CAPITOLATO
SERVIZI VULNERABILITY ASSESSMENT/PENETRATION TEST E SECURITY CONSULTING

1. CONTESTO

PagoPA SpA (di seguito, la Società) intende mantenere una elevata postura di sicurezza nell'erogazione dei servizi forniti ad Enti e cittadini, con particolare riferimento a quelli fruibili tramite la piattaforma IO. Pertanto, la Società è alla ricerca di una società terza (di seguito, Fornitore) che possa contribuire a mantenere aggiornato un processo di efficace analisi e valutazione del rischio cyber, soprattutto, quello legato alla violazione della privacy dei PII trasmessi e conservati, tramite l'erogazione di servizi di Vulnerability Assessment / Penetration Test, e Security Consulting.

2. ESIGENZA/OBIETTIVI

Per le ragioni suddette, si intende acquisire da un Fornitore alcuni servizi volti alla verifica della sicurezza e, in particolare, della resilienza ad attacchi e data breach delle app mobile e web della Società, comprensive dei propri backend e del complesso dei servizi erogati.
La forma di fruizione più conveniente per la Società consiste in giornate uomo prestate da un Team di professionisti che il Fornitore dovrà mettere a disposizione secondo necessità; tali giornate saranno amministrativamente organizzate in lotti annuali ed impiegate a consumo secondo un calendario di test periodici stabilito dalla Società, nonché in corrispondenza di richieste estemporanee per esigenze specifiche e contingenti (rilasci di nuove versioni, modifiche alle politiche di sicurezza, ecc.). Il periodo minimo di copertura garantita è di tre anni.
Alla ricerca esaustiva di vulnerabilità così condotta, il servizio dovrà far seguito con il supporto al processo di follow-up attuato dalla Società, ovvero all'individuazione e applicazione delle contromisure atte a evitare i disservizi e la diffusione di dati riservati.
Particolare cura dovrà, inoltre, essere posta alla verifica del rispetto delle compliance, soprattutto, in occasione dell'introduzione di nuovi servizi al cittadino.
Nell'ottica di impedire che attacchi condotti cercando di sfruttare vulnerabilità note alla comunità della sicurezza da settimane o mesi terminino con successo, è fondamentale che il Fornitore componga la propria knowledge-base di vulnerabilità e attacchi impiegando fonti affidabili e autorevoli (il più possibile ufficiali, quali sono i feed rilasciati dai vendor, dai CERT istituzionali e dai laboratori di ricerca). Contestualmente, dovrà essere in grado di attribuire una attenta e circostanziata misura di gravità (quindi, priorità di rimozione) in relazione all'entità del rischio di effettiva sfruttabilità della vulnerabilità e al conseguente impatto tangibile per la Società. In altre parole, si dovrà consentire al team Security della Società di

conseguire una visione pragmatica di ogni vulnerabilità e di dare priorità alle patch in base al valore per la Società.
Si precisa che, per nessuna ragione, il Fornitore dovrà volontariamente o accidentalmente sfruttare le anomalie rilevate per esfiltrare le informazioni contenute negli ambienti di produzione. In generale, tutte le attività compiute dal Fornitore dovranno essere esclusivamente volte a valutare lo stato di sicurezza e la resilienza dei sistemi in uso da parte di PagoPA, senza che ci siano altri fini di ogni sorta. Particolare riguardo, inoltre, dovrà essere posto nella gestione delle informazioni raccolte, le quali andranno consegnate solo ai referenti che la Società indicherà al Fornitore e mai divulgate attraverso altri canali pubblici o privati.
Infine, allo scopo di contestualizzare meglio l'ambito di destinazione del servizio, si indicano nel seguito gli obiettivi ancillari perseguiti dalla Società:

- Svolgere i controlli di sicurezza richiesti per ISO/IEC 27001 nell'ambito del Risk Management, e supporto su eventuali verifiche di specifici standard (es. PCI-DSS);
- Massimizzare il ROI degli investimenti di sicurezza;
- Confermare il livello di sicurezza dopo aggiornamenti software, security policy change, ecc.;
- Consentire una sistematica valutazione di prodotti e servizi di sicurezza impiegati.

