by an outside provider (MSP)? ☐ Yes ☐ No ☐ Partly

Name of MSP / security provider (if any)

Do they need to authorize testing? (Y/N)

Where may we test from? ☐ Remote (VPN / our device) ☐ On-site ☐ Either

How much do you want to tell us in advance? ☐ Nothing (outsider view) ☐ Some (standard user account) ☐ Everything (admin / documentation)

6 WEB APPLICATIONS & APIs

List each application or API you want tested. Add more on a separate sheet if needed.

Application name / URL	Type (public / internal)	User roles	Tech (e.g., .NET)	Prod / staging

May we test the live (production) version? ☐ Yes ☐ Staging only ☐ Not sure

Will you provide test accounts for each user role? ☐ Yes ☐ No ☐ Not sure

Do the apps handle payment cards, health data or other regulated data? ☐ Yes ☐ No ☐ Don't know

Do you have a mobile app we should include? ☐ iOS ☐ Android ☐ Both ☐ None

7 CLOUD ENVIRONMENT

Which cloud and SaaS platforms do you use?

- ☐ Microsoft 365
- ☐ Azure
- ☐ AWS
- ☐ Google Cloud
- ☐ Google Workspace
- ☐ Salesforce
- ☐ Other SaaS (list below)
- ☐ None

Number of cloud accounts / subscriptions / tenants

Main regions used

Infrastructure-as-code? (Y/N)

Key business systems or data stored in the cloud

8 WIRELESS

Number of locations with Wi-Fi

Approx. number of access points

Network names (SSIDs)

Wi-Fi security type ☐ WPA2-Enterprise / 802.1X ☐ WPA3 ☐ WPA2 pre-shared key ☐ Don't know

Is there guest Wi-Fi? ☐ Yes ☐ No

Is Wi-Fi shared with warehouse, POS, IoT or OT devices? ☐ Yes ☐ No ☐ Don't know

9 SOCIAL ENGINEERING (complete only if interested)

Which tests are you comfortable with?

- ☐ Phishing emails
- ☐ Text-message (SMS) phishing
- ☐ Phone (vishing) calls
- ☐ Physical building entry attempts
- ☐ USB drop / device tests

Number of employees to include

Email provider / security gateway

Locations for physical tests

Who inside your company will know in advance? ☐ Executives only ☐ IT / security team ☐ No one else

People or departments that must NOT be targeted

10 CONSTRAINTS & LOGISTICS

Systems, networks or data that are OFF-LIMITS (e.g., production database, medical devices, third-party systems)

Fragile or business-critical systems that need extra care

Preferred testing hours / days

Blackout dates (e.g., month-end, holidays, launches)

Is it OK to test during business hours? ☐ Yes ☐ After hours only ☐ Weekends only ☐ Either

Should your security team be told when testing starts? ☐ Yes, fully informed ☐ No, test detection ☐ Undecided

Will you allow-list our testing IP addresses? ☐ Yes ☐ No, test as-is ☐ Not sure

Does any contract, hosting or MSP agreement restrict security testing? ☐ Yes ☐ No ☐ Don't know

Is any data subject to special handling (PHI, PCI, government, export-controlled)? ☐ Yes ☐ No ☐ Don't know

If yes, describe the handling requirements

11 SECURITY HISTORY & MATURITY

Date of last penetration test | **Performed by** | **Were findings fixed? (all / some / none)**

Do you run vulnerability scans? ☐ Weekly ☐ Monthly ☐ Quarterly ☐ Rarely / never

Patching cadence ☐ Within 2 weeks ☐ Monthly ☐ Ad hoc ☐ Don't know

Do you have a written incident response plan? ☐ Yes, tested ☐ Yes, untested ☐ No

Number of dedicated IT / security staff | **Security incidents in the past 2 years (count)**

Do you carry cyber-liability insurance? ☐ Yes ☐ No ☐ Don't know

Anything about your security posture we should know up front?

12 TIMELINE, BUDGET & PROCUREMENT

Earliest start date | **Must be finished by** | **Reason for deadline**

Approximate budget range ☐ Under $10K ☐ $10K–$25K ☐ $25K–$50K ☐ $50K–$100K ☐ $100K+ ☐ Not sure

Is the budget already approved? ☐ Yes ☐ Pending ☐ No

Who approves the purchase? | **Approval / procurement steps and typical lead time**

Paperwork we should expect

- ☐ NDA (ours)
- ☐ NDA (yours)
- ☐ Vendor onboarding / security questionnaire
- ☐ Certificate of insurance
- ☐ W-9 / tax forms
- ☐ Purchase order
- ☐ Master services agreement
- ☐ Other:

Anything else we should know?

13 ACKNOWLEDGEMENT

Acknowledgement. I confirm that the information above is accurate to the best of my knowledge, and that I am authorized to provide it on behalf of the organization. I understand that listing a system here does not authorize testing. Testing will begin only after the organization signs a statement of work, rules of engagement and written authorization confirming that it owns, or is permitted to authorize testing of, every system in scope.

Name	Title	Date

Signature (type your name, or sign after printing)	Email

FOR SENTINEL CONSULTING USE ONLY

Received: _____	Reviewed by: _____	Scope tier: S / M / L	Proposal due: _____