BISHOPFOX

WHAT TO EXPECT

GOOGLE PARTNER SECURITY ASSESSMENT

JUNE 2019

PROPRIETARY INFORMATION

TABLE OF **CONTENTS**

01

OVERVIEW

A little bit about us.

OUR PURPOSE:
SUPPORTING PARTNER & CUSTOMER SECURITY

The **Google Partner Security Program** is a collaborative effort to protect partner, customer, and Google data by increasing the security of Google partners' applications and networks that integrate with the Google ecosystems.

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

Bishop Fox's main goal is to help you complete the Security Assessment requirements listed on OAuth Application Verification FAQ.

WHY CHOOSE BISHOP FOX

Inquiring minds want to know

WE DESIGNED THE PROGRAM

Bishop Fox collaborated closely with Google to design the Partner security program, so we know what's needed for you will to pass the testing requirements.

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.

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

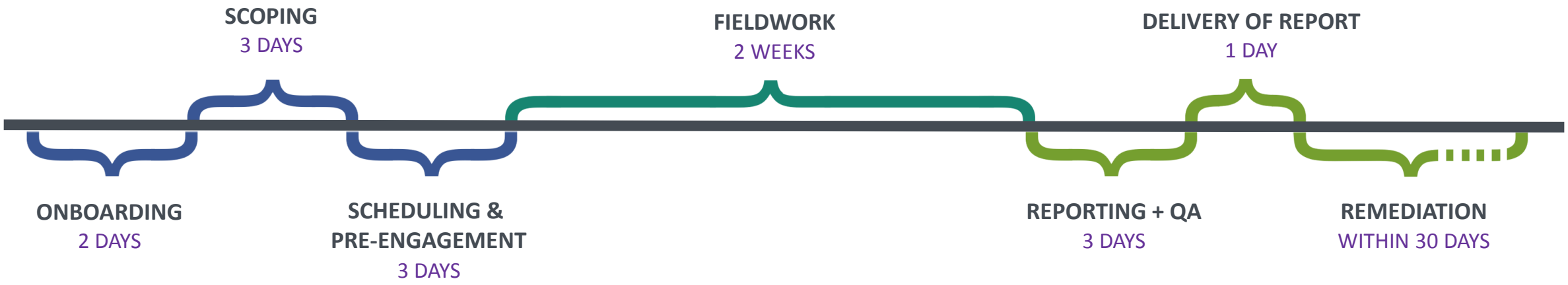
ENGAGEMENT MODEL

How we partner with you.

PROJECT ACTIVITIES

PROJECT TIMELINE

Estimated timeline based on average engagement size



KEY POINTS

SCOPING THE ASSESSMENT

ONBOARDING

A Bishop Fox account manager will work with you to complete a scoping survey and collect initial details about your company and application to be used for onboarding.

SCOPING

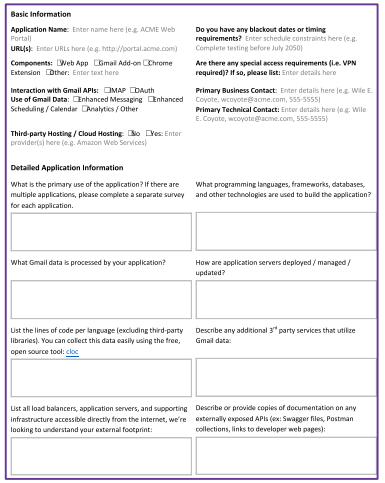
A Solutions Architect will use the information from the scoping survey to determine the appropriate testing scope. This is determined on the size and complexity of the application and environment, so it is important to fill out the survey accurately and provide documentation where possible

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

SCHEDULING

A Bishop Fox account manager will reach out to your team with an estimated quote and scheduling options.

SCOPING SURVEY:



Basic Information

Application Name: Enter name here (e.g. ACME Web Portal)
URL(s): Enter URLs here (e.g. http://portal.acme.com)
Components: ☐Web App ☐Gmail Add-on ☐Chrome Extension ☐Other: Enter text here
Interaction with Gmail APIs: ☐IMAP ☐OAuth
Use of Gmail Data: ☐Enhanced Messaging ☐Enhanced Scheduling / Calendar ☐Analytics / Other
Third-party Hosting / Cloud Hosting: ☐No ☐Yes: Enter provider(s) here (e.g. Amazon Web Services)
Do you have any blackout dates or timing requirements? Enter schedule constraints here (e.g. Complete testing before July 2050)
Are there any special access requirements (i.e. VPN required)? If so, please list: Enter details here
Primary Business Contact: Enter details here (e.g. Wile E. Coyote, wcoyote@acme.com, 555-5555)
Primary Technical Contact: Enter details here (e.g. Wile E. Coyote, wcoyote@acme.com, 555-5555)

Detailed Application Information

What is the primary use of the application? If there are multiple applications, please complete a separate survey for each application.