3. AMBITO DI APPLICAZIONE

Nel presente paragrafo sono elencati i contesti principali che saranno oggetto del servizio richiesto; si noti che tale insieme ha puro fine indicativo in quanto l'effettivo perimetro sarà definito dalla Società nel corso del periodo di fruizione del servizio stesso.

- **Mobile Application**: App Android e iOS;
- **Web Application**: portali vari;
- **Infrastrutture Cloud**: elementi applicativi ed infrastrutturali, di sicurezza e non;
- **Servizi interni**: infrastrutture ed elementi propri della Società, compresi endpoint;
- **Security Operation**: procedure e processi.

4. REQUISITI

4.1 VA/PT SECURITY

Mobile Application Penetration Test

L'attività di Mobile Application Penetration Testing (MAPT) dovrà consistere nell'esecuzione di una simulazione reale di un attacco all'applicativo in oggetto al fine di valutarne l'effettivo livello di sicurezza. La verifica dovrà essere efficace e riproducibile, soprattutto per verificare che il livello di sicurezza desiderato sia mantenuto nel tempo; pertanto, sarà necessario adottare metodologie riconosciute nel settore, quali sono quelle afferenti agli standard OWASP Mobile Top 10 e OWASP Mobile Testing Guide per effettuare il test dinamico.

Come linea guida indicativa, facendo riferimento al framework OWASP, si elencano nel seguito le tipologie minime di test che sono attese.

M1 Improper Platform Usage	Verificare la possibilità di abuso delle funzioni offerte o la violazione dei controlli di sicurezza predisposti nell'app o nella piattaforma (sistema operativo, middleware, ecc.)
M2 Insecure Data Storage	Verificare l'efficacia dei meccanismi di protezione del dato conservato a bordo del dispositivo con particolare attenzione alla possibilità di data leak volontario o accidentale.
M3 Insecure Communication	Verificare che tutte le comunicazioni avvengano in modo protetto e cifrato, che non siano impiegati protocolli deprecati o inadatti, che sia eseguito un controllo bilaterale degli endpoint della comunicazione quando richiesto, ecc.
M4 Insecure Authentication	Verificare l'efficacia dei processi di autenticazione dell'utente e della successiva efficace gestione della sessione di lavoro, con particolare riferimento all'accesso alle risorse.
M5 Insufficient Cryptography	Verificare l'esecuzione di tutte le operazioni di cifratura del dato che già non ricadono in M2 ed M3.
M6 Insecure Authorization	Verificare la corretta applicazione delle regole di authorization per l'accesso alle risorse e alle funzioni dell'app e del backend.
M7 Client Code Quality	Verifica globale del codice dell'app, con particolare riferimento al controllo degli input
M8 Code Tampering	Verifica dei meccanismi di prevenzione e rilevamento della manomissione del codice e dai dati che potrebbero avvenire dopo l'installazione dell'app. Fra l'altro, si deve testare il processo di patching, la possibilità di modificare le informazioni su storage locale o in memoria, il rischio di dirottamento delle richieste alla API di sistema.
M9 Reverse Engineering	Verificare la possibilità di successo di un'analisi del codice eseguibile con l'intento di ricostruirne il funzionamento, comprendere quali librerie e protocolli sono usati, parametri sensibili della cifratura, informazioni sul backend, ecc.
M10 Extraneous Functionality	Verificare la presenza e la possibilità di sfruttamento di funzioni impiegate per i test durante la fase di sviluppo, ma non rimosse dalla versione usata per il deploy.

Web Application Penetration Testing

Anche l'attività di Web Application Penetration Testing (WAPT) dovrà basarsi sull'effettuazione di una simulazione reale di attacchi verso gli applicativi web che saranno indicati come oggetto della prova, con il fine ultimo di valutarne l'effettivo livello di sicurezza. In analogia alla componente Mobile, risulta anche qui necessaria la sussistenza delle caratteristiche di sistematicità, riproducibilità e completezza, ed è quindi fortemente richiesta l'adozione di una metodologia di riconosciuta efficacia, quale la OWASP Testing Guide. Per meglio chiarire e dimensionare i test richiesti, nella tabella seguente sono riportate le principali (ma non tutte quelle che saranno richieste) macro aree di verifica che dovranno essere analizzate dal Fornitore.

