IRE ISTITUTO NAZIONALE TUMORI REGINA ELENA ISG ISTITUTO DERMATOLOGICO SAN GALLICANO
ISTITUTI DI RICOVERO E CURA A CARATTERE SCIENTIFICO

UOSD Ingegneria Clinica e Tecnologie e Sistemi Informatici

Il dirigente della UOSD Ingegneria Clinica e Tecnologie e Sistemi Informatici

in virtù della delega conferita con deliberazione N°232/2015

HA ASSUNTO LA PRESENTE DETERMINAZIONE

N. 251 del 24/03/2022

OGGETTO: AFFIDAMENTO, TRAMITE MEPA, DEL SERVIZIO DI CHECKLIST, REDAZIONE E GESTIONE DEL REGISTRO ATTIVITÀ, REGISTRO PASSWORD E PRIVACY/DATA PROTECTION IN AMBITO DI SANITÀ ELETTRONICA AI FINI DELL'ADEGUAMENTO DEGLI IFO AL REGOLAMENTO EUROPEO N. 2016/79 DEL 27 GIUGNO 2016 (GDPR "GENERAL DATA PROTECTION REGULATION") DAL 01 MARZO 2022 AL 28 FEBBRAIO 2024 - CIG: Z3935AEB85

Esercizi/o 2022 - 2023 - 2024 Centri/o di costo 5.02.02.01.06

- Importo presente Atto: € 46.360,00

- Importo esercizio corrente: € 19.316,67

Budget

- Assegnato: € .

- Utilizzato: € .

- Residuo: € .

Autorizzazione n°: 2022/140235.1150

Servizio Risorse Economiche: **Giovanna Evangelista**

UOSD Ingegneria Clinica e Tecnologie e Sistemi Informatici Proposta n° DT-259-2022

L'estensore

Anna Cirulli

Il Responsabile del Procedimento

Giuseppe Navanteri

Il Dirigente della UOSD Ingegneria Clinica e Tecnologie e Sistemi Informatici

Giuseppe Navanteri

La presente determinazione si compone di n° 9 pagine e dei seguenti allegati che ne formano parte integrante e sostanziale:
- Allegato 1 composto da n. 4 pagine

Il Dirigente della UOSD Ingegneria Clinica e Tecnologie e Sistemi Informatici

Visto	il decreto legislativo 30.12.1992, n. 502 e successive modificazioni ed integrazioni;
Visto	il decreto legislativo 16.10.2003, n. 288;
Vista	la legge regionale 23.01.2006, n. 2;
Visto	l'Atto Aziendale adottato con deliberazione n. 153 del 19.02.2019 ed approvato dalla Regione Lazio con DCA n. U00248 del 2.07.2019, modificato e integrato con la delibera 1254 del 02.12.2020, n. 46 del 21/01/2021 e n. 380 del 25/03/2021, approvate dalla Direzione Salute ed Integrazione Sociosanitaria della Regione Lazio, con Determinazione n. G03488 del 30/03/2021;
Premesso	che con l'entrata in vigore del Regolamento Europeo 2016/79 del 27 giugno 2016 (GDPR "General Data Protection Regulation"), l'U.E. ha uniformemente regolamentato la materia della protezione delle persone fisiche con riguardo al trattamento dei dati personali;
	che con circolare AgID n. 1/2017 del 17 marzo 2017 recante: "Misure minime di sicurezza ICT per le pubbliche amministrazioni (DPCM 1 agosto 2015)" indica alle pubbliche amministrazioni le misure minime per la sicurezza ICT da adottare entro tempistiche circoscritte, al fine di proteggere il patrimonio informatico ed i dati gestiti al suo interno, da eventuali minacce più comuni e frequenti cui sono soggetti i sistemi informativi";
Preso atto	in particolare, della nuova regolamentazione giuridica della privacy di che trattasi che prevede un cambio radicale nell'impostazione della tutela dei dati personali, che dovrà concretizzarsi in un "modello organizzativo" da implementare in ragione di un'attenta analisi dei rischi e a seguito di un'autovalutazione finalizzata all'adozione delle migliori strategie volte a presidiare i trattamenti di dati effettuati in ottica di privacy by design e privacy by default, e

