puntozero
LA NUOVA VERSIONE DELL'INNOVAZIONE

CONDIZIONI DI FORNITURA DI UNA PIATTAFORMA SOAR E DEI CONNESSI SERVIZI DI ATTIVAZIONE E STARTUP

CIG A0037F3C86

CUP I61B21004920002

PREMESSA

Per proteggere la propria infrastruttura tecnologica, PuntoZero necessita di tecnologie di sicurezza che offrano:

- protezione fisica - sia perimetrale che interna;
- protezione funzionale - che deriva non solo dall'applicazione delle policy sotto forma di controllo granulare dell'accesso, ma anche di rilevamento / prevenzione esplicita delle minacce;
- protezione logica - applicata a tutti i livelli dello stack di elaborazione: servizi/protocolli a livello di rete, applicazioni infrastrutturali, applicazioni aziendali personalizzate e dati.

Pertanto PuntoZero intende dotarsi di una Piattaforma SOAR (Security Orchestration, Automation and Response) che possa aiutare i cyber security specialist nella gestione degli scenari e dei flussi di lavoro, automazione delle attività e sistema centralizzato di accesso, query e condivisione dei dati di intelligence sulle minacce.

1. CONTESTO

PuntoZero si avvale, tra l'altro, di un punto di accesso alla rete Internet (POP), utilizzato per il traffico di navigazione, per la pubblicazione di tutti i servizi ospitati al Data Center Regionale ed anche per la pubblicazione di alcuni servizi ospitati al Data Center gestiti autonomamente dagli Enti che sono collegati all'infrastruttura di rete in Fibra Ottica di proprietà di PuntoZero. Presso il POP sono collocati due Firewall che garantiscono l'adeguato filtro da e verso l'infrastruttura sopra descritta ed è inoltre stato attivato un servizio DDoS per assicurare un'ulteriore protezione. Sono stati attivati anche servizi IPS e WAF, oltre che la EndPoint Security per tutti i virtual servers presenti all'interno del Data Center. Tutte le fonti log sopra descritte, ed alcune degli enti che si avvalgono della nostra infrastruttura di rete, sono convogliate verso il SIEM Regionale IBM QRadar.

2. OGGETTO

La fornitura prevede una Piattaforma SOAR, in modalità SaaS, nativamente integrata con il SIEM attualmente in uso in PuntoZero, IBM QRadar (versione 7.5.4).

La fornitura include l'attivazione e lo startup del servizio, da realizzare in base alle specifiche fornite dal committente. La fornitura prevede, anche, l'erogazione di 10 giornate di training-on-the-job per i tecnici del committente perché siano adeguatamente formati all'utilizzo, alla conduzione ed al monitoraggio del servizio.

3. REQUISITI TECNICO-FUNZIONALI E CONFIGURAZIONE MINIMA RICHIESTA

La fornitura della soluzione deve essere conforme ai requisiti minimi che di seguito vengono elencati.

Piattaforma SOAR

La soluzione proposta dovrà prevedere la fornitura di licenze per l'utilizzo della piattaforma da parte di almeno 2 utenti, corredata di tutte le features di seguito elencate.

Features della piattaforma:

- la soluzione deve essere nativamente integrata con il SIEM QRadar IBM
    - la soluzione dovrà essere certificata compatibile con SIEM QRadar IBM versione 7.5.4, in esercizio presso il committente
- la piattaforma deve garantire l'interoperabilità con il sistema di collaboration Google Work Space, attualmente in uso dalla stazione appaltante
- possibilità di fornire report per garantire la massima visibilità e comprensione di team/dati/avvisi
- possibilità di raggruppare le minacce mediante l'applicazione di un layout in stile MITRE ATT&CK navigator
- disponibilità di un ambiente multi tenant che permetta la completa separazione sia di dati che di playbook
- possibilità di creazione utenti specifici per tenant
- controllo accesso basato sui ruoli
- disponibilità di una dashboard con la visualizzazione delle azioni in sospeso, con eventuale supporto di widget HTML per garantire agli analisti un processo decisionale più rapido
- disponibilità per ogni caso di una rappresentazione che indichi la relazione contestuale tra i diversi alert raggruppati e tra gli IOC interessati, con l'indicazione della sequenza temporale che riproduca la catena degli eventi
- disponibilità di dati per l'analisi di esecuzione di playbook (tempi medi, statistiche, utilizzatori, etc)

- ampia possibilità di customizzazione dei playbook tramite GUI
- identificazione relazioni e conseguente aggregazione degli alert in base al contesto ed alla specifica categoria di minaccia
- possibilità di visualizzare mediante dashboard metriche e KPI
- funzionalità di collaborazione per gli analisti, come tagging, comunicazioni ed assegnazione dei cases
- chats specifiche per i cases aperti
- possibilità di generazione automatica di report su minacce, tempi di intervento e tempi di risoluzione
- integrazione con i principali strumenti di ticketing.

