

# PRE-ENGAGEMENT QUESTIONNAIRE

## Internal Network & Active Directory Penetration Test

**Client** Navigating Security Corp.  
**Provider** TadiSec  
**SOW Reference** TDSC-SOW-2026-001  
**Date Issued** March 5, 2026  
**Completed By** Aarav Patel, IT Director  
**Classification** Confidential

### Purpose

This questionnaire collects the technical and operational information TadiSec needs to prepare for the engagement. It should be completed by the Client's Technical POC and returned to TadiSec at least 5 business days before the kickoff meeting. Answers will be verified during kickoff.

## A. Network & Infrastructure

#	Question & Answer
A1	<b>What is the in-scope network range?</b> 10.1.1.0/24 - single flat subnet (Corporate LAN). Only DC01 (10.1.1.10) is authorized for testing; all other hosts are out of scope.
A2	<b>How many live hosts are expected on the subnet?</b> Approximately 18–23 live hosts, but only DC01 is in scope for testing. May discover less during testing.
A3	<b>What is the IP address and hostname of the domain controller?</b> DC01 at 10.1.1.10, running Windows Server 2019.
A4	<b>Is there a network gateway or firewall on the subnet? What IP?</b> Yes - 10.1.1.1 (network gateway/firewall). Out of scope.
A5	<b>Are there any other infrastructure devices on the subnet that should not be scanned (VOIP, printers, etc.)?</b> No.
A6	<b>What is the network topology? Single VLAN, segmented, or other?</b> Single flat VLAN - no segmentation within the /24 subnet.
A7	<b>Is there a VPN or remote access solution TadiSec testers should use?</b> Yes - VPN access will be provisioned. Details to be confirmed at kickoff.

## B. Active Directory

#	Question & Answer
B1	<b>What is the Active Directory domain name?</b> navigatingsecurity.corp
B2	<b>How many domain controllers are in the environment?</b> One - DC01 (10.1.1.10). Single-forest, single-domain.
B3	<b>What is the domain and forest functional level?</b> TBC.
B4	<b>Are there any domain or forest trust relationships?</b> None. Isolated single-domain environment.
B5	<b>Is Active Directory Certificate Services (ADCS) deployed? If so, on which host?</b> Not to our knowledge.
B6	<b>Is LAPS deployed? What is the coverage?</b> No.
B7	<b>Approximately how many domain user accounts are active?</b> Approximately 120 (or less) active user accounts.
B8	<b>Are there any known service accounts with SPNs registered?</b> To be confirmed at kickoff.
B9	<b>Are there any Azure AD / hybrid identity components connected to this domain?</b> Not in scope for this engagement. Cloud identity assessment planned for Q3 2026.

## C. Security Controls

#	Question & Answer
C1	<b>What endpoint protection / EDR product is deployed?</b> Windows Defender
C2	<b>Is the EDR in active blocking mode or passive/monitoring mode?</b> Passive monitoring. Defences are still reactive at the moment.
C3	<b>Is there a SIEM in place? Which product?</b> Wazuh. SOC monitors via Wazuh.
C4	<b>Is there a managed SOC or MSSP? If so, do they need to be notified?</b> In-house SOC managed by Cathy Williams. Cathy will brief the SOC team before testing.
C5	<b>What is the current domain password policy?</b>

	Minimum 8 characters, complexity enabled, account lockout at 5 failed attempts per 30-minute window, auto-unlock after 30 minutes.
<b>C6</b>	<b>Is SMB signing required on DC01?</b> To be confirmed during testing.
<b>C7</b>	<b>Are there any IDS/IPS systems on the network that might interfere with testing?</b> To be confirmed at kickoff.

## D. Credentials & Access

#	Question & Answer
<b>D1</b>	<b>What domain user account will be provisioned for the assumed breach?</b> t.chigubhu - assigned to Domain Users group only. No elevated privileges.
<b>D2</b>	<b>Has the account been created and tested for successful domain authentication?</b> To be confirmed at kickoff. The account should be created and tested by March 23.
<b>D3</b>	<b>How will credentials be delivered to TadiSec?</b> Secure handoff via Bitwarden file or encrypted channel during kickoff.
<b>D4</b>	<b>Will TadiSec be testing from on-site or remotely?</b> Remote (via VPN), unless otherwise arranged.
<b>D5</b>	<b>If remote, what VPN solution is in use and has TadiSec access been configured?</b> VPN solution and access to be provisioned prior to kickoff. Details TBC.

## E. Operations & Logistics

#	Question & Answer
<b>E1</b>	<b>Are there scheduled maintenance windows, batch jobs, or backups during testing hours?</b> Nightly backups run at 2:00 AM EST. Month-end batch processing on March 30–31 (testing blackout).
<b>E2</b>	<b>Has DC01 been backed up? Is the backup verified as restorable?</b> Backup scheduled for March 21, 2026. To be verified by Aarav Patel.
<b>E3</b>	<b>Are there any change freezes or blackout periods during the testing window?</b> March 30–31, 2026 - month-end processing. No testing permitted.
<b>E4</b>	<b>Will the Client make any infrastructure changes (patching, GPO updates, etc.) during the testing window?</b> No changes planned. Client will notify TadiSec if any become necessary.
<b>E5</b>	<b>What is the preferred communication channel for daily status updates?</b> Microsoft Teams - shared channel "TadiSec × NavSec - Pentest".

<b>E6</b>	<b>Are there any upcoming compliance audits or certification deadlines the engagement should support?</b> SOC 2 Type II audit scheduled for Q3 2026. Pentest findings will inform remediation priorities.
-----------	--

## F. Compliance & Data Sensitivity

---

#	Question & Answer
<b>F1</b>	<b>Which regulatory frameworks apply to the Client's environment?</b> SOC 2 Type II. Applicable state privacy regulations for PII handling.
<b>F2</b>	<b>Does the Active Directory environment store or process PII?</b> Potentially - user attributes, HR-related data in AD fields, and SYSVOL contents may include PII.
<b>F3</b>	<b>Are there specific data handling requirements for PII discovered during testing?</b> PII must be redacted in all evidence. No PII exfiltrated from the environment. Findings involving PII flagged in the report.
<b>F4</b>	<b>Does the Client require TadiSec personnel to pass background checks?</b> No background checks required. TadiSec confirms all testers hold valid industry certifications or equivalent and have undergone internal vetting.

## Completion & Acknowledgment

---

By completing this questionnaire, the Client confirms that the information provided is accurate to the best of their knowledge. Any inaccuracies discovered during the engagement will be addressed jointly with TadiSec.

**Completed by:** Aarav Patel, IT Director

**Date:** March 10, 2026

**Reviewed by:** Rumbidzai Moyo, Principal Consultant, TadiSec

**Date:** March 12, 2026

*- End of Pre-Engagement Questionnaire -*