cioè in base a un approccio non più di tipo formale o limitato alla mera adozione di misure di sicurezza, ma a un sistema organizzativo caratterizzato da un'attenzione multidisciplinare alle specificità della struttura e della tipologia di trattamento, sia dal punto di vista della sicurezza informatica, sia in conformità agli obblighi legali;

Considerato che i principali elementi da implementare rispetto all'attuale quadro normativo sono così riassumibili:

1) Diritti degli interessati (conoscitivi e di controllo), dati personali e trattamenti

2) Obblighi dei titolari del trattamento e organizzazione

3) Adozione di specifiche policy e documenti interni

4) Semplificazioni di compliance interna

5) Misure di sicurezza

Considerata pertanto la necessità degli IFO di adeguare i propri sistemi ed adoperare servizi aggiuntivi in modo da essere in linea con la normativa nell'adottare nuove regole riguardanti il trattamento, la gestione e la protezione dei dati personali, in conformità al soprarichiamato Regolamento EU sulla privacy (GDPR) sia mediante l'innalzamento del proprio livello informatico e sia mediante l'individuazione di eventuali interventi correttivi;

Preso atto che, gli IFO hanno iniziato il loro percorso di allineamento alla normativa attraverso un piano di allineamento già nel 2017;

Considerato che tale piano evolutivo ed adeguativo alla normativa prevede:

1. Analisi: identificazione dei dati personali e dove essi risiedono secondo le varie procedure sanitarie ed amministrative;
2. Gestione: Controllo dell'utilizzo dei dati personali e come è gestito il loro accesso;
3. Protezione: determinazione dei controlli di sicurezza per prevenire, rilevare e rispondere a eventuali vulnerabilità e violazioni di dati personali *(data breach)*.
4. Report: Mantenimento della documentazione richiesta, gestione delle richieste di dati e notifiche di eventuali violazioni.

Considerato che, come descritto nel piano triennale dell'informatizzazione IFO, tale attività ha rappresentato la fase iniziale di adeguamento normativo e che da esso scaturiranno differenti azioni migliorative da intraprendere per rendere gli IFO completamente allineati al GDPR n. 679/2016 entro i termini di legge;
che in questo momento, anche in relazione ai risultati ottenuti dall'audit descritto in precedenza, si rende necessario approfondire ed allineare i sistemi informatici IFO alla richiesta del GDPR n. 679/2016 in relazione alle "Misure di sicurezza" ed in particolare:

- Dotarsi di un servizio di Cyber Security finalizzato all'analisi e prevenzione di potenziali minacce alla sicurezza delle informazioni all'interno ed all'esterno dell'organizzazione: servizio cloud "as a service" che permetta di disporre di una piattaforma di Cyber Threat Intelligence in grado di controllare ed analizzare il livello di sicurezza di infrastrutture ICT, dati, processi informativi, identificare minacce in ambiente OSINT e DarkWeb (ad es. data breach), cyber reputation, social engineering, phishing e criticità in ambienti fisici.

Considerato che, in seguito a ricerca di mercato è stata presentata offerta dalla Società Vola SpA (Allegato 1 alla presente in modo da formarne parte integrante e sostanziale), che risponde ai requisiti tecnici richiesti e che offre una piattaforma in modalità As A Service in grado di offrire quanto necessario d IFO ed in particolare:

- Monitoraggio continuo: La funzionalità di Continuous Assessment consente alle organizzazioni di rilevare periodicamente e costantemente le vulnerabilità delle infrastrutture informatiche internamente ed esternamente al perimetro dell'organizzazione e qualisiasi altra presenza di minacce in rete come ad es. furto di credenziali, data breach, attacchi di phishing, compromissione degli asset critici dovuti a malware, botnet, etc... Per ogni anomalia riscontrata, dove possibile, vengono suggerite le eventuali azioni di mitigazione da adottare. La funzionalità consente di ridurre il rischio derivante da attacchi informatici in maniera rapida e tempestiva, prima che le vulnerabilità possano essere sfruttate dagli attaccanti.

