# STATEMENT OF WORK

## Internal Network & Active Directory Penetration Testing Services

Prepared for: **Navigating Security Corp.**

Prepared by: **TadiSec**

| | |
|---|---|
| **Document No.** | TDSC-SOW-2026-001 |
| **Version** | 1.0 |
| **Date Issued** | March 12, 2026 |
| **Classification** | Confidential |



***Take note that all items in this document are completely fictional for learning purposes.***

# 1. Document Control

## 1.1 Revision History

| Version | Date | Author | Description |
|---|---|---|---|
| 1.0 | March 12, 2026 | Rumbidzai Moyo | Initial draft |

## 1.2 Points of Contact

| Role | Name | Title | Email | Phone |
|---|---|---|---|---|
| TadiSec Project Lead | Rumbidzai Moyo | Principal Consultant | r.moyo@tadisec.co.zw | +263 77 234 8901 |
| TadiSec Lead Tester | Tonderai Chigubhu | Senior Penetration Tester | t.chigubhu@tadisec.co.zw | +263 71 445 6782 |
| Client Primary POC | Oliver Whitaker | CISO | o.whitaker@navseccorp.com | +1 (212) 555-0147 |
| Client Technical POC | Aarav Patel | IT Director | a.patel@navseccorp.com | +1 (212) 555-0162 |
| Client Emergency POC | Cathy Williams | SOC Manager | c.williams@navseccorp.com | +1 (212) 555-0199 |

## 1.3 Document Distribution

This Statement of Work is classified as Confidential. Distribution is limited to the individuals listed in Section 1.2 and any additional parties authorized in writing by both TadiSec and Navigating Security Corp. This document shall not be forwarded, copied, or shared with any unauthorized party.

# 2. Engagement Overview

## 2.1 Purpose

TadiSec ("TadiSec" or "Provider") has been engaged by Navigating Security Corp. ("NavSec Corp" or "Client") to perform an Internal Network and Active Directory Penetration Test of the Client's corporate environment. This Statement of Work ("SOW") defines the scope, objectives, methodology, deliverables, timeline, and terms governing the engagement.

This SOW is incorporated into and governed by the Master Services Agreement ("MSA") executed between TadiSec and the Client. In the event of any conflict between this SOW and the MSA, the terms of the MSA shall prevail unless explicitly stated otherwise herein.

### 2.2 Engagement Summary

| Field | Detail |
|---|---|
| Engagement Title | Q2 2026 Internal Network & Active Directory Penetration Test |
| Engagement Type | Internal Network Penetration Test with Active Directory focus |
| Testing Perspective | Assumed Breach / Internal Threat Actor (See Section 4.1) |
| Testing Approach | Manual testing with automated tool support (See Section 4) |
| Estimated Duration | 8 business days of active testing |
| Testing Window | March 24, 2026 – April 3, 2026 |
| Report Delivery | April 10, 2026 (within 5 business days of testing completion) |
| Readout Presentation | April 23, 2026 |

### 2.3 Background

Navigating Security Corp. is a mid-size firm headquartered in the United States with approximately 120 employees. As part of its annual security assessment program and ongoing compliance obligations under SOC 2 and applicable state privacy regulations, the Client has engaged TadiSec to assess the security posture of its internal network and Active Directory infrastructure.

This is the Client's first dedicated internal network penetration test. Previous assessments have focused on external perimeter and web application testing conducted by a separate provider. The Client's IT leadership has identified Active Directory security as a priority following an industry-wide increase in identity-based attacks.

## 3. Objectives

### 3.1 Primary Objectives

The penetration test is designed to answer the following questions about the Client's internal security posture:

- Can an attacker with internal network access escalate privileges to gain Domain Administrator or equivalent access within the Active Directory environment?
- Are there credential hygiene issues (weak passwords, password reuse, Kerberoastable service accounts, cached credentials) that could be exploited?
- Are Group Policy configurations and AD security settings aligned with industry best practices?
- Does the Client's endpoint protection platform detect and respond to common post-exploitation techniques?
- Can sensitive data (PII, credentials, financial records) be accessed through misconfigured AD attributes, GPO preferences, or SYSVOL contents?