Authentication	Test sui sistemi di autenticazione degli utenti
Access Control	Test delle funzioni di restrizione dell'accesso ai dati e alle funzioni disponibili
Data Validation	Test sui controlli di validità dei dati immessi dall'utente
Session Management	Test sui meccanismi di sfruttamento del token di sessione per l'autenticazione e autorizzazione dell'utente
Cryptography	Test sull'efficacia dei protocolli e dei sistemi di crittografia applicati, nonché sulla gestione delle chiavi
Configuration Management	Test sulla configurazione dell'infrastruttura sulla quale viene eseguito l'applicativo
Error Handling (Information Disclosure)	Test sulla gestione delle condizioni d'errore e, in particolare, sulla possibile divulgazione di informazioni sensibili che ne consegue
Client Side	Test dinamico di esecuzione del codice nel browser del client e relativi plug-in

Si osservi che, benché l'impiego di strumenti di test automatici di efficacia riconosciuta sia attesa e consentita per le operazioni di WAPT, la Società richiede che il Fornitore metta a sua disposizione del personale in grado di concepire e svolgere attacchi custom, ritagliati sulle caratteristiche delle proprie applicazioni, così come di valutare i risultati ottenuti alla luce di una consolidata esperienza nel settore della sicurezza.

4.2 SECURITY CONSULTING

Secure Code Review del codice sorgente

L'attività di Secure Code Review consisterà nell'analisi di sicurezza del codice sorgente, linea per linea e, quindi, avverrà in modalità white box, ovvero, con la completa conoscenza dell'applicativo (insieme dei sorgenti).

Si noti che, pur prevedendo l'uso di strumenti a supporto del processo, è esplicitamente richiesto che esso avvenga in maniera manuale e sia compiuto da personale in grado di comprendere il contesto applicativo e la reale entità del rischio. Più dettagliatamente, l'attività deve comprendere:

- ➢ l'analisi completa del codice;
- ➢ la rimozione dei falsi positivi durante la fase di test dinamico;
- ➢ l'individuazione della remediation da implementare a fronte delle vulnerabilità riscontrate, ordinate sulla base di un'attenta e ponderata prioritizzazione.

I test dovranno essere eseguiti in modo sistematico ed esaustivo, pertanto, il Fornitore proporrà nell'offerta tecnica un elenco di vettori di test, il quale sarà poi finalizzato insieme alla Società in fase di esecuzione del Contratto. Tale elenco dovrà costituire anche la base per la redazione dei report. A titolo esemplificativo, ma non esaustivo, si riportano nella tabella seguente alcune delle tipiche aree di ricerca delle vulnerabilità che la Società si attende che il Fornitore esplori durante l'esecuzione delle prove in oggetto.

Information Gathering	Analisi del codice
Authentication	Review del sistemi di autenticazione
Authorization	Review dei sistemi di controllo dell'accesso alle risorse
Data Validation	Verifica del controllo dell'input da parte dell'applicativo
Session Management	Review del sistema di gestione delle sessioni
Error handling	Review dei meccanismi di gestione delle condizioni d'errore
Cryptography	Review dei meccanismi di cifratura
Logging	Review dei sistemi di logging messi in atto
Communication	Review di tutti i processi di scambio con utenti ed entità esterne

Infine, è esplicitamente richiesto che le verifiche sul codice siano eseguite sia in modalità statica che dinamica, quest'ultima con lo scopo di esplorare in modo esaustivo il comportamento a runtime, con focus sui messaggi di controllo e sui dati scambiati.