- HOST / NETWORK / APPLICATION VULNERABILITY ASSESSMENT: Vulnerability Assessment interno ed esterno all'organizzazione in modalità continua o periodica, a scelta dell'utente. Evidenza immediata dei risultati, Remediation Plan e analisi storica del livello di sicurezza nel tempo. Cerbeyra è in grado di effettuare scansioni su qualsiasi device connesso alla rete, sia wired che wireless come ad es. IoT, impianti industriali (ad es. Scada) sistemi di build automation connessi a reti ethernet e in generale qualsiasi oggetto disponga di un indirizzo IP. Inoltre Cerbeyra permette la scansione di applicazioni Web per la verifica di ulteriori vulnerabilità dovute a errori nella scrittura del codice sorgente o delle piattaforme applicative.
- CYBER FEED E CYBER REPUTATION: Cerbeyra effettua un monitoraggio periodico di tutti gli host (IP/FQDN) e dei domini DNS dell'organizzazione esposti su internet, ne verifica il livello reputazionale e/o di compromissione, come ad es. la presenza in blacklist per attività di spam, phishing, frode, etc.., o se sono presenti host coinvolti in attività di botnet, malware, attacco, ne geolocalizza la posizione e ricerca le informazioni identificative a lui associate.
- CYBER THREAT INTELLIGENCE: Cerbeyra effettua un monitoraggio continuo del web (OSINT) e del Dark Web alla ricerca della presenza di eventuali data breach contenenti informazionis sull' utente. Credenziali, documenti sensibili ed eventuali presenze dei loro asset in liste o indicizzazioni di siti malevoli;
- CYBER SURVEY: Il Cyber Survey permette di effettuare una valutazione in self-assessment del livello di maturità di un'organizzazione nella gestione della sicurezza delle informazioni e della compliance normativa. L' analisi investigativa è sviluppata in coerenza con le caratteristiche dell'organizzazione (es. n° tipo di azienda, num. dipendenti, etc.) ed ai principali indicatori di riferimento. Il risultato viene correlato con le altre funzionalità di analisi (ad es. vulnerability assessment) e permette di effettuare una previsione di esposizione economica del danno;

- Internet Of Things Sensors: Dalla sonda PTBOX pensata per effettuare i vulnerability assessment di network private ai sensori IoT (Internet Of Things), Cerbeyra, grazie alla sua proprietaria tecnologia Senso rileva i principali parametri ambientali, fondamentali in aree critiche come datacenter o più in generale di infrastrutture tecnologiche. Tramite i sensori IoT è possibile implementare una rete di monitoraggio geografica distribuita, in modalità zero configuration.
- REPORT, GOVERNANCE E COMPLIANCE: Cerbeyra permette di valutare il livello di vulnerabilità dell'infrastruttura ICT del cliente, le politiche di sicurezza organizzativa a difesa delle informazioni, l'individuazione di criticità, potenziali minacce interne ed esterne, il rischio di impatto sia economico che normativo, verificando attraverso specifici indicatori di riferimento eventuali gap e rappresentando attraverso una dashboard la situazione in tempo reale. In questo ambito Cerbeyra rappresenta lo strumento ideale per soddisfare determinate richieste normative quali ad esempio l'art. 32 del 2016/679 (GDPR) punto 1. d) dove si richiede "una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento. Cerbeyra permette una rappresentazione sinottica della struttura di sicurezza delle informazioni e un'analisi predittiva delle eventuali minacce;
- CERBEYRA INDEX: Cerbeyra estende il monitoraggio sul controllo cibernetico del cliente, dall' ambito virtuale a quello fisico e normativo, effettuata un' attività di intelligence predittiva correlando i dati acquisiti ed analizzati attraverso i suoi sensori e motori di scansione. Questa capacità analitica viene sintetizzata in un unico indicatore di valutazione complessiva, denominato il Cerbeyra Index. Rispetto ai classici software o piattaforme di PT e VA che si limitano ad effettuare una fotografia statica del livello di sicurezza analizzato e spesso solo di alcuni ambiti, Il Cerbeyra Index è in grado di esprimere un giudizio complessivo eterogeneo, dinamico continuamente aggiornato in base allo stato del livello di critici-

