SOP-SEC-001_Defender_Training_v1.0.0

SOP-SEC-001_Defender_Training_v1.0.0

Standard Operating Procedure: Microsoft Defender Attack Training Simulation

Document ID	SOP-SEC-001
Version	1.0
Status	Final
Date	2025-12-02
Owner	IT Security Department

1.0 Purpose

To establish a standardized process for conducting Microsoft Defender Attack Training Simulations for clients. The primary objectives of this procedure are: - To educate client personnel on the identification and risks of phishing emails. - To demonstrate the capabilities and operation of the Microsoft Defender Attack Simulation tool. - To collaboratively plan, schedule, and execute attack simulations. - To review simulation results and provide actionable recommendations for improving security posture.

2.0 Scope

This SOP applies to all IT personnel involved in the planning and execution of client-facing security training initiatives. It specifically governs the Microsoft Defender Attack Training Simulation sessions conducted for clients and their designated security and technical teams.

3.0 Responsibilities

Role	Responsibility
Presenter (Phishing Identification)	Responsible for developing and delivering the educational presentation on identifying phishing attempts, including real-world examples and best practices.
Presenter (Simulation Overview)	Responsible for presenting the overview, benefits, and demonstration of the Microsoft Defender Attack Simulation platform.
Moderator/Facilitator	Responsible for leading the training session, managing the agenda, facilitating discussions, and ensuring session objectives are met.
Client Representative(s)	Responsible for collaborating on the scheduling and structure of simulations, providing relevant technical context, and participating in the training.
All Participants	Responsible for confirming availability for the scheduled session and reviewing any pre-shared materials.

4.0 Definitions

Term	Definition
Phishing	A fraudulent attempt, usually made through email, to deceive individuals into revealing sensitive information such as usernames, passwords, and credit card details.
Attack Simulation	A feature within Microsoft Defender used to run realistic, benign cyberattack scenarios (e.g., phishing campaigns) within an organization to test security policies and employee awareness.

5.0 Procedure

5.1 Phase 1: Preparation and Scheduling

1. **Identify Participants:** The Moderator will identify and list the key participants from both the internal team and the client's team.

2. **Propose Dates:** The Moderator will propose a minimum of three potential dates for the training session to the client.
3. **Finalize Schedule:** Based on participant feedback and client convenience, the Moderator will finalize and confirm the session date and time.
4. **Collaborate on Logistics:** The Moderator and Presenters will engage with the client's technical team to discuss the initial structure, focus areas, and goals for the attack simulation.
5. **Prepare Materials:** The designated Presenters will prepare their respective presentation materials (Phishing Identification and Defender Simulation Overview).
6. **Distribute Materials:** The Moderator will share the agenda and any relevant presentation materials with all participants ahead of the scheduled session.

5.2 Phase 2: Training Session Execution

The training session will follow the structured agenda below:

Part 1: Welcome and Introductions (10 min) - The Moderator officially starts the meeting and welcomes all attendees. - Each participant briefly introduces themselves and their role. - The Moderator reviews the objectives and agenda for the session.

Part 2: Presentation on Identifying Phishing Emails (20 min) - The designated Presenter conducts a detailed presentation covering: - Key characteristics and red flags of phishing emails. - Analysis of real-world phishing examples. - Actionable tips and best practices for employees to recognize and report phishing attempts.

Part 3: Presentation on Microsoft Defender Attack Simulation (20 min) - The designated Presenter conducts a presentation and demonstration covering: - An overview of the attack simulation concept and its value. - The operational mechanics and benefits of the Microsoft Defender tool. - A live demonstration of how to configure and set up a new simulation.

5.3 Technical Procedure: Creating an Attack Simulation

Prerequisites: - Microsoft 365 E5 or Microsoft Defender for Office 365 Plan 2 license - Membership in Security Administrator or Attack Simulation Administrator role

Step-by-Step Configuration:

1. **Access the Security Portal:**
    - Navigate to: **security.microsoft.com**
    - Go to: **Email & collaboration > Attack simulation training**
2. **Launch New Simulation:**
    - Click **Simulations** tab
    - Click **+ Launch a simulation**