4.3 API Assessment

La natura dei servizi di PagoPA richiede lo sviluppo continuo delle API da rendere disponibili agli Enti che sottoscrivono i propri servizi.
Le loro caratteristiche peculiari le rendono non studiabili, dal punto di vista della sicurezza, nello stesso modo delle applicazioni web; pertanto, si dovrà provvedere alla progettazione ed esecuzione di test specifici sulle stesse, seguendo le indicazioni che la Società fornirà in occasione della richiesta del particolare servizio al Fornitore. Esse dovranno tenere conto

della natura prevalentemente machine-to-machine delle interazioni fra API e le entità utilizzatrici, nonché delle modalità tipiche di sfruttamento delle vulnerabilità in tali ambienti.
Ciò premesso, la Società richiede anche in questo caso l'adozione di una metodologia di ricerca consolidata e di provata efficacia, indicando in questa fase l'insieme (non esaustivo) dei vettori di attacco che si attende il Fornitore prenda in considerazione:

Information Gathering	Analisi del complesso di sistemi da analizzare e raccolta delle relative informazioni
Authentication	Review del sistemi di autenticazione
Authorization	Review dei sistemi di controllo dell'accesso alle risorse
Data Validation	Verifica del controlli eseguiti sui parametri di ogni singola chiamata
Session Management	Review del sistema di gestione delle sessioni
Error handling	Review dei meccanismi di gestione delle condizioni d'errore
Cryptography	Review dei meccanismi di cifratura

4.4 Infrastruttura

Anche l'infrastruttura, pressoché interamente basata sul cloud, dovrà essere sottoposta a test per verificarne la resilienza e la postura generale di sicurezza. Questa categoria di verifiche, comunque, dovrà rispettare il modello di responsabilità condivisa fra la Società e i provider dei servizi cloud. Sarà pertanto richiesta una approfondita review delle appliance e dei meccanismi di sicurezza posti a protezione dei servizi, dei sistemi che li operano e, soprattutto, dei dati trattati. Nel seguito, sono elencate alcune delle componenti che sarà richiesto di esaminare con l'indicazione dello scopo principale di conduzione dei test.

- ➢ Verifica del processo di raccolta, gestione e conservazione **Logging & Monitoring**: compliance, efficacia ed efficienza dell'analisi, flussi interni di collaborazione fra team, ecc.
- ➢ Accertamento di **Security Misconfiguration** su servizi e prodotti anche non specifici per la sicurezza (quali ad esempio middleware, database, web server, ecc.).
- ➢ Confronto fra soluzioni di protezione, rilevamento e risposta (eventuale misura differenziale fra tecnologia già impiegata e PoC della nuova).
- ➢ Review delle configurazioni di **Firewall, WAF, IPS, DLP, SIEM, AntiDDoS**, ecc.:
    - monitoraggio (per un congruo periodo) a scopo di valutazione dell'efficienza e dell'efficacia dei sistemi in esercizio: conduzione di attacchi simulati (lateral movement, vulnerability exploitation, web application malicious input, data exfiltration, ecc.) verso sistemi delle reti interne e/o pubbliche;
    - valutazione e misurazione (criteri da concordare per garantire tracciamento dei miglioramenti nel tempo) dell'efficacia nella risposta delle soluzioni di cybersecurity in essere e delle loro configurazioni;

    - gli attacchi condotti dovranno essere raccolti e selezionati da molteplici fonti, quali Threat Intelligence Service (es. MITRE ATT&CK), security vendor, exploit database, hacker forum, CERT pubblici e privati, laboratori di ricerca vulnerabilità e altri.
- ➢ Verifica e valutazione/misurazione delle procedure e dei servizi affidati a una terza parte.
- ➢ Segnalazione delle minacce emergenti e (potenziali) zero-day applicabili e contestualizzate.
- ➢ Red Teaming su base contingente per verifica di nuovi servizi o in seguito a incidente.

4.5 Servizi di sicurezza generali

La Società potrà richiedere al Fornitore l'esecuzione di attività di supporto alle proprie funzioni di cybersecurity, le quali potranno essere espletate dai medesimi profili professionali elencati nel paragrafo COMPOSIZIONE DEL TEAM nel presente Capitolato.
Tali servizi saranno definiti su base contingente; a titolo esemplificativo, ma non esaustivo, si elencano alcuni possibili ambiti di utilizzazione:

- Verifica della compliance alle misure minime di sicurezza ICT definite da AgID.
- Verifica della corretta implementazione dei controlli e delle contromisure individuate.
- Supporto durante la risposta ad incidenti di sicurezza.
- Ecc.