tà di tutti gli asset, valutandone il fattore di cambiamento, l'attendibilità, l'impatto e la probabilità;

- DASHBOARD E CENTRO NOTIFICHE: L'utente può accedere alla Dashboard di Cerbeyra direttamente via web browser, dalla Dashboard, che riassume i principali indicatori e parametri fondamentali per capire immediatamente il livello di sicurezza in essere, l'utente può effettuare un drill down dettagliato su ogni singola anomalia evidenzia permettendo di visualizzare ogni informazioni a livello granulare. L'interfaccia web responsive permette l'accesso anche da tablet e smartphone di ultima generazione. Tramite il centro notifiche, l'utente può selezionare quali informazioni ricevere in ogni momento e scegliere anche se inviarlo ad altri utenti (ad es. ditta esterne gestore di servizi).

per un importo pari ad € 25.000,00 oltre IVA/annuo ed € 47.000,00 oltre IVA/biennio;

Considerato che il servizio offerto non necessita, da parte IFO, dell'acquisto di prodotti e/o l'implementazione di sofisticate piattaforme all'interno della propria organizzazione che costringono ad onerosi costi di manutenzione e gestione;

Considerato che in seguito a trattativa economica è stato apportato uno sconto che porta l'offerta ad € 22.000,00 oltre IVA/annuo ed € 38.000,00 oltre IVA/biennio;
inoltre che la UOSD Ingegneria Clinica e Tecnologie e Sistemi Informatici reputa opportuno procedere con l'attivazione del servizio per la durata di 2 (due) anni e quindi all'importo pari ad € 38.000,00 oltre IVA e cioè pari ad € 46.360,00 IVA inclusa per il periodo 01 marzo 2022 – 28 febbraio 2024;
che in particolare, l'offerta presentata dalla Società Vola S.p.A., allegato n. 1 alla presente quale parte integrante e sostanziale, è stata considerata congrua e coerente con le necessità degli IFO;

Acquisito il parere favorevole del Data Protection Officer degli IFO;

Verificata l'utilità e la convenienza economica della acquisizione in argomento, che in tal modo assicura un percorso di allineamento alla normativa vigente in materia di protezione e tutela del dato sensibile ed agli obblighi della Pubblica Amministrazione a riguardo;

Ritenuto pertanto opportuno procedere con l'affidamento del servizio di Cyber Security finalizzato all'analisi e prevenzione di potenziali minacce alla sicurezza delle informazioni all'interno ed all'esterno dell'organizzazione, di cui all'allegato n. 1 alla presente deliberazione in modo da formarne parte integrante e sostanziale, alla Società Vola SpA, secondo quanto previsto nell'offerta presentata, per il periodo 01/03/2022 – 28/02/2024, e per un importo pari ad € 38.000,00 oltre IVA e cioè pari ad € 46.360,00 IVA inclusa, CIG: Z3935AEB85;

Considerato che tale costo, a fronte delle prestazioni rese, si ritiene congruo e conveniente per l'Amministrazione;

Tenuto conto che la spesa complessiva pari ad € 38.000,00 oltre IVA e cioè pari ad € 46.360,00 IVA inclusa per il periodo 01 marzo 2022 – 28 febbraio 2024, può essere registrata come di seguito riportato:

