PRESENTAZIONE OFFERTA

per

ARES Sardegna
Proroga servizi di sicurezza

Versione 1.0

FASTWEB
un passo avanti

INDICE

1 Esigenze dell'Amministrazione

L'Amministrazione ha manifestato l'esigenza prorgare i servizi attivati attraverso la convenzione SPC Cloud Lotto 2, per avere continuità dei servizi in vista dell'adesione al nuovo Accordo Quadro 2296.

2 Descrizione della soluzione proposta

Di seguito la lista dei servizi previsti nella fornitura.

Id servizio	Titolo	Descrizione
L2.S3.4	Vulnerability Assessment	Servizio di verifica dinamica della sicurezza dei dispositivi di rete allo scopo di identificare eventuali vulnerabilità, configurazioni di sicurezza errate, carenze sui livelli di protezione attivi che espongano il contesto ad attacchi interni ed esterni
L2.S3.10	Servizi di Monitoraggio	I servizi di monitoraggio consentono alle Amministrazioni l'individuazione e la prevenzione dei rischi derivanti dagli attacchi informatici.

Di seguito i dettagli delle varie componenti

2.1 Vulnerability Assessment

Obiettivi del Servizio VA

L'obiettivo del Servizio è fornire le attività di *Vulnerability Assessment* (di seguito VA) di tipo infrastrutturale per il perimetro di riferimento dell'Amministrazione per disporre di un quadro completo delle vulnerabilità presenti all'interno della propria infrastruttura IT, tramite lo svolgimento di verifiche tecniche orientate alla sicurezza, al fine di ricavarne indicazioni sulle potenziali debolezze e lacune che potrebbero essere sfruttate e su eventuali ulteriori interventi che occorre porre in essere per aumentarne la robustezza.

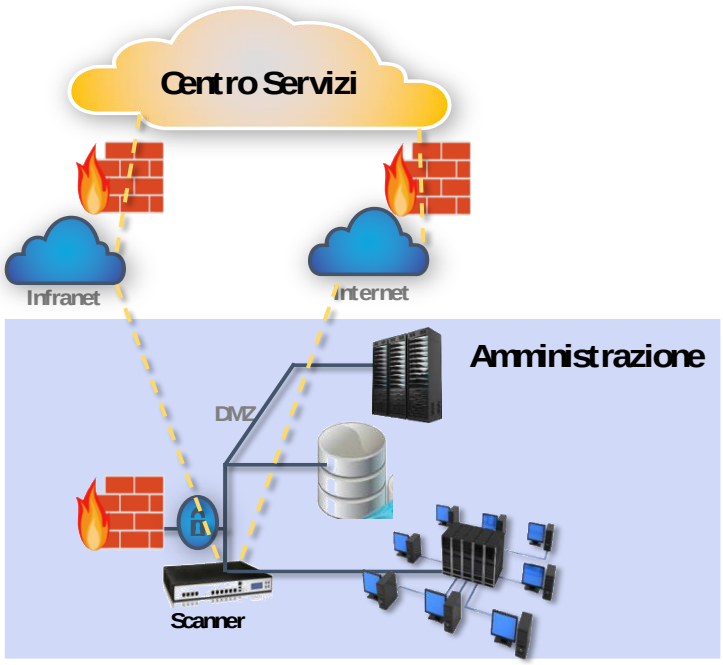
Descrizione del Servizio VA

Il servizio si compone di specifiche fasi di seguito dettagliate:

1. *Information* Gathering (avviamento al servizio): Durante questa fase viene eseguita la raccolta automatica delle configurazioni e della topologia di rete per la definizione dei profili di scansione, ovvero:
    - Operazione di *network discovery* della rete: rilevazione attiva e passiva di ogni nuovo dispositivo installato nella rete; questo riduce in maniera significativa il rischio associato alle risorse non protette e non governate dalle Amministrazioni collegate alla rete includendo apparati, porte, sistemi, servizi, applicazioni;
    - Valutazione di tutti gli indirizzi IP attivi e non attivi all'interno di un determinato intervallo.