- Are there Active Directory Certificate Services (ADCS) misconfigurations that could enable persistence or privilege escalation?
- What is the blast radius of a compromised standard domain user account within the navigatingsecurity.corp domain?

### 3.2 Additional Custom Objectives

- Evaluate the effectiveness of the deployed EDR solution against common AD attack tooling (BloodHound, Rubeus, Mimikatz).
- Assess whether LAPS is correctly configured and enforced across the environment, if at all.

## 4. Testing Approach & Methodology

### 4.1 Engagement Model

This engagement follows an **Assumed Breach** model. The Client will provision a standard domain user account (t.chigubhu) for TadiSec Lead Tester Tonderai Chigubhu, assigned to the Domain Users group. Testing will be conducted remotely by using VPN credentials to connect to our network and to the 10.1.1.0/24 subnet.

> **Why Assumed Breach?**
> An assumed breach engagement typically bypasses most of the effort spent on simulating initial access and focuses on high-impact post-compromise activities such as lateral movement, privilege escalation, and data exfiltration. This model is widely promoted in industry and aligns with modern threat intelligence on adversary post-compromise behavior and is derived from guidance documents such as NIST SP 800-115.

### 4.2 Methodology

TadiSec follows a structured penetration testing methodology aligned with the Penetration Testing Execution Standard (PTES) and NIST SP 800-115, adapted for Active Directory environments:

| Phase | Description | Key Activities |
|---|---|---|
| 1. Reconnaissance & Enumeration | Active information gathering within 10.1.1.0/24 and the navigatingsecurity.corp domain. | Host discovery, port/service scanning, AD enumeration (users, groups, GPOs, trusts, SPNs, ACLs), DNS analysis |
| 2. Vulnerability Discovery | Identification of exploitable weaknesses across the domain controller and AD configurations. | Credential spraying, Kerberoasting, AS-REP roasting, LDAP analysis, GPP password checks, ADCS template enumeration |
| 3. Exploitation | Controlled exploitation of confirmed vulnerabilities to validate impact. | Hash extraction, relay attacks, token impersonation, Kerberos delegation |

| | | |
|---|---|---|
| | | abuse, DACL abuse, ADCS certificate abuse |
| 4. Privilege Escalation | Attempting to escalate from t.chigubhu (Domain Users) to Domain Admin or equivalent. | DCSync, Silver/Golden Ticket, AdminSDHolder abuse, GPO abuse, certificate template abuse |
| 5. Post-Exploitation | Assessing the impact of full domain compromise. | Sensitive data access via AD attributes, SYSVOL, domain persistence mechanisms, exfiltration path validation |
| 6. Documentation & Reporting | Compilation of findings, evidence, and remediation guidance. | Finding write-ups, evidence capture, CVSS v3.1 scoring, executive summary, full technical report |

### 4.3 Tools

TadiSec utilizes a combination of industry-standard tools. Representative, non-exhaustive list:

- Network Scanning & Enumeration: Nmap, NetExec, Enum4linux-ng
- Active Directory: BloodHound, Impacket, Rubeus, Certify, ADRecon, PowerView
- Exploitation: Metasploit Framework, manual exploit code
- Credential Attacks: Hashcat, John the Ripper, Responder, ntlmrelayx, Kerbrute
- Post-Exploitation: Mimikatz, SharpHound, Sliver, LaZagne
- Documentation: PwnDoc (reporting platform), Flameshot (evidence capture)

### 4.4 Testing Constraints

The following constraints apply unless the Client provides explicit written authorization to the contrary:

- No denial-of-service (DoS) testing or intentional service disruption.
- No physical security testing or social engineering.
- No testing of systems outside the 10.1.1.0/24 subnet or the single in-scope domain controller (DC01).
- Any hosts discovered on 10.1.1.0/24 other than DC01 are considered out of scope unless explicitly authorized in writing by the Client.
- No modification or deletion of production data.
- No introduction of persistent backdoors or implants that survive engagement conclusion.
- Testing will not intentionally disrupt business operations, scheduled maintenance, or production workloads.