- Per € 19.316,67 sul bilancio economico dell'esercizio 2022 – 5.02.02.01.06;
- Per € 23.180,00 sul bilancio economico dell'esercizio 2023 – 5.02.02.01.06;
- Per € 3.863,33 sul bilancio economico dell'esercizio 2024 – 5.02.02.01.06;

Attestato che il presente provvedimento, a seguito dell'istruttoria effettuata, nella forma e nella sostanza è totalmente legittimo e utile per il servizio pubblico, ai sensi della legge 14 gennaio 1994, n. 20 art. 1 e successive modifiche, nonché alla stregua dei criteri di economicità e di efficacia di cui alla legge 7 agosto 1990, n. 241 art. 1, primo comma come modificata dalla legge 11 febbraio 2005, n. 15;

DETERMINA

ai sensi dell'art. 36 comma 2 lett. A) del D.lgs. 50/2016 e per i motivi di cui in narrativa che si intendono integralmente confermati di:

- Affidare ai sensi dell'art.36 comma 2 lett. A) del D.Lgs. 50/2016, il servizio di Cyber Security finalizzato all'analisi e prevenzione di potenziali minacce alla sicurezza delle informazioni all'interno ed all'esterno dell'organizzazione, di cui all'allegato n.1 alla presente deliberazione in modo da formarne parte integrante e sostanziale, alla Società Vola S.p.A., secondo quanto

previsto nell'offerta presentata per un importo pari ad € 38.000,00 oltre IVA e cioè pari ad € 46.360,00 IVA inclusa per il periodo 01 marzo 2022 – 28 febbraio 2024, CIG: Z3935AEB85;

-

- Addebitare l'importo complessivo di € 38.000,00 oltre IVA e cioè pari ad € 46.360,00 IVA inclusa per il periodo 01 marzo 2022 – 28 febbraio 2024, come di seguito riportato:
  - Per € 19.316,67 sul bilancio economico dell'esercizio 2022 – 5.02.02.01.06;
  - Per € 23.180,00 sul bilancio economico dell'esercizio 2023 – 5.02.02.01.06;
  - Per € 3.863,33 sul bilancio economico dell'esercizio 2024 – 5.02.02.01.06;

- Trasmettere apposito ordine NSO;
- Nominare DEC del contratto il Sig. Umberto Santi.

La UOSD Ingegneria Clinica e Tecnologie e Sistemi Informatici curerà tutti gli adempimenti per l'esecuzione della presente determinazione.

Il Dirigente della UOSD Ingegneria Clinica e Tecnologie e Sistemi Informatici

Giuseppe Navanteri

Documento firmato digitalmente ai sensi del D.Lgs 82/2005 s.m.i. e norme collegate

Spett.le

Istituti fisioterapici Ospitalieri

Via Elio Chianesi, 53, 00144 Roma RM

All'attenzione di

Ing. Navanteri

Offerta n. 148-2022-CRB

Data: 15/02/2022

Oggetto: SERVIZI PROFESSIONALI AVANZATI PER LA SICUREZZA DELLE INFORMAZIONI, SERVIZIO DI CYBER SECURITY E THREAT INTELLIGENCE CERBEYRA .

Preg.mo Ing. Navanteri,

facendo seguito ai colloqui intercorsi siamo lieti di presentarLe la nostra migliore offerta riguardante la fornitura del servizio di Cyber Security e Threat Intelligence Cerbeyra in riferimento alla esposizione al rischio di cyber attacchi ed alla sicurezza delle informazioni.

Restando a disposizione per qualunque informazione in merito, cogliamo l'occasione per porgere cordiali saluti.