What programming languages, frameworks, databases, and other technologies are used to build the application?

What Gmail data is processed by your application?

How are application servers deployed / managed / updated?

List the lines of code per language (excluding third-party libraries). You can collect this data easily using the free, open source tool: cloc

Describe any additional 3rd party services that utilize Gmail data:

List all load balancers, application servers, and supporting infrastructure accessible directly from the Internet, we're looking to understand your external footprint:

Describe or provide copies of documentation on any externally exposed APIs (ex: Swagger files, Postman collections, links to developer web pages):

GETTING READY FOR THE ASSESSMENT

PRE-ENGAGEMENT

Sample list of items needed to begin the assessment:

PRE-ENGAGEMENT REQUIREMENTS (Needed prior to project start)	**EXTERNAL PENETRATION TESTING**	**APPLICATION PENETRATION TESTING**
URLs / IP Addresses	Please provide the IP addresses in scope, along with registered domains and subdomains	Please provide Application URL
Credentials / Test Accounts	N/A	3 test accounts per role
Confirm Hosting Environments	Yes	Yes
Documentation, Diagrams, Guides	Optional; Network diagram or relevant external network documentation	Optional; Documentation on user functionality and documentation on APIs

DURING THE ASSESSMENT

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.

WRAPPING UP THE ASSESSMENT

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 walkthrough 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 also 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.

HOW TO QUALIFY

TESTING LETTER FAQ

- Bishop Fox will author a testing letter to serve as evidence to Google if the following qualification have been met. This includes:
    - Remediation of all critical and high risk issues in order to receive a testing letter
        - This includes any critical or high risk issues found during the deployment and SAQ reviews.
    - Medium risk issues must be remediated before the next annual testing period
    - Low and Informational issues are optional to be fixed
- This letter includes an engagement overview, services or activities performed (i.e. reference the Google testing requirements), testing dates, testing environment, and list of testing targets.
- Testing letters are valid for 12 months after the issue date.

PLANNING AHEAD FOR NEXT YEAR

ANNUAL TESTING EFFICIENCIES

- Bishop Fox can rescope the partner testing environment following the same scoping process with the added benefit of prior data and testing notes.
- Bishop Fox will **keep track of each partners 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?**

  We have negotiated discounted pricing with Google for this program, and the cost is between $15,000 - $75,000 depending on the size of the application, size of the environment, and how Google user data is utilized.

- **WHEN WILL THE ASSESSMENT START?**

  We will work with you to get the project started as quickly as possible, and we can provide you with a few start dates to choose from. Scheduling is typically 2-4 weeks out.

- **HOW LONG WILL THE ASSESSMENT TAKE?**

  Once all the paperwork is in place, fieldwork can typically take 1-4 weeks. After that, reporting and QA can take up to 1 week for report delivery.

FREQUENTLY ASKED QUESTIONS

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

  The focus of the penetration testing will be on the external perimeter internet-facing assets and applications that store Google user data on non-Google servers, a self-assessment questionnaire, and a cloud deployment review.

- **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/footprinting 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.

FREQUENTLY ASKED QUESTIONS

- **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.

- **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.

04

METHODOLOGIES

Project Activities

PROJECT ACTIVITIES

EXTERNAL PENETRATION TESTING

APPROACH

- **Real-world attack simulation** focused on identification and exploitation
- **Discovery and enumeration** of live hosts, open ports, services, unpatched software, administration interfaces, authentication endpoints lacking MFA, and other external-facing assets
- Automated vulnerability scanning combined with manual validation
- **Brute-forcing** of authentication endpoints, directory listings, and other external assets
- Analysis of vulnerabilities to validate and develop complex **attack chaining** patterns and custom exploits
- **Exploitation of software** vulnerabilities, insecure configurations, and design flaws

SCOPE

- External, internet-facing infrastructure, systems, and relevant applications interfacing with the Google ecosystem and/or handling sensitive customer data

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

- Partner applications that integrate with a Google ecosystem especially those handling sensitive Google or customer data

PROJECT ACTIVITIES

CLOUD DEPLOYMENT REVIEW

APPROACH

- Gather all available cloud configuration settings and metadata
- Identify gaps or deviations from accepted cloud provider's security best practices

SCOPE

- Cloud environment for all partner infrastructure, systems, and relevant applications interfacing with the Google ecosystem or handling sensitive customer data

PROJECT ACTIVITIES

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 partner infrastructure, systems, and relevant applications interfacing with the Google ecosystem or handling sensitive customer data

PROJECT ACTIVITIES

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

google@bishopfox.com

THANK
YOU