2. *Individuazione delle vulnerabilità (Operations):* sono eseguite scansioni rapide condotte in tutta la rete (con cadenza periodica) per trovare le eventuali falle di sicurezza e ridurre i rischi di esposizione, evidenziando l'aderenza o meno alle normative vigenti tramite raccolta, correlazione e reportistica delle informazioni rilevate durante le scansioni. Le scansioni applicano una combinazione di controlli attivi (quali l'invio di pacchetti e l'analisi in remoto) e controlli di correlazione passiva.
3. *Assegnazione della priorità alle vulnerabilità (Operations)*: avviene in ottica di risoluzione e mitigazione del rischio attraverso la comprensione dell'intero contesto di rete.
   Il rischio di ogni vulnerabilità è classificato tramite un algoritmo basato su fattori come impatto o facilità di sfruttamento. Le vulnerabilità scoperte possono essere filtrate per asset, rete, servizio o tipo di vulnerabilità permettendo di produrre reportistica personalizzata secondo le esigenze dell'Amministrazione.

L'architettura di riferimento del servizio è rappresentata in **Error! Reference source not found.**:



L'Amministrazione può beneficiare di una completa e aggiornata visione delle proprie vulnerabilità e dei relativi rischi connessi che costituiscono fattore abilitante alla gestione proattiva della sicurezza.

Modalità di erogazione del Servizio VA

Il servizio sarà erogato in modalità "as a service" in modalità continuativa e da remoto.

2.2 Database Security

Il servizio garantisce una vasta gamma di controlli della sicurezza per la protezione del database nel suo complesso (dati, procedure o funzioni stored, il sistema di gestione, i server ed i collegamenti di rete associati) allo scopo di salvaguardarne la riservatezza, integrità e disponibilità.

Obiettivi del Servizio

Il servizio consente la protezione in tempo reale delle basi di dati da minacce esterne o interne e consente inoltre la difesa da eventuali exploit di vulnerabilità presenti nei database.

Descrizione del Servizio L2.S3.6

Il servizio di compone delle seguenti funzionalità (elenco non esaustivo):

- monitoraggio in tempo reale di tutte le transazioni del database
- valutazione dei rischi mediante controlli di vulnerabilità;
  individuazione delle alterazioni dei dati, degli utenti e dei profili di accesso;
- creazione personalizzata di policy di sicurezza per soddisfare le normative del settore o gli standard di governance IT interni.

Il servizio può prevedere l'installazione di un software agent "on premise" ed è compatibile con i principali DB quali Oracle, MS SQL Server, IBM DB2, SAP Sybase, MySQL, è invece sempre presente una console di gestione centralizzata.
La piattaforma tecnologica a supporto del servizio Database Security consente all'Amministrazione la protezione in tempo reale delle basi dati da minacce esterne o interne mediante la configurazione di policy "ad hoc" in grado di generare alerting su attività sospette fino al suo eventuale blocco. Tale soluzione è in grado di impostare una vasta gamma di controlli per la protezione dei database. Individua automaticamente i database nella rete, determina se le ultime patch sono state applicate ed esegue test su password deboli, account predefiniti e altre minacce diffuse, abilitando quindi la dimostrazione della conformità e migliorando la protezione delle risorse di dati critiche.

2.3 Servizio di Monitoraggio

Descrizione del SOC (Security Operation Center)

Il SOC, dotato di competenze e tecnologie allo stato dell'arte, è stato realizzato espressamente per garantire la fornitura di Servizi Gestiti di Sicurezza alle grandi realtà Aziendali e Organizzazioni nazionali ed internazionali.

Gli obiettivi del SOC sono:

- Controllare in maniera attiva l'infrastruttura di sicurezza delle reti e dei sistemi attraverso l'attività di monitoring real-time e supervisione degli apparati di sicurezza prevenendo efficacemente gli incidenti di sicurezza;
- Contribuire al governo ed alla gestione della sicurezza delle aziende clienti fornendo servizi di installazione, configurazione e manutenzione sia on-site che presso le proprie strutture dei sistemi hardware e software necessari per l'erogazione dei servizi di sicurezza;
- Erogare servizi professionali di alto profilo, finalizzati ad aiutare i clienti a definire il proprio livello di sicurezza determinando potenziali problemi e le relative aree di intervento.

Il SOC è organizzato come di seguito descritto:

- Help Desk di I Livello; Tale struttura avrà il compito di fornire assistenza tecnica per tutte le eventuali segnalazioni e richieste provenienti dai referenti dell'Amministrazione;
- Gruppo di Supporto Specialistico di II Livello che si occupa del supporto di secondo livello garantendo la copertura H24 per tutti i servizi erogati dal SOC;
- Gruppo di Tecnici "On Site".