Vola Spa

GN

Premessa

Le informazioni sono un bene che aggiungono valore ad una organizzazione e le soluzioni di sicurezza rappresentano sempre di più un nuovo mezzo per arricchire la relazione tra processo di business e tecnologia. Le decisioni e le strategie di security non devono essere vissute come un obbligo ma come un investimento, la protezione di dati confidenziali da possibili furti o distruzione fa sì che un'organizzazione aumenti la propria competitività e protegga quindi con successo dati "riservati" come quelli dei propri clienti, dell'innovazione su nuovi prodotti, strategie di mercato ed altro. La sicurezza aiuta a proteggere l'immagine di un'azienda.

Descrizione del Servizio

Cerbeyra è la soluzione di Cyber Security pensata per analizzare e prevenire potenziali minacce alla sicurezza delle informazioni all'interno ed all'esterno di un'organizzazione. Un servizio cloud "as a service" che permette di disporre di una piattaforma di Cyber Threat Intelligence in grado di controllare ed analizzare il livello di sicurezza di infrastrutture ICT, dati, processi informativi, identificare minacce in ambiente OSINT e DarkWeb (ad es. data breach), cyber reputation, social engineering, phishing e criticità in ambienti fisici. Cerbeyra è un servizio "zero effort" non necessita, da parte del cliente, dell'acquisto di prodotti e/o l'implementazione di sofisticate piattaforme all'interno della propria organizzazione che generalmente lo costringono a sostenere onerosi costi di manutenzione e gestione.

Principali funzionalità del servizio

MONITORAGGIO CONTINUO (CONTINUOUS ASSESSMENT)

La funzionalità di Continuous Assessment consente alle organizzazioni di rilevare periodicamente e costantemente le vulnerabilità delle infrastrutture informatiche internamente ed esternamente al perimetro dell'organizzazione e qualisiasi altra presenza di minacce in rete come ad es. furto di credenziali, data breach, attacchi di phishing, compromissione degli asset critici dovuti a malware, botnet, etc… Per ogni anomalia riscontrata, dove possibile, vengono suggerite le eventuali azioni di mitigazione da adottare. La funzionalità consente di ridurre il rischio derivante da attacchi informatici in maniera rapida e tempestiva, prima che le vulnerabilità possano essere sfruttate dagli attaccanti.

HOST / NETWORK / APPLICATION VULNERABILITY ASSESSMENT

Vulnerability Assessment interno ed esterno all 'organizzazione in modalità continua o periodica, a scelta dell'utente. Evidenza immediata dei risultati, Remediation Plan e analisi storica del livello di sicurezza nel tempo. Cerbeyra è in grado di effettuare scansioni su qualsiasi device connesso alla rete, sia wired che wireless come ad es. IoT, impianti industriali (ad es. Scada) , sistemi di build automation connessi a reti ethernet e in generale qualsiasi oggetto disponga di un indirizzo IP. Inoltre Cerbeyra permette la scansione di applicazioni Web per la verifica di ulteriori vulnerabilità dovute a errori nella scrittura del codice sorgente o delle piattaforme applicative.

CYBER FEED E CYBER REPUTATION

Cerbeyra effettua un monitoraggio periodico di tutti gli host (IP/FQDN) e dei domini DNS dell'organizzazione esposti su internet, ne verifica il livello reputazionale e/o di compromissione, come ad es. la presenza in blacklist per attività di spam, phishing, frode, etc.., o se sono presenti host coinvolti in attività di botnet, malware, attacco, ne geolocalizza la posizione e ricerca le informazioni identificative a lui associate.

CYBER THREAT INTELLIGENCE

Cerbeyra effettua un monitoraggio continuo del web (OSINT) e del Dark Web alla ricerca della presenza di eventuali data breach contenenti informazionis sull' utente. Credenziali, documenti sensibili ed eventuali presenze dei loro asset in liste o indicizzazioni di siti malevoli.

