BISHOPFOX

WHAT TO
EXPECT

WORKPLACE FROM FACEBOOK SECURITY ASSESSMENT

MAY 2021

PROPRIETARY INFORMATION

TABLE OF CONTENTS

01

OVERVIEW

A little bit about us.

OUR PURPOSE:

SUPPORTING PARTNER & CUSTOMER SECURITY

———

The **Workplace from Facebook Security Program** is a collaborative effort to protect partner, customer, and Facebook data by increasing the security of partner ISV's application that integrate with the Facebook Workplace ecosystem.

Facebook has engaged Bishop Fox to conduct appropriate security testing with the goal of validating the security of Facebook Workplace ISVs' applications and **ensuring Workplace user data is being handled securely.**

Bishop Fox's main goal is to help you complete the Facebook Workplace Security Assessment requirements listed on **Workplace Platform Security Program FAQ.**

WHY CHOOSE
BISHOP FOX

Inquiring minds want to know

- **WE DO ONE THING**

  Bishop Fox was founded on the principle that all we do is advise our clients so they can make the best possible security decisions.

» **DEEP EXPERIENCE**

  Our team's technical depth and expertise means we can tailor every solution or project to your unique requirements. We don't just check boxes!

» **SENIOR ATTENTION**

  Partners and senior consultants drive service delivery, and we are committed to every project's success. You won't be handed off to a junior team.

02
ENGAGEMENT MODEL
How we partner with you.

SCOPING THE ASSESSMENT

» ONBOARDING

You will be sent a **scoping survey** to collect initial details about your company and application (including your App name and ID number). If you have questions or need assistance, a call can be scheduled with your Bishop Fox Account Manager.

» SCOPING

A Solutions Architect will use the information from the scoping survey to determine the appropriate testing scope. This is determined on the size, level of data sensitivity and complexity of the application and environment, so it is important to fill out the survey accurately and provide documentation where possible

Note: Please exclude test code and 3rd party code from the line of code count where possible, this helps prevent over-scoping.

» NEXT STEPS

A Bishop Fox account manager will reach out to your team with an estimated quote. Once pricing is agreed on, a statement of work will be sent over for your review. After signing, your account manager/account liaison will facilitate introductions to the engagement management team to start on the collection of project enablement requirements.

SCOPING SURVEY:

PRE-ENGAGEMENT

Sample list of items needed to begin the assessment:

PROJECT ENABLEMENT REQUIREMENTS (Test environment needed prior to project start)	RFI (SELF-ASSESSMENT QUESTIONNAIRE)	APPLICATION PENETRATION TESTING
Test environment URLs / IP Addresses	Please begin to fill out your RFI (not required to start assessment)	Please provide testing application environment URL in scope
Credentials / Test Accounts	N/A	3 test accounts per role
Confirm Hosting Environments	Yes	Yes
Documentation, Diagrams, Guides	Required documentation; Incident Response Plan and Data Classification Policy	Optional; Documentation on user functionality and documentation on APIs

FIELDWORK

❯❯ REMOTE TESTING

All testing will be performed remotely unless otherwise an exception is granted and determined in advance.

❯❯ COLLABORATIVE APPROACH

Our testing approach is collaborative with partners (instead of adversarial). We are performing time-limited penetration testing to find as many potential security issues as possible, with a focus on validating a minimum level of capability in handling data securely (see project activities for more detail).

❯❯ STATUS UPDATES

During testing, Bishop Fox team will provide weekly status updates to your team. Status updates will include completed tasks, preliminary findings, current activities, and planned activities. Any escalations outside of weekly updates will be handled in accordance with pre-defined escalation procedures.

DELIVERABLES AND REMEDIATION TESTING

ASSESSMENT REPORT

The report includes an executive summary detailing a project overview, project scope, summary of findings, and strategic next steps. The Assessment Report will include a review of the methodology, technical findings including vulnerability description, severity level, affected systems, business and technical impact, remediation recommendations, and walkthrough of exploitation with screenshots if applicable.

REPORT WALKTHROUGH

Bishop Fox will walk through the report with the partner team and any relevant stakeholders. Walkthrough includes a review of the project approach and scope, discussion of individual findings and recommendations, and guidance on next steps.

REMEDIATION TESTING

Once the partner has remediated any vulnerabilities found during testing, Bishop Fox will perform one (1) round of remediation testing to validate the issues are fully resolved. Remediation must be requested after fieldwork has been completed and within 30 days of report delivery.

TESTING LETTER

All Testing Letters will be issued at Bishop Fox's discretion and submitted to Facebook by Bishop Fox.

TESTING LETTER FAQ

- Bishop Fox will author a testing letter to serve as evidence to Facebook if the following qualification have been met. This includes:

- This letter includes an engagement overview, services or activities performed (i.e., reference the Facebook testing requirements), testing dates, testing environment, list of testing targets and …..

- Testing letters are valid for 12 months after the issue date.

ANNUAL TESTING EFFICIENCIES

- Bishop Fox can rescope the ISV's testing environment following the same scoping process with the added benefit of prior data and testing notes.

- Bishop Fox will **keep track of each ISV's scoping information from year to year** and leverage this data when scoping subsequent testing projects. This has the benefit of potentially reducing effort required for follow-on testing.