5. IMPLEMENTAZIONE DEL PROCESSO

Con la premessa che il processo di VA/PT o SC sarà profilato ed ottimizzato di volta in volta in occasione della richiesta della Società, si elencano nel seguito i passi minimi che sono attesi ad ogni tornata di ripetizione periodica o basata su richiesta contingente:

1. Definizione dei sistemi target e dei test eseguiti;
2. Predisposizione dei target dummy negli ambienti (reti) di produzione da utilizzare come bersaglio per gli attacchi esterni; usando target gemelli si evita di recare danno agli ambienti di produzione;
3. Configurazione delle sorgenti del traffico di test; potranno essere implementate nelle reti di produzione, oppure in ambienti cloud dedicati; questo sarà stabilito in base alla tipologia di test concordata;
4. Esecuzione dei test (VA) avendo cura di non influire sul normale traffico operativo locale e geografico (opportuna regolazione della cadenza, del throughput, delle fasce orarie, ecc.); le sorgenti di attacco dovranno rilevare il più possibile in maniera autonoma i risultati, limitando il ricorso alla consultazione dei log raccolti dalla Società. I criteri per l'Identificazione delle vulnerabilità dovranno essere dichiarati e concordati (es. OWASP Top 10, MITRE ATT&CK,…);
5. Analisi dei risultati e produzione dei report. A tale proposito, si dovrà concordare con la società il metodo di valutazione (es. RAV di OSSTMM) e di reporting (priorità, riservatezza,…) e, inoltre, si dovrà fornire il supporto all'individuazione dei KPI e delle misure più indicative per alimentare i processi e ottimizzare le soluzioni di Security Operation e Security Governance;

6. Presentazione dei risultati alla Società, che li sottoporrà a revisione critica e accettazione;
7. Supporto a (eventuale) processo di follow-up, ovvero, mitigazione o rimozione della vulnerabilità (remediation, patching,...) e verifica finale dell'efficacia della soluzione compensativa adottata.

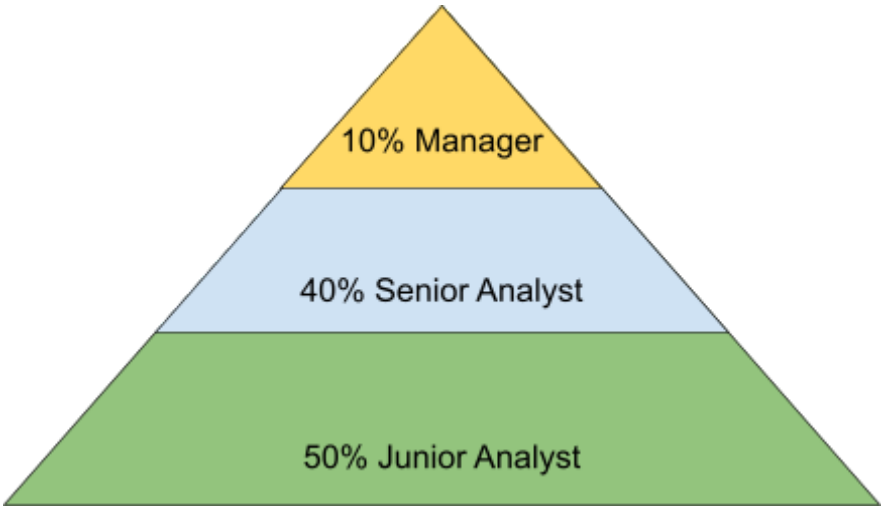
6. COMPOSIZIONE DEL TEAM

Per chiarire la tipologia delle figure richieste, la tabella seguente elenca i requisiti minimi che ognuna di esse dovrà possedere (l'indicazione della numerosità richiesta è indicativa e risulterà dalla specifica offerta del Fornitore):

Figura	# richiesto	Seniority	Esperienze/Caratteristiche
Security Project Leader	1	10 anni	Analisi di sicurezza applicazioni e infrastruttura Penetration Testing, Secure Code Review in ambienti complessi e mission-critical Conoscenza framework OWASP e MITRE ATT&CK Supervisione delle attività e del team, controllo della roadmap
Senior Web Application Penetration Tester	2	5 anni	Verifica di sicurezza delle applicazioni web Conoscenza di exploiting delle vulnerabilità web: Authentication Bypass, Authorization Bypass, Session Hijacking, CSRF , XSS, DomBased XSS, SQL Injection, JS Execution, Command Execution, HTTP Parameter Pollution, Business logic bypass, ecc. Conoscenza approfondita di tutte le tecnologie web, dai web server, application server ai framework ad oggi utilizzati
Senior Code Reviewer	2	5 anni	Verifica di sicurezza del codice delle applicazioni Web e delle mobile app

			Esecuzione di test dinamici e sul codice di applicazioni complesse e mission-critical Conoscenza approfondita di tutte le tecnologie e dei framework ad oggi utilizzati per lo sviluppo di applicazioni
Infrastructure Security Engineer	2	5 anni	Verifica della sicurezza di server web, container, database, hypervisor, ecc. Esecuzione di Penetration Test contro sistemi operativi, middleware in architetture complesse e mission-critical Conoscenza approfondita dei sistemi di rilevamento e protezione (WAF, Anti-DDoS, ecc.) e dei sistemi di Autenticazione e Autorizzazione

A discrezione del Fornitore è il numero di risorse Junior da affiancare al suddetto personale per completare i test nei modi e tempi concordati. Si tenga conto che la Società ha già stimato l'impegno relativo delle singole figure rispetto alle attività da compiersi; a tale proposito si riporta la piramide dell'effort attesa:



7. MODALITÀ DI EROGAZIONE

Le esigenze della Società contemplano l'esecuzione periodica del servizio (3 mesi o 6 mesi in base ai sistemi target, al trend delle minacce considerate e alle esigenze di compliance alla certificazione ISO/IEC 27001 e a quelle che verranno acquisite durante il periodo contrattuale). Ad essa si aggiunge la richiesta di sessioni di test specifiche e contingenti in occasione del lancio di nuovi servizi, di importanti cambi di release, di incidenti di sicurezza e di tutte le altre condizioni che lo richiederanno ad insindacabile giudizio della Società.

Per coprire queste esigenze, la Società ha stimato un **monte giornate annuale di 160 gg/u** di prestazioni che il Fornitore potrà erogare per le attività di VA/PT (inclusivi della preparazione e della redazione dei report) e/o dei servizi di Security Consulting, impiegando le figure elencate nel paragrafo precedente; il consumo sarà consuntivato dal personale della Società stessa, su indicazione del Fornitore ed a chiusura del preventivo specifico fornito anticipatamente, al termine di ogni sessione. Si precisa che non è in alcun modo garantito che tale monte giornate sia esaurito dalla Società nell'intero periodo contrattuale di **tre anni**, nonché nelle sue milestone intermedie.

La tipologia delle informazioni rese disponibili al Fornitore, le fasce orarie e la procedura di esecuzione dei test saranno concordate di volta in volta.

8. LIVELLI DI SERVIZIO

Al fine di tarare al meglio il servizio e di regolare i rapporti fra Società e Fornitore, sono di seguito elencati gli SLA ed i KPI che dovranno essere rispettati durante tutto l'arco contrattuale.

SLA	
Tempo massimo di risposta a richiesta di VA/PT	5 gg lavorativi
Tempo massimo di risposta a richiesta di SC	3 gg lavorativi
Tempo massimo di consegna di un report (comprensivo di remediation e calcolato dalla fine dei test pattuiti)	10 gg lavorativi

KPI	
Tempo massimo di disservizio (concordato) causato per esecuzione test	< 2 h
Falsi positivi segnalati nei report	< 2 per run
Scenari di utilizzo malevolo replicati	> 10 per run
Report provvisori intermedi	dopo ogni sistema testato

Le modalità di svolgimento dei test dovranno garantire quanto segue:

- ➢ Nessuna dipendenza dalla tecnologia o versioni dei prodotti/servizi;
- ➢ Applicabilità diretta sugli ambienti di produzione senza impatti su utilizzo o performance (ove richiesto dalla Società),
- ➢ Applicabilità ad ambienti cloud multi-provider integrati;
- ➢ Eseguibilità su applicativi in modalità black-box.

Il mancato rispetto dei termini previsti nel presente paragrafo comportano l'applicazione delle penali previste nel Contratto.

9. RISULTATO ATTESO

Elenco minimo degli outcome e altro materiale da produrre al termine delle attività:

- ➢ Executive Summary (Report sintetico)
- ➢ Report di dettaglio (secretato)
- ➢ Contromisure suggerite (vulnerability treatment): identificare le mitigazioni specifiche dei vari vendor, i metodi di remediation non vendor-specific, eventuali necessità di virtual patching,…
- ➢ Valutazione dell'impatto delle contromisure
- ➢ Tool impiegati
- ➢ Procedimento eseguito
- ➢ Evidenza di gestione sicura di tutti i dati raccolti
- ➢ Consegna di tutti i dati raccolti

Tali informazioni dovranno essere esposte in maniera completa e dettagliata all'interno dei seguenti documenti essenziali.

Executive Summary
Documento volto a riassumere ad alto livello la descrizione e la quantificazione dell'esposizione ai rischi e, in generale, la security posture rispetto alle cyber minacce più concrete.

Dettaglio delle minacce
Documento che illustra in forma dettagliata ed esaustiva tutte le vulnerabilità rilevate sui sistemi in produzione e, in particolare, le minacce che non sono state rilevate e/o bloccate dai dispositivi di cybersecurity. Ogni minaccia elencata dovrà essere corredata dalla relativa valutazione di criticità, la quale deve essere strettamente correlata all'ambito dove la minaccia stessa è stata riscontrata. La Società considera la corretta valutazione dell'effettiva probabilità di sfruttamento e dell'impatto nell'ambito del sistema analizzato un elemento essenziale del servizio.
Questo report è destinato ai responsabili del team Security e deve essere corredato da allegati in forma elettronica contenenti tutti i dati raccolti; in questo modo la Società potrà replicare l'analisi ed avere completa evidenza dei risultati ottenuti dal Fornitore.
Si precisa che, il documento in oggetto contiene informazioni riservate, pertanto, dovrà essere gestito e conservato utilizzando ogni accortezza necessaria ad evitarne la diffusione a soggetti non autorizzati ad esaminarne il contenuto (es. se inviato tramite mail potrà

essere contenuto in un messaggio che impiega Traffic Lamp Protocol). In ogni caso le modalità di trasmissione del documento in oggetto saranno concordate tra la Committente e il Fornitore in corso d'esecuzione del contratto.

Remediation Plan Rispecchiando il documento precedente, per ognuna delle vulnerabilità rilevate e dei corrispondenti attacchi andati a segno, deve fornire l'elenco delle azioni da intraprendere sui dispositivi di sicurezza e sui sistemi in produzione per mitigare i rischi descritti. Ogni azione, inoltre, deve essere corredata da opportuna valutazione di impatto temporaneo (fermi macchina,…) e permanente (fruizione del servizio, interoperabilità con altre componenti applicative e sistemi in produzione,…).
Si precisa che, il documento in oggetto contiene informazioni riservate, pertanto, dovrà essere gestito e conservato utilizzando ogni accortezza necessaria ad evitarne la diffusione a soggetti non autorizzati ad esaminarne il contenuto (es. se inviato tramite mail potrà essere contenuto in un messaggio che impiega Traffic Lamp Protocol). In ogni caso le modalità di trasmissione del documento in oggetto saranno concordate tra la Committente e il Fornitore in corso d'esecuzione del contratto.