CYBER SURVEY

Il Cyber Survey permette di effettuare una valutazione in self-assessment del livello di maturità di un'organizzazione nella gestione della sicurezza delle informazioni e della compliance normativa. L' analisi investigativa è sviluppata in coerenza con le caratteristiche dell'organizzazione (es. n° tipo di azienda, num. dipendenti, etc) ed ai principali indicatori di riferimento. Il risultato viene correlato con le altre funzionalità di analisi (ad es. vulnerability assessment) e permette di effettuare una previsione di esposizione economica del danno.

Internet Of Things Sensors

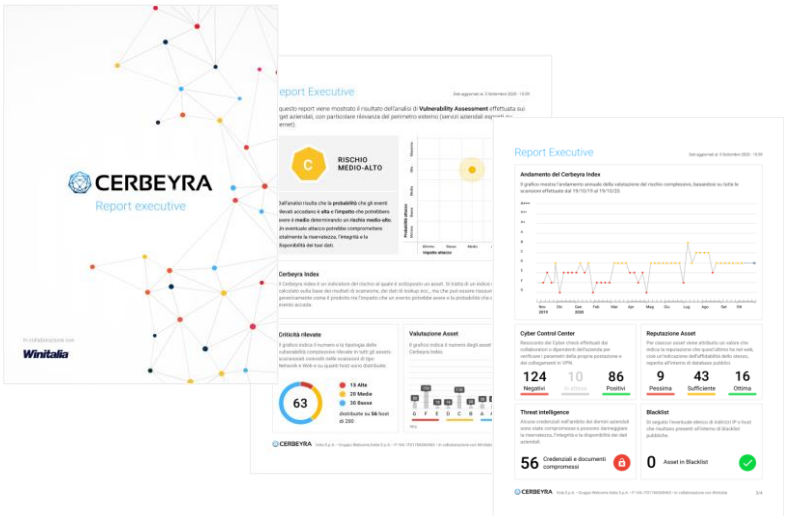
Dalla sonda PTBOX pensata per effettuare i vulnerability assessment di network private ai sensori IoT (Internet Of Things), Cerbeyra, grazie alla sua proprietaria tecnologia Senso rileva i principali parametri ambientali, fondamentali in aree critiche come datacenter o più in generale di infrastrutture tecnologiche. Tramite i sensori IoT è possibile implementare una rete di monitoraggio geografica distribuita, in modalità zero configuration.

GN

REPORT, GOVERNANCE E COMPLIANCE

Cerbeyra permette di valutare il livello di vulnerabilità dell'infrastruttura ICT del cliente, le politiche di sicurezza organizzativa a difesa delle informazioni, l'individuazione di criticità, potenziali minacce interne ed esterne, il rischio di impatto sia economico che normativo, verificando attraverso specifici indicatori di riferimento eventuali gap e rappresentando attraverso una dashboard la situazione in tempo reale. In questo ambito Cerbeyra rappresenta lo strumento ideale per soddisfare determinate richieste normative quali ad es. l'art. 32 del 2016/679 (GDPR) punto 1. d) , dove si richiede "una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento." Cerbeyra permette una rappresentazione sinottica della struttura di sicurezza delle informazioni e un'analisi predittiva delle eventuali minacce.

Cerbeyra permette di generare report in tempo reale, sullo stato in essere del livello di sicurezza dell'organizzazione. Due tipologie di report: Executive per il management e tecnico dove vengono rappresentate nel dettaglio tutte le singole vulnerabilità con relative remedation (ove possibile), pronti per essere allegati alla documentazione richiesta dalla normativa vigente (ad es. GDPR).