Il SOC risponde ad un unico Coordinatore che ha funzione di centro di competenza ed escalation nei confronti di tutti i clienti/servizi cui si applicano i servizi specialistici relativi alla sicurezza.

Servizi di monitoraggio (SOC)

Il Security Operation Center (SOC) è la struttura del centro servizi preposta alla raccolta e correlazione degli eventi provenienti dalle aree operative e tecnologiche dell'Amministrazione al fine di garantire il corretto monitoraggio delle infrastrutture di sicurezza e la tempestiva rilevazione degli incidenti e delle attività sospette.

A livello tecnologico, l'elemento cardine alla base dell'infrastruttura SOC è la piattaforma Security Information Event Management (SIEM) in grado di supportare i servizi di monitoraggio, di detection ed incident management. Una soluzione di SIEM è un sistema in grado di raccogliere ingenti quantità di eventi di sicurezza provenienti da fonti eterogenee e strategiche dell'infrastruttura dell'Amministrazione (firewall, IPS/IDS, antivirus, endopoint protection, nodi di rete, servizi applicativi, directory aziendali, ecc.), di normalizzarle e di correlarle secondo precise regole di indagine personalizzate rispetto al contesto e agli scenari di attacchi informatici applicabili. Il SIEM abilita l'individuazione "in tempo reale" di eventuali anomalie, attacchi e/o compromissioni sottoponendole all'attenzione dell'operatore di sicurezza del SOC che, attraverso una console di gestione specifica, opera una prima verifica per escludere falsi positivi e successivamente trasferire il caso ad un analista di sicurezza dell'unità competente per la gestione e la risposta all'incidente.
Si assumono tutte le tecnologie oggetto del servizio nativamente parsate dalla piattaforma centralizzata: l'eventuale realizzazione di parser ad hoc e connettori dedicati dovrà essere sottoposta a fattibilità da parte del Centro Servizi e legata a valutazione commerciale.

Erogazione

Il Servizio di Monitoraggio sarà erogato in modalità "as a service" da un Security Operation Center (SOC) dislocato all'interno del Centro Servizi. I servizi saranno erogati dal SOC su base continuativa H24 o nelle fasce orarie concordate a seconda delle esigenze dell'Amministrazione. I servizi forniti includono i seguenti elementi:

- **Monitoring & Alerting;**
- **Reporting;**
- **Log Management.**

Monitoring & Alerting

L'elemento di servizio Monitoring & Alerting prevede:

- **L'identificazione di eventuali incidenti,** ossia la fase in cui un attacco o una presunta violazione viene individuata. In particolare, gli eventi rilevati dai dispositivi di sicurezza (firewall, IDS, antivirus ecc.) sono analizzati al fine di determinare, attraverso la correlazione, se si è effettivamente in presenza di potenziali eventi anomali ed incidenti di sicurezza;
- **La classificazione degli incidenti** in cui viene determinato il livello di severità (conformemente a quanto definito nel Lotto 2 della Gara SPC) e l'impatto del potenziale incidente qualora siano stati forniti in fase di Information Gathering da parte dell'Amministrazione la valorizzazione degli Asset. I parametri considerati comprendono la tipologia/categoria di attacco (ad esempio DoS, Malicious Code, Misuse, ecc.) e la valutazione delle criticità che riguardano i target coinvolti;
- **La notifica di eventuali incidenti** e altre anomalie. Stabilita la tassonomia dell'anomalia viene comunicato alle opportune strutture lo stato di allarme (con le informazioni necessarie a qualificarlo) affinché si attivi il processo vero e proprio di contrasto degli incidenti (Incident Response).