## 5. Scope of Work

### 5.1 In-Scope Target

This engagement has a single in-scope target: the domain controller for the navigatingsecurity.corp domain.

| Category | Description |
|---|---|
| Internal IP Range | 10.1.1.0/24 (for host discovery only; see Section 5.3) |
| Active Directory Domain | navigatingsecurity.corp |
| Domain Controller | DC01 ( Windows Server 2019) |
| Certificate Services (ADCS) | Installed on DC01 - single-tier CA |
| DNS / DHCP | Hosted on DC01 (AD-integrated DNS) |
| Endpoint Protection Platform | EDR (active blocking mode) |

## 5.2 In-Scope Active Directory Components

The following AD components hosted on DC01 are explicitly included in the testing scope:

- Domain user accounts, groups, and organizational units (OUs)
- Group Policy Objects (GPOs) and their security configurations
- Kerberos authentication configuration, delegation settings, and SPN mappings
- Active Directory Certificate Services (ADCS) templates and enrollment policies
- LAPS deployment and configuration
- AdminSDHolder, Protected Users group, and privileged access controls
- DNS records and zone configurations within AD-integrated DNS
- SYSVOL and NETLOGON share contents

## 5.3 Out-of-Scope Assets

**Critical: Scope is Limited to DC01**

This engagement is scoped exclusively to DC01 and the Active Directory domain it hosts. TadiSec is authorized to perform host discovery scanning across 10.1.1.0/24 to map the network, but all hosts other than DC01 are out of scope for exploitation and interaction; none intrusive enumeration is permitted. If an attack path traverses a non-DC01 host, TadiSec will document the path and halt exploitation at the boundary.

| Asset / System | Reason for Exclusion |
|---|---|
| All hosts on 10.1.1.0/24 other than DC01 | Not authorized - engagement scoped to DC01 only |
| 10.1.1.1 (Network Gateway / Firewall) | Network infrastructure - disruption risk |
| Any IP outside 10.1.1.0/24 | Not authorized - outside engagement scope |
| Azure AD / Microsoft 365 / Cloud tenants | Cloud identity not in scope for this engagement |
| File servers, database servers, workstations | Not authorized |

### 5.4 Scope Change Procedure

Any modification to the scope defined in this section requires written approval from both Rumbidzai Moyo (TadiSec Project Lead) and Oliver Whitaker (Client Primary POC). Scope changes may affect the engagement timeline, deliverables, and pricing. TadiSec will provide a written assessment of impact before any scope change is executed.

If during testing TadiSec identifies a critical vulnerability on an out-of-scope system that poses immediate risk to the Client, TadiSec will notify Cathy Williams (Emergency POC) immediately and will not proceed with exploitation without explicit written authorization.

## 6. Rules of Engagement

### 6.1 Authorization

All testing activities described in this SOW are authorized by Oliver Whitaker, Chief Information Security Officer, Navigating Security Corp. TadiSec will not commence testing until both parties have executed this SOW.

### 6.2 Testing Windows

| Parameter | Detail |
|---|---|
| Primary Testing Hours | Monday–Friday, 9:00 AM – 6:00 PM EST |
| Extended / Off-Hours Testing | Permitted with 24-hour written notice to Aarav Patel |
| Weekend Testing | Not permitted |
| Blackout Periods | Month-end processing: March 30–31, 2026 (testing paused) |
| High-Risk Testing Window | Saturday 2:00 AM – 6:00 AM EST (available upon request for Responder/relay testing) |

### 6.3 Communication Protocols

- **Daily Status Updates:** TadiSec will provide a brief written status update via the shared Microsoft Teams channel ("TadiSec × NavSec - Pentest") at the end of each testing day.
- **Critical/Emergency Finding:** TadiSec will notify Cathy Williams (Emergency POC) by phone within 1 hour of discovery, followed by a written summary within 4 hours.
- **Communication Channel:** Microsoft Teams for daily coordination; encrypted email (PGP) for report delivery and sensitive findings.

### 6.4 Credential Handling

The Client will provide TadiSec with the following credentials at the start of the engagement:

| Account | Privilege Level | Purpose |
|---|---|---|
| t.chigubhu | Standard Domain User (Domain Users only) | Assumed breach starting position for lead tester Tonderai Chigubhu |

| | | |
|---|---|---|
| VPN credentials (if remote) | Network access to 10.1.1.0/24 | Connectivity to internal environment from TadiSec office |

TadiSec will not be provided with elevated or administrative credentials. Privilege escalation to Domain Admin or equivalent is a testing objective, not a starting condition.

### 6.5 De-confliction

- **TadiSec Source IPs:** All testing will originate from the TadiSec VPN endpoint IP provided during kickoff. The Client SOC will be informed prior to testing.
- **Testing Hostnames:** The tester is to clearly note the IP address provided for testing in the report.
- **SOC Notification:** Alert but No Response posture - the SOC will monitor and log TadiSec activity but will not take blocking or isolation actions.

## 7. Emergency Contacts & Escalation Procedures

### 7.1 Unintended Service Disruption

1. TadiSec immediately halts all testing activity.
2. TadiSec contacts Cathy Williams (Emergency POC) by phone within 15 minutes.
3. TadiSec provides a written incident summary within 2 hours.
4. Testing resumes only after written authorization from Oliver Whitaker.

### 7.2 Discovery of Active Compromise

1. TadiSec immediately ceases activity that may disturb forensic evidence.
2. TadiSec contacts Cathy Williams by phone immediately.
3. TadiSec provides all relevant IOCs to the Client.
4. Testing scope and timeline are re-evaluated jointly.

### 7.3 Emergency Contact Card

| Role | Name | Phone | Email | Availability |
|---|---|---|---|---|
| Client Emergency POC | Cathy Williams | +1 (212) 555-0199 | c.williams@navseccorp.com | 24/7 during testing |
| Client IT On-Call | Aarav Patel | +1 (212) 555-0162 | a.patel@navseccorp.com | Business hours |
| TadiSec Engagement Lead | Rumbidzai Moyo | +263 77 234 8901 | r.moyo@tadisec.co.zw | Testing hours |
| TadiSec Emergency Line | - | +263 86 770 0100 | - | Business hours |

# 8. Testing Schedule

## 8.1 Engagement Timeline

| Phase | Dates | Duration | Notes |
|---|---|---|---|
| Pre-Engagement & Kickoff | March 23, 2026 | 1 day | Kickoff call, credential provisioning, VPN setup, SOC notification |
| Reconnaissance & Enumeration | March 24–25, 2026 | 2 days | Host discovery across /24; DC01 enumeration |
| Vulnerability Discovery & Exploitation | March 26–27, 2026 | 2 days | Primary testing phase against DC01 |
| Privilege Escalation | April 1–2, 2026 | 2 days | March 30–31 blackout; resumes April 1 |
| Post-Exploitation & Cleanup | April 3, 2026 | 1 day | Impact validation, remove artifacts, finalize evidence |
| Report Writing | April 6–10, 2026 | 5 business days | Off-site, no active testing |
| Draft Report Delivery | April 10, 2026 | | |
| Client Review Period | April 13–17, 2026 | 5 business days | |
| Final Report Delivery | April 21, 2026 | | |
| Readout Presentation | April 23, 2026 | 1–2 hours | Live presentation and Q&A |

## 8.2 Kickoff Meeting

A formal kickoff meeting will be conducted on March 23, 2026 via Microsoft Teams. Agenda:

- Confirmation of scope (DC01 on 10.1.1.0/24), objectives, and testing windows
- Credential delivery for t.chigubhu and VPN access verification
- Emergency contact and escalation procedure review
- SOC notification and de-confliction confirmation

# 9. Deliverables & Reporting

## 9.1 Deliverables Summary

| # | Deliverable | Format | Due Date |
|---|---|---|---|
| 1 | Daily Status Updates | Teams Channel Post | End of each testing day |
| 2 | Draft Penetration Test Report | PDF | April 10, 2026 |
| 3 | Final Penetration Test Report | PDF | April 21, 2026 |

| | | | |
|---|---|---|---|
| 4 | Executive Summary | PDF (included in report) | Delivered with Final Report |
| 5 | Findings Readout Presentation | Live session + report (PDF) | April 23, 2026 |
| 6 | Raw Evidence Package (if any) | Encrypted ZIP | Delivered with Final Report |
| 7 | Remediation Verification (Optional) | PDF addendum | Within 60 days of Final Report |

### 9.2 Report Contents

- **Executive Summary:** Non-technical overview for C-suite and board-level stakeholders.
- **Scope & Methodology:** Description of what was tested, how, and any constraints.
- **Attack Narrative:** Chronological walkthrough of the attack chain from t.chigubhu through domain compromise (if achieved).
- **Technical Findings:** Each finding with CVSS v3.1 severity, description, affected systems, evidence, business impact, and remediation guidance.
- **Remediation Guidance:** Specific, actionable steps prioritized by severity and business context.

| Rating | CVSS Score | Description |
|---|---|---|
| Critical | 9.0 – 10.0 | Trivial exploitation leading to full compromise. |
| High | 7.0 – 8.9 | Likely exploitation with significant impact. |
| Medium | 4.0 – 6.9 | Moderate skill required; meaningful impact. |
| Low | 0.1 – 3.9 | Limited impact or difficult exploitation. |
| Informational | N/A | Best-practice recommendations. |

### 9.3 Acceptance Criteria

The Client shall have five (5) business days from receipt of the Draft Report to review and provide written feedback. If no feedback is received by April 17, 2026, the Draft Report will be considered accepted.

### 9.4 Remediation Verification (Optional)

If purchased as an add-on, TadiSec will conduct a targeted re-test within 60 calendar days of Final Report delivery (by June 20, 2026).

## 10. Data Handling, Retention & Destruction

All data collected during the engagement is classified as Confidential.

- All testing data stored on encrypted, TadiSec-controlled systems (AES-256).
- Credentials stored in Bitwarden; never transmitted via unencrypted channels.

- Data transfers use encrypted channels (TLS 1.2+, SFTP, or Teams).

### 10.1 Retention Period

TadiSec will retain engagement data for 90 days following delivery of the Final Report (until July 20, 2026), after which all data will be securely destroyed.

### 10.2 Destruction Method

Secure wipe in accordance with industry standard guidelines. Certificate of Data Destruction provided upon request.

### 10.3 Cleanup

Upon completion of active testing on April 3, 2026, TadiSec will remove all tools, scripts, and artifacts from DC01. Any changes made during testing will be documented and reversed.

If any artifacts are left over, TadiSec will note these in the report for NavSec Corp to remove.

## 11. Backups & Risk Acceptance

### 11.1 Backup Confirmation

| System | Backup Completed? | Backup Date | Verified By |
|---|---|---|---|
| DC01 (Domain Controller) | Yes | March 21, 2026 | Aarav Patel |

> **Important**
> TadiSec reserves the right to pause or decline testing if the Client cannot confirm that an adequate backup of DC01 is in place. As DC01 is the sole domain controller, any instability could impact all domain services.

### 11.2 Risk Acknowledgment

Penetration testing inherently involves controlled exploitation and may cause unintended effects. The Client acknowledges and accepts the inherent risk. TadiSec will exercise heightened caution given the single-DC environment.

## 12. Compliance Considerations

The following compliance frameworks are relevant to this engagement:

- SOC 2 Type II - Security, availability, and confidentiality trust service criteria
- Applicable state privacy regulations - PII handling and breach notification requirements

If TadiSec encounters personally identifiable information (PII) during testing, it will be documented as an access finding with redacted evidence. No PII will be exfiltrated from the Client environment.