3.1 ULTERIORI CARATTERISTICHE TECNICHE E FUNZIONALI

La soluzione proposta dovrà specificare, descrivere e documentare nella proposta tecnico economica la presenza delle ulteriori caratteristiche tecniche e funzionali di seguito indicate, aggiuntive a quelle definite al precedente Capitolo 3.

3.1.1 Scalabilità

Verrà analizzata la soluzione proposta al fine di valutarne la capacità di evoluzione in relazione a possibili scenari di ampliamento del perimetro di analisi del SIEM con conseguente aumento dei cases aperti e/o dei security analyst coinvolti.

La valutazione terrà in considerazione che la piattaforma deve basarsi su microservizi con scalabilità automatica. Deve permettere di aumentare/ridurre risorse ed elaborazioni aggiuntive durante periodi di attività anomali.

3.1.2 Features aggiuntive

Le Features aggiuntive verranno valutate sulla base delle seguenti caratteristiche principali:

- possibilità di integrazione con feed di sicurezza MISP e creare playbook che possano automaticamente rimediare IOC noti forniti dalla threat intelligence
- supporto di lavoro in modalità mobile
- possibilità di testare nuovi playbook tramite la simulazione di eventi/attacchi

- disponibilità di un modulo di Crisis Management per la gestione di eventuali crisi, che possa riunire utenti di diverse aree ed esterni alla piattaforma (avvocati, enti governativi, polizia postale, etc.), senza richiedere licenze aggiuntive per questi ultimi
- varietà e numerosità delle integrazioni native con sorgenti di eventi di sicurezza (firewalls, endpoint protection, SIEM, threat intelligence, authentication, ticketing, etc.) sia in fase di apertura dell'incidente informatico, sia per la raccolta di ulteriori informazioni per il triage e l'analisi degli incidenti che per la fase di remediation
- qualità del feed di threat intelligence. In particolare:
    - la numerosità e la varietà di fonti, fra cui fonti OSINT, utilizzate dal feed di threat intelligence;
    - la capacità di arricchimento degli indicatori di compromissione (threat actors, IP addresses, etc.)
    - l'innovatività e la capacità dei motori di machine learning di correlare le informazioni di sicurezza provenienti da varie fonti, al fine di rendere più rapida l'analisi di tali informazioni e il processo decisionale da parte degli operatori di sicurezza
- disponibilità di strumenti di collaboration integrati, efficaci, innovativi, completi, multimediali e semplici, che consentano la condivisione delle informazioni fra gli analisti di sicurezza, al fine di ottimizzare la fase di risposta agli incidenti informatici
- varietà e semplicità di utilizzo dei playbook integrati nella soluzione e adattabilità al contesto specifico dell'Amministrazione, al fine di semplificare e accelerare il processo di risposta agli incidenti di sicurezza.

3.2 SERVIZI BASE INCLUSI NELLA FORNITURA

I servizi base inclusi nella fornitura sono i seguenti:

- installazione e configurazione;
- n. 10 gg/pp di formazione e affiancamento;
- manutenzione della piattaforma e di tutte le sue componenti per 24 mesi dalla data di sottoscrizione della licenza d'uso in modalità Low profile (Lun-Ven 9.00 - 18.00);
- supporto specialistico:
    - 10gg/pp di Servizio di supporto specialistico - Security Principal
    - 15gg/pp di Servizio di supporto specialistico - Senior Security Architect (di cui 5gg devono essere erogate nella fascia oraria Lun-Sab 20.00-7.00 o la domenica o nei giorni festivi)
    - 15gg/pp di Servizio di supporto specialistico - Senior Security Analyst (di cui 5gg devono essere erogate nella fascia oraria Lun-Sab 20.00-7.00 o la domenica o nei giorni festivi)

Si precisa che per giornata di lavoro si intende la fruizione di 8 ore lavorative complessive.