3. **Select Technique:**
    - Choose attack type: | Technique | Description | |———|————-| | **Credential Harvest** | Fake login page to capture credentials | | **Malware Attachment** | Simulated malicious attachment | | **Link in Attachment** | Malicious link inside a document | | **Link to Malware** | Link that would download malware | | **Drive-by URL** | Link to compromised website |
4. **Select Payload:**
    - Choose from built-in payloads or create custom
    - Preview the email and landing page
    - Recommended: Start with "Global" payloads for realistic scenarios
5. **Configure Target Users:**
    - **All users** - Full organization test
    - **Specific users/groups** - Targeted departments
    - Recommended: Start with IT department as pilot
6. **Assign Training:**
    - Select training modules for users who fail
    - Set training due date (recommended: 7-14 days)
    - Enable training reminders
7. **Schedule Simulation:**
    - Set launch date and time
    - Set simulation duration (recommended: 7-30 days)
    - Enable/disable repeat offender tracking
8. **Review and Launch:**
    - Review all settings
    - Click **Submit** to launch simulation

Post-Simulation Analysis:

1. **View Results:**

    - **Simulations** > Select simulation > **Report**

2. **Key Metrics:** | Metric | Definition | Target | |——|————|——| | Compromised rate | Users who clicked + entered credentials | <10% | | Click rate | Users who clicked the link | <20% | | Reported rate | Users who reported the email | >30% |

3. **Export Report:**

    - Click **Export** for detailed CSV with user-level data

Part 4: Collaborative Simulation Workshop (60 min) - The Moderator facilitates a collaborative working session with the client team. - **Action:** Collaboratively schedule the first official attack simulation. - **Action:** Define the structure, payloads, and target groups for the simulation. - **Action:** Establish a timeline and cadence for future, ongoing training sessions.

Part 5: Initial Simulation Results Review (20 min, *if applicable*) - If a preliminary simulation has been conducted, the Presenter will share the initial results. - The team will discuss the implications of the findings and potential areas for improvement. - A Q&A session is held to address any questions regarding the results.

Part 6: Wrap-Up and Next Steps (10 min) - The Moderator summarizes the key decisions and takeaways from the session. - The Moderator confirms the schedule for the first simulation and any subsequent follow-up sessions.

6.0 Troubleshooting

Issue	Cause	Resolution
Cannot access Attack Simulation Training	Insufficient license or permissions	Requires M365 E5 or Defender for Office 365 P2. Verify user has Security Administrator or Attack Simulation Administrator role.
Simulation emails not delivered	Mail flow rules or spam filters	Check Exchange mail flow rules. Verify simulation sender domain not blocked. Check quarantine for simulation emails.
Users report simulation as real phishing	Simulation too realistic or no awareness	Brief users that simulations will occur (without specifics). Add internal banner to simulation emails.
Low click rates (too low to be real)	Users forwarding warnings or tech-savvy audience	Vary simulation timing. Use different payload types. Consider targeted simulations.
Training assignments not appearing	User not in target group or sync delay	Verify user in simulation target. Wait 24 hours for sync. Check user mailbox is active.
Simulation results show 0%	Simulation not started or wrong date range	Verify simulation status is “Completed”. Check date filters in report.
Cannot create custom payload	Permission or template issue	Verify Attack Simulation Administrator role. Start with modifying existing payload.
Users cannot access training	Training URL blocked or license issue	Whitelist `*.safelinks.protection.outlook.com` and `*.microsoft.com`. Verify user has license.
Repeat offenders not tracked	Feature not enabled	Enable “Repeat offender” tracking in simulation settings. Runs across multiple simulations.

Issue	Cause	Resolution
Simulation scheduled but not launching	Time zone mismatch or approval pending	Verify time zone settings. Check if approval workflow is blocking.

Pre-Simulation Checklist: - [ ] Verify M365 E5 or Defender P2 licensing - [ ] Confirm admin roles assigned - [ ] Test email delivery to pilot group - [ ] Whitelist simulation domains if needed - [ ] Brief IT helpdesk about upcoming simulation - [ ] Prepare response for users who report simulation

Useful URLs: - Security Portal: https://security.microsoft.com - Attack Simulation: https://security.microsoft.com/attacksimulator - Training Modules: https://security.microsoft.com/trainingassignments

7.0 References

- Microsoft Defender for Office 365 Documentation
- `Microsoft Defender Attack Training Simulation Presentation Plan.docx`
- Microsoft Security Portal: https://security.microsoft.com

8.0 Revision History

Version	Date	Author	Description
1.0	2025-12-02	IT Security Department	Initial document creation.
1.1	2025-12-29	Jeremy Smith	SME Review: Added Section 5.3 (Technical Procedure for creating simulations). Added Section 6.0 (Troubleshooting) with common issues and pre-simulation checklist.