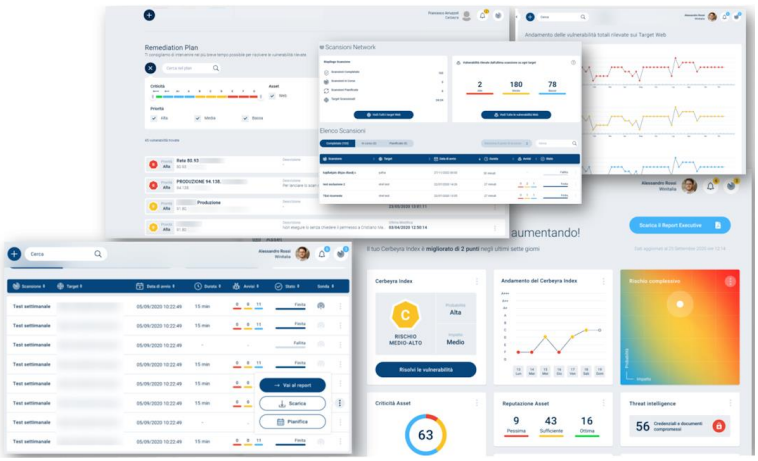


CERBEYRA INDEX

Cerbeyra estende il monitoraggio sul controllo cibernetico del cliente, dall' ambito virtuale a quello fisico e normativo, effettuata un' attività di intelligence predittiva correlando i dati acquisiti ed analizzati attraverso i suoi sensori e motori di scansione. Questa capacità analitica viene sintetizzata in un unico indicatore di valutazione complessiva, denominato il **Cerbeyra Index**. Rispetto ai classici software o piattaforme di PT e VA che si limitano ad effettuare una fotografia statica del livello di sicurezza analizzato e spesso solo di alcuni ambiti, Il Cerbeyra Index è in grado di esprimere un giudizio complessivo eterogeneo, dinamico continuamente aggiornato in base allo stato del livello di criticità di tutti gli asset, valutandone il fattore di cambiamento, l'attendibilità, l'impatto e la probabilità.

DASHBOARD E CENTRO NOTIFICHE

L'utente può accedere alla Dashboard di Cerbeyra direttamente via web browser, dalla Dashboard, che riassume i principali indicatori e parametri fondamentali per capire immediatamente il livello di sicurezza in essere, l'utente può effettuare un drill down dettagliato su ogni singola anomalia evidenzia permettendo di visualizzare ogni informazioni a livello granulare. L'interfaccia web responsive permette l'accesso anche da tablet e smartphone di ultima generazione. Tramite il centro notifiche, l'utente può selezionare quali informazioni ricevere in ogni momento e scegliere anche se inviarlo ad altri utenti (ad es. ditta esterne gestore di servizi).



SPECIFICHE CLIENTE

Dai colloqui intercorsi con il cliente sono state evidenziate le seguenti necessità di monitoraggio:

- IP pubblici:
  - N.8 IP Pubblici / FQDN
  - N.2 Domini DNS

- IP PRIVATI:
  - N. 2500 IP PRIVATI

L'offerta prevede l'installazione in comodato d'uso presso il cliente di N. 1 sonda PTBOX comprensiva di N.1 sensore ambientale (di serie).

OFFERTA ECONOMICA

Abbonamento di durata 12 mesi o 24 mesi

COD. PRODOTTO	DESCRIZIONE	ABBONAMENTO 1 ANNO	ABBONAMENTO 2 ANNI
CRBYR-MSSP-CST1	• **N.8 IP Pubblici / FQDN (Automated Pen-Test e Vuln. Ass.)** • **N. 2500 IP privati** • **N.2 Domain Name – DNS (Analisi Threat Intelligence)** • **Cyber Survey** • **Report Tecnico** • **Executive Report** • **Analisi on-demand o continua** • **Accesso Dashboard Cerbeyra Cliente** • **N.1 PTBOX (Sonda per analisi reti private)** • **N.1 Sensore ambientale IoT A1**	€ 25.000,00	€ 47.000,00
	PREZZO TOTALE	~~**€ 25.000,00**~~	~~**€ 47.000,00**~~
	PREZZO A VOI RISERVATO	**€ 22.000,00**	**€ 38.000,00**

Durata offerta: 60 giorni. Prezzi IVA 22% esclusa.

GN