In particolare, per quanto riguarda i servizi di supporto specialistico, le figure professionali coinvolte dovranno avere le caratteristiche riportate in "ALLEGATO A".

4. TEMPISTICHE DI ATTIVAZIONE E COLLAUDO

La soluzione proposta dovrà essere completamente attivata (on boarding) entro 30 giorni dalla data di stipula del contratto.

Entro 30 giorni dall'attivazione del servizio, si terrà una sessione di collaudo nella quale saranno descritte le prove idonee ad accertare la rispondenza della fornitura agli obiettivi descritti al precedente capitolo 3.1.

Al termine del collaudo, PuntoZero e la Ditta fornitrice, sottoscriveranno un apposito verbale che attesti l'esito della fornitura.

5. IMPORTO E DURATA

L'importo massimo complessivo è pari a € 139.000,00 oltre IVA per la durata di 24 mesi.

Il servizio di manutenzione della piattaforma e di tutte le sue componenti avrà una durata di 24 mesi dalla data di sottoscrizione della licenza d'uso in modalità Low profile (Lun-Ven 9.00 - 18.00).

6. PREDISPOSIZIONE DELL'OFFERTA TECNICO-ECONOMICA

Il fornitore dovrà predisporre l'offerta tecnico-economica, sotto forma di relazione di max 30 pagine, con allegati i Curriculum Vitae (CV) del personale che si intende impiegare effettivamente nel servizio., che dovranno possedere i requisiti di cui all'Allegato A - FIGURE PROFESSIONALI.

I curriculum presentati dovranno riguardare un numero di figure tale da coprire i fabbisogni richiesti. Eventuali sostituzioni di personale dovranno essere preventivamente autorizzate da PuntoZero Scarl.

Il fornitore dovrà indicare i nominativi dei professionisti destinati a tale commessa e allegare i relativi curriculum. In corso d'opera il fornitore potrà modificare le risorse solo a fronte di convalida da parte di PuntoZero.

ALLEGATO "A" - FIGURE PROFESSIONALI

Per effettuare il supporto specialistico il Fornitore dovrà prevedere le figure professionali con le caratteristiche riportate nel seguito. Le competenze, le esperienze e le certificazioni devono essere attestate mediante la produzione del relativo curriculum vitae che ne comprovi la veridicità.

Si precisa che, fatto salvo il possesso del diploma di scuola media superiore, i requisiti accademici richiesti per ogni figura (titoli di studio) possono essere utilmente soddisfatti attraverso il possesso di una cultura equivalente, maturata attraverso lo svolgimento di esperienze lavorativo-professionali, pari a:

· **5 (cinque) anni aggiuntivi nel settore ICT** nel caso di laurea specialistica

· **3 (tre) anni aggiuntivi nel settore ICT** nel caso di laurea triennale.

Quindi, ad esempio, per la figura di Security Principal è accettata una risorsa in possesso di diploma ma con esperienza lavorativa di almeno 15 anni (di cui almeno 5 anni di provata esperienza nella specifica funzione).

Figura professionale	**Security Principal**
Titolo di studio	Laurea specialistica in discipline scientifiche
Anzianità lavorativa	anzianità lavorativa di almeno 10 (dieci) anni nel settore ICT, da computarsi successivamente alla data di conseguimento della laurea, di cui almeno 5 (cinque) anni di provata esperienza nella specifica funzione
Competenze ed esperienze richieste	- conoscenza della metodologia di Project Management; - esperienza di Project Management in progetti analoghi; - conoscenza approfondita dei processi di Security Governance e Security Management; - conoscenza approfondita delle metodologie di vulnerability assessment, penetration test, compliance management e security audit; - esperienza nel disegno e nella valutazione dei sistemi per la gestione della sicurezza delle informazioni; - conoscenza delle metodologie e degli strumenti operativi richiesti in progetti di IT Security; - conoscenza dei processi e delle procedure operative IT;

	- conoscenza delle tecnologie principali per la sicurezza IT.