Il servizio di Monitoraggio potrà essere esteso alle seguenti tipologie di dispositivi di sicurezza, elencate in modo esemplificativo e non esaustivo, previa verifica parsing delle sorgenti:

- **IDS/IPS e dei Firewall**: monitoraggio in tempo reale dei dispositivi IDS/IPS e dei firewall gestiti dal Centro Servizi del RTI (qualora inclusi nei servizi di Sicurezza previsti per il Lotto2) o dalle funzioni dell'Amministrazione. Questo controllo permette la rilevazione in tempo reale delle minacce segnalate dai suddetti dispositivi e la loro tempestiva segnalazione;
- **Antimalware e Antispam**: monitoraggio in tempo reale dei dispositivi antimalware/antispam gestiti dal Centro Servizi del RTI (qualora inclusi nei servizi di Sicurezza previsti per il Lotto2) o dalle funzioni dell'Amministrazione. Questo controllo permette la rilevazione in tempo reale delle minacce segnalate dalle piattaforme antimalware e la loro tempestiva segnalazione;

- **VPN Gateway**: monitoraggio in tempo reale dei VPN Gateway e degli accessi remoti. Questo controllo permette la rilevazione in tempo reale delle minacce o i tentativi di accesso segnalati dai VPN gateway e la loro tempestiva segnalazione;
- **Internet Proxy/Web Security**: monitoraggio in tempo reale del servizio di navigazione Internet via Proxy gestiti dal Centro Servizi del RTI (qualora inclusi nei servizi di Sicurezza previsti per il Lotto2) o dalle funzioni dell'Amministrazione. Questo controllo permette la rilevazione in tempo reale delle minacce segnalate dalle piattaforme proxy, comprese le eventuali violazioni di policy, o navigazione su URL sospette o compromesse, e la loro tempestiva segnalazione;
- **Web content filtering**: monitoraggio in tempo reale del servizio di web content filtering. Questo controllo permette la rilevazione in tempo reale delle minacce segnalate dalle piattaforme di web content management, comprese le eventuali violazioni di policy, o navigazione su URL non consentite o segnalate, e la loro tempestiva segnalazione;
- **Application control**: monitoraggio in tempo reale del servizio di controllo applicazioni. Questo controllo permette la rilevazione in tempo reale delle minacce segnalate dalle piattaforme di application control, comprese le eventuali violazioni di policy, utilizzo elusivo di applicazioni web non consentite e la loro tempestiva segnalazione;
- **Database Control**: monitoraggio degli accessi ai RDBMS, tramite controllo degli accessi e profili di Audit. Questo controllo permette la rilevazione in tempo reale delle minacce o i tentativi di accesso segnalati RDBMS e la loro tempestiva segnalazione;

Con la finalizzazione della fase di collaudo della soluzione SIEM con esito positivo, viene formalmente attivato il Servizio di Monitoraggio. All'interno del SOC sarà presente un team di specialisti e analisti di sicurezza che controlleranno in maniera continuativa la console di monitoraggio. Tutte le anomalie, laddove previsto dalla classificazione degli eventi/potenziali incidenti, saranno tracciate mediante apertura di un ticket sulla piattaforma di trouble ticketing ad uso del SOC su cui saranno registrate tutte le attività di indagine preliminare atte ad effettuare una prima identificazione e a escludere eventuali falsi positivi. Nel caso di riscontro dell'incidente sarà effettuata la segnalazione alle funzioni preposte alla gestione dell'incidente o a responsabili dell'Amministrazione (in genere a seconda del grado di impatto) secondo apposita procedura di notifica. All'interno della notifica, veicolata mediante vari canali da concordare in fase preliminare, tra cui il canale standard della piattaforma di Trouble Ticket in uso all'Help Desk per la comunicazione con l'Amministrazione, sarà presente un link per accesso diretto al sistema di TT del SOC. Oltre all'accesso al ticket, sicuramente nei casi più critici, il personale dell'Amministrazione dell'Unità Locale di Sicurezza (ULS) e responsabile dei sistemi coinvolti nell'incidente sarà supportato nell'analisi e nella classificazione dell'incidente dall'operatore SOC.
Il Servizio di Monitoraggio prevede oltre all'individuazione e alla comunicazione dell'incidente, anche il continuo miglioramento delle configurazioni delle regole di correlazioni del SIEM (Policy Enforcement) e l'emissione di report periodici.
L'elemento di servizio Monitoring & Alerting sarà erogato in modalità **H24**, per 365 giorni all'anno.

Reporting
Per mantenere la massima compatibilità con i deliverable degli altri servizi di sicurezza previsti a catalogo nel Contratto SPC sono previste due tipologie di report:

- **Executive Summary**, un rapporto di sintesi destinato prevalentemente al management e al personale non tecnico per una comprensione immediata degli attacchi riscontrati. Illustrerà con tecniche di aggregazