No.28 サービス紹介・全6ページ

3分でわかる

SIMULATE
リスクの検証

SIMULATE を頼むと決める前に、御社が用意するもの・かかる時間・残る成果物を確かめる。分担・見本・質問と答え



Securiy

SIMULATE は、何をして、何が残るか

御社に決めていただくのは、守りたいデータがどれか・気になる操作・検証環境の3つです（データそのものは受け取りません）。
正規のアカウントで、攻撃者が試すように範囲外の操作を試し、成立した経路を再現できる形で記録します。3つのサービスの関係とどれから始めるかは No.06 早わかりに、この資料は SIMULATE を社内で検討するときの材料（準備・分担・成果物）に絞っています。



残るもの: 検証前に合意する一覧と、報告の1ページ目

左は検証前に御社が承認するテスト項目一覧、右は報告書1ページ目のリスク一覧。説明のための架空の例です。

範囲の合意書 別紙 ／ テスト項目一覧　　見本

対象: 説明用アプリ v2.4.1（検証環境）　　承認: 御社の開発責任者

No.	操作	誰として	何を指定して	経路	状態（報告時）
01	顧客一覧の取得	組織 A の一般ユーザー	URL の組織 ID を B に	画面・API・CSV・検索 API	済
02	顧客一覧の取得	組織 A の管理者	退会済み組織の ID	API	済
03	送金先の変更	承認権限のない担当者	承認待ちのまま実行	API	済
04	送金先の変更	担当者	承認後に口座番号を書き換え	画面	済
05	送金先の変更	外部連携キー	連携の範囲外の口座	連携 API	未実施

検証前に御社が承認。試さないもの（本番環境・負荷・削除や破壊・合意外のアカウント）も別紙に書く

検証報告書 1ページ目 ／ リスク一覧　　見本

対象版 v2.4.1 ／ 検証環境　　検証 Day 3〜7

重大度	操作（テスト項目）	結果	影響の範囲	修正候補
高	顧客一覧の取得（01）	成立	画面は拒否。顧客一覧 API・CSV・検索 API で他組織のデータが返る（SIM-003）	要求の組織 ID をセッションの所属と照合
高	送金先の変更（03）	成立	API のみ。画面は承認待ちで止まる（SIM-004）	承認状態をサーバー側で照合
−	顧客一覧の取得（02）	成立せず	退会済み組織は拒否された	—
−	送金先の変更（04）	成立せず	承認後の書き換えは拒否された	—
未	送金先の変更（05）	未実施	連携キーの発行が間に合わず未実施。未検証範囲に記載	—

成立した行ごとに、再現手順つきの検証記録が続く（No.06 P.04）

テスト項目一覧の読み方

「誰として・何を指定して・どの経路で」まで書いてから始めます。試さないものも書くので、検証の範囲が合意書の別紙として残ります。

リスク一覧の読み方

1行目が最初に直すものです。「成立せず」の行は安全の証明ではなく、その操作・経路・版で成立しなかった記録です。「未」の行は未検証範囲として報告書に残ります。

10営業日の分担: 御社にお願いするのは4つと報告会

御社にお願いするのは、検証環境の準備、権限表の確認、テスト項目の承認、報告書の確認の4つと、最終日の報告会への出席です。見つかったものを直す ADAPT のレビューと適用は、別に1件1〜2時間かかります。検証中は、いつでも止められる窓口を決めてから始めます。



準備が整った日を Day 0 として10営業日。報告会は最終日。見積りは着手前に提示し、お断りいただいても構いません。

SIMULATE について、先にお答えしておくこと

検討の段階で確かめておきたいことのうち、SIMULATE に固有のものを先に書きます。年次診断との重なりは上の表のとおりで、診断の見積書と重なる項目は提案から外します。費用・実績・AI へのデータ送信は No.06 早わかり P.08 にあります。

	年次の脆弱性診断	SIMULATE
何を試すか	どのアプリにも共通する脆弱性の型（注入、認可制御の不備など）を網羅的に	**御社と合意した2操作について、「誰として・何を指定して・どの経路で」まで条件を決めて**
試せる範囲	診断時点の版と、渡したアカウント・見積りに入れた画面と API の範囲	**画面・API・CSV・連携キー（外部ツール用の API キー）・AI 機能の経路。診断後に足した操作も対象にできる**
結果の書き方	検出した項目と重大度	**成立した経路は再現手順つき。成立しなかった操作も条件つきで記録し、未検証範囲を書く**

AI が「成立した」と言った結果は、どう確かめますか。

人が同じ手順で再現できたものだけを検証記録に載せます。再現できなかったものは記録に載せず、件数だけを報告書に書きます。

「成立しなかった」は、安全ということですか。

いいえ。試した操作・経路・版に限った結果です。試していない操作と経路は未検証範囲として必ず書き、「安全」の総合判定はしません。

検証環境で成立しなければ、本番も大丈夫ですか。

いいえ。結果は検証した版と環境に限ります。報告書には版と環境を書き、本番と違う設定・版は未検証範囲に入れます。

検証中にサービスが止まりませんか。

合意した検証環境でだけ試します。負荷をかける操作、データの削除や破壊を伴う操作は試しません。止める窓口を先に決め、御社の指示があれば即時に止めます。

ソースコードは必要ですか。

SIMULATE だけなら不要です。見つかったものの修正案を作る段階（ADAPT）で、合意した範囲と方法で拝見します。ご希望があれば秘密保持契約を結びます。

2操作で足りますか。3つ目以降は。

初回の2操作だけでは分かりません。2操作は守りたいデータから事故になる順に選ぶので、影響の大きいところから確かめることになります。残りの操作は、テスト項目一覧の型を使えば御社でも足していけます。外部で続けるかは、初回の結果を見て決めてください。

確かめたい操作を、ひとつ決めるところから。

守りたいデータと気になる操作を書き出し、決めた条件で画面と API から試すところまでは自社でできます（No.09 P.09）。外に出す価値があるのは、まだ決めていない条件と経路（承認内容の書き換え・連携キー・AI 機能）を広く洗い出して試し、試さなかったものも未検証範囲として書いた、取引先に出せる記録にするところです。初回のご相談は30分・無料です。

お申し込み・お問い合わせ　`securiy-preview.pages.dev`　のフォームから
Tempura technologies株式会社

※ すべての攻撃の網羅や「安全」の総合判定は保証しません。金融の規制適合審査、決済基盤全体の監査、カード不正判定は対象外です。

無料相談

30分無料相談

守りたいデータと気になる操作を伺い、初回に検証する2操作とテスト項目の候補を決めます。本番の認証情報や顧客データは不要です。

相談を申し込む →

共同検証プログラムとは

検証テーマを一緒に作る企業に、初回スコープで提供する枠組み

1アプリ・1検証環境・2操作、準備完了後10営業日・合計40時間（修正案と再検証は2件・12時間まで）。費用は着手前に提示します。

次に読む

No.29 ADAPT 修正・再検証の支援 ／ No.06 早わかり

見つかったものを直して確かめる流れと、検証記録1件の中身はこちら。