Figura professionale	**Senior Security Architect**
Titolo di studio	Laurea triennale in discipline scientifiche
Anzianità lavorativa	anzianità lavorativa di almeno 8 (otto) anni nel settore ICT, da computarsi successivamente alla data di conseguimento del diploma di laurea, di cui almeno 4 (quattro) anni di provata esperienza nella specifica funzione
competenze ed esperienze richieste	- capacità di comprendere l'infrastruttura sotto analisi e le relazioni tra i differenti sistemi e componenti infrastrutturali; - esperienza nell'analisi e nella valutazione delle configurazioni e delle regole tecniche delle principali soluzioni di sicurezza utilizzate per proteggere l'infrastruttura e i servizi (Firewall, IPS/IDS, SIEM, soluzioni anti-malware, Web Application Firewall, Database Monitoring, servizi Anti-DDoS, servizi cloud oriented per la sicurezza, ecc.); - esperienza nell'analisi di un'infrastruttura IT complessa volta all'individuazione di problematiche architetturali che ne potrebbero compromettere la sicurezza; - esperienza nella verifica dell'efficacia delle misure tecniche ed organizzative preposte alla sicurezza di un'infrastruttura IT complessa; - consolidata esperienza nella progettazione della sicurezza ICT maturata in contesti analoghi; - conoscenza approfondita delle problematiche di sicurezza delle infrastrutture IT; - conoscenza delle metodologie e degli strumenti operativi richiesti per verificare l'efficacia delle contromisure di sicurezza poste a salvaguardia delle infrastrutture IT; - esperienza nell'identificazione di soluzioni tecnologiche ed organizzative da porre in essere per ottimizzare e migliorare le configurazioni e le politiche e per traguardare la piena adozione delle contromisure previste; - conoscenza delle tecnologie principali per la sicurezza IT, soprattutto in ambito sicurezza cloud, sicurezza minacce di nuova generazione, modalità di

	contenimento, ecc.; - ottima conoscenza sistemi di correlazione eventi, progettazione regole di correlazione e tuning sistemi di analisi eventi con esperienza di integrazione in contesti analoghi; - buona conoscenza sistemi di autenticazione, specialmente sistemi di Identity & Access Management con esperienza di integrazione su ambienti analoghi; - conoscenza delle tecnologie in uso nel contesto di riferimento, con esperienza nella configurazione e nell'inserimento in rete delle stesse, in funzione delle minacce riscontrate.

Figura professionale	**Senior Security Analyst**
Titolo di studio	Laurea triennale in discipline scientifiche
Anzianità lavorativa	anzianità lavorativa di almeno 6 (sei) anni nel settore ICT, da computarsi successivamente alla data di conseguimento del diploma di laurea, di cui almeno 4 (quattro) anni di esperienza nella specifica funzione
Competenze ed esperienze richieste	- capacità di coordinamento dei Consulenti Junior; - conoscenza dei processi e delle procedure operative IT; - conoscenza approfondita dei processi di Incident Handling ed Escalation per la gestione degli incidenti di sicurezza informatica; - conoscenza approfondita dei processi di analisi forense, acquisizione degli elementi probatori e conservazione degli stessi; - conoscenza approfondita dei sistemi di rilevazione e analisi degli allarmi; - esperienza consolidata nell'analisi tecnica di incidenti all'interno di strutture SOC o CERT nell'ambito della Pubblica Amministrazione; - esperienza consolidata nella gestione delle attività di supporto agli organi di Polizia Giudiziaria in caso di illeciti informatici;

	- esperienza consolidata nella definizione proattiva di configurazioni e analisi di sicurezza; - esperienza nella definizione di regole di correlazione e nel tuning delle stesse; - conoscenza dei processi di reverse engineering dei malware ed esperienza consolidata nella analisi forense di malware mediante strumenti di analisi e attività di reverse; - conoscenza approfondita dei protocolli di rete e della tipologia di traffico all'interno di un contesto complesso con esperienza consolidata nell'analisi forense del traffico di rete e nell'identificazione di anomalie o elementi a supporto per la corretta gestione degli incidenti di sicurezza.

Inoltre, deve essere previsto l'impiego di personale in possesso di certificazioni in ambito *security* secondo quanto previsto nella seguente tabella.

Security Principal	Almeno il 50% di risorse offerte (arrotondato all'unità superiore) in possesso della certificazione ISACA CISM (Certified Information Security Manager)
Senior Security Architect	Almeno il 50% di risorse offerte (arrotondato all'unità superiore) in possesso della certificazione (ISC)^2 CISSP (Certified Information System Security Professional)
Senior Security Analyst	Almeno il 50% di risorse offerte (arrotondato all'unità superiore) in possesso di almeno una delle seguenti certificazioni: GIAC Certified Incident Handler (GCIH) e/o EC-Council CSA (Certified SOC Analyst) e/o CompTIA CySA+ (Cyber Security Analyst) e/o GIAC Certified Intrusion Analyst