## 13. Client Responsibilities

- Signed SOW and MSA prior to testing.
- Domain user account (t.chigubhu) provisioned and tested prior to kickoff on March 23, 2026.
- VPN connectivity configured and verified prior to kickoff.
- Network documentation for 10.1.1.0/24 and DC01 configuration details.
- SOC notification of engagement window and TadiSec source indicators.
- Backup confirmation for DC01 per Section 11.1.
- Oliver Whitaker and Aarav Patel available within 4 business hours during testing.
- Cathy Williams reachable by phone during testing hours.
- Timely review of Draft Report within the 5-business-day window (April 10–17, 2026).

# 14. Pricing & Payment Terms

## 14.1 Engagement Pricing

| Line Item | Description | Price |
|---|---|---|
| 1 | Internal Network & AD Penetration Test (8 business days, report, and readout) | $22,000.00 |
| 2 | Remediation Verification Re-Test (Optional) | $3,800.00 |
| 3 | Additional Testing Days (if scope expansion approved) | $2,500.00 per day |
| | Total (Line Item 1 only) | $22,000.00 |

All pricing is inclusive of personnel, tools, licensing, and report production. No additional fees without prior written approval.

## 14.2 Payment Schedule

| Milestone | Amount | Due |
|---|---|---|
| Engagement deposit upon SOW execution | 50% ($11,000.00) | Upon execution |
| Final payment upon Final Report acceptance | 50% ($11,000.00) | Net 30 from invoice |
| Remediation Verification (if applicable) | $3,800.00 | Net 30 from invoice |

## 14.3 Invoicing

Invoices will be submitted to accounts@navseccorp.com and copied to Oliver Whitaker. Each invoice will reference TDSC-SOW-2026-001.

# 15. Confidentiality & Non-Disclosure

- TadiSec will not disclose any NavSec Corp information to any third party without prior written consent.
- NavSec Corp will not disclose TadiSec's proprietary methodology, tooling, or pricing without prior written consent.
- Both parties agree that the existence and terms of this engagement are confidential.

# 16. Assumptions & Constraints

- The Client's internal network (10.1.1.0/24) is accessible from the testing location with sufficient bandwidth.
- The t.chigubhu domain user credentials will be valid and functional at the start of testing.
- The AD environment is single-forest, single-domain (navigatingsecurity.corp) with one domain controller (DC01).

- EDR is in normal production configuration (active blocking mode).
- The Client will not make significant infrastructure changes during the testing window without notifying TadiSec.
- The single-DC environment means any instability on DC01 impacts all domain services. TadiSec will exercise heightened caution.
- Only DC01 is authorized for testing. All other hosts discovered on the subnet are out of scope.

## 17. Limitations & Disclaimers

A penetration test is a point-in-time assessment and does not guarantee discovery of all vulnerabilities. The absence of a finding does not confirm the absence of a vulnerability.

This engagement does not constitute a compliance audit or certification. Findings may support SOC 2 objectives but do not certify compliance.

## 18. Term & Termination

This SOW is effective upon execution by both parties. Anticipated period of performance: March 12, 2026 through June 20, 2026 (inclusive of optional remediation verification window).

Either party may terminate with written notice per the MSA. In the event of early termination, NavSec Corp shall compensate TadiSec for all work completed through the date of termination.

## 19. Client-Provided Documentation

- Network diagram for 10.1.1.0/24 showing DC01 location
- AD domain topology (single-domain, single-forest confirmation)
- EDR deployment architecture and policy configuration
- Current password policy and account lockout settings
- Any recent vulnerability scan reports or prior pentest reports

## 20. Acceptance & Authorization

By signing below, both parties approve this Statement of Work and authorize TadiSec to perform the penetration testing services described herein.

### TadiSec - Authorized Representative

**Name:** Rumbidzai Moyo

**Title:** Principal Consultant

**Signature:** _____RMoyoooo_____

**Date:** _____03/10/2026_____

### Navigating Security Corp. - Authorized Representative

**Name:** Oliver Whitaker

**Title:** Chief Information Security Officer

**Signature:** _____OW_____

**Date:** _____03/11/2026_____

*- End of Statement of Work -*