- Any relevant testing notes taken during the initial project will be archived by Bishop Fox for follow-on testing to **reduce ramp up time for Bishop Fox consultants**.

- Previously developed test harnesses or testing scenarios will be re-used or repurposed to **improve testing efficiency**.

03

FAQs

You have questions, we have answers.

FREQUENTLY ASKED QUESTIONS

- ### HOW MUCH WILL THE ASSESSMENT COST?

  Cost is between $10,000 and $20,000 + depending on the size of the application, size of the environment, and the sensitivity level of Facebook user data is utilized.

- ### WHEN WILL THE ASSESSMENT START?

  After SOW is signed, it typically will take approximately 4 weeks to staff the assessment. During that time, we will request ISV will provide full project enablement items (e.g., test environment that mirrors prod, credentials, test accounts, documentation, etc.) before receiving a start date. This is to ensure that there are no delays to the project schedule.

- ### HOW LONG WILL THE ASSESSMENT TAKE?

  Once all the paperwork is in place, fieldwork can typically take up to 1-2 weeks. After that, reporting and QA can take up to 1 week for assessment report delivery. This does not include remediation time.

FREQUENTLY ASKED QUESTIONS

- **WHAT WILL THE SCOPE OF THE TESTING BE?**

   The focus of the penetration testing will be on:

   - o **Application Penetration Testing**
   - o **Security RFI** - We will evaluate the effectiveness of the ISV's security practices and procedures across a breath of areas, including data handling, secure software development, and vulnerability management.

- **WHAT WILL THE SCOPING INFORMATION BE USED FOR?**

   Information shared with us for scoping will be used to determine overall effort required and also shorten the ramp up time needed for testing. If we can understand the environment before testing, we can spend less time on discovery/foot printing and more time and on active pen testing. The more accurate the scoping details are, the more accurate and cost sensitive we can be with the scope and quote.

- **DO I NEED TO PROVIDE SOURCE CODE?**

   We'll leave that up to you. If you want to provide source code, it can help us be more efficient with our time and get to a deeper level of testing. That said, source code is not required for this assessment.

FREQUENTLY ASKED QUESTIONS

- **HOW LONG DOES REMEDIATION TAKE?**

  Typically, about 1-2 weeks for remediation testing depending on size of remediation testing.

  ONLY A SMALL PART OF MY APPLICATION USES FACEBOOK XXXXX. DOES IT ALL GET INCLUDED IN SCOPE?

  Yes, unless Workplace customer data is clearly isolated from other parts of your application, we need to test the entire application. If an attacker can exploit one part of your application not directly related to Workplace, that exploit could be used to compromise Workplace customer data.

- **HOW WILL MY SENSITIVE DATA BE HANDLED?**

  All sensitive data including source code will be stored, processed, and transmitted securely. Your Bishop Fox Engagement Manager can help setup a secure file share to use throughout the project.

FREQUENTLY ASKED QUESTIONS

- **WE ARE INTERESTED IN A STANDARD BISHOP FOX LETTER OF ASSESSMENT IN ADDITION TO THE FACEBOOK TESTING LETTER. DOES THIS CHANGE THE SCOPE / COST?**

  Yes, we will need to review the scope and determine if additional testing is required to meet our standards for a general Letter of Assessment in addition to the Facebook Workplace Testing Letter. If you have a particular compliance requirement, please describe it and the framework so we can consider it appropriately in scoping.

04

METHODOLOGIES

Project Activities

APPLICATION PENETRATION TESTING

APPROACH

- **Real-world attack simulation** focused on identification and exploitation

- **Discovery of attack surface**, authorization bypass, and input validation issues

- Automated vulnerability scanning combined with manual validation

- **Exploitation** of software vulnerabilities, insecure configurations, design flaws, and weak authentication

- Analysis of vulnerabilities to validate and develop complex **attack chaining** patterns and custom exploits

SCOPE

- ISV's applications that integrate with a Facebook ecosystem especially those handling sensitive Facebook or customer data

RFI - SELF-ASSESSMENT QUESTIONNAIRE

APPROACH

- Ask **targeted questions** about how the partner organization addresses common threats, based on industry trend reports, CIS CSC Top 20, and Bishop Fox's experience.

- Review self-assessment questionnaire responses, rating responses as met, partially met, or not met based on **standardized evaluation criteria**.

SCOPE

- Internal control environment for all ISV's infrastructure, systems, and relevant applications interfacing with the Facebook ecosystem or handling sensitive customer data

REMEDIATION TESTING

APPROACH

- **Perform remediation testing** against those issues identified by partner as having been remediated.

- **One round of remediation testing** will be performed **after fieldwork is completed** and must be requested **within 30 days after report delivery**.

SCOPE

- Vulnerabilities identified as part of the partner security testing program

NOTE

- Remediation testing can be separately scoped based on final report or built-in to the initial assessment scope. If additional rounds of remediation testing are needed, we can create a change order for the additional days of testing that are required.

- Remediation testing will be performed at the end of the assessment **once all required fixes** have been completed. This helps keep the assessment schedule on track and ensures fieldwork hours go towards completing the assessment work.

GET IN TOUCH
WITH US

bishopfox.com/facebook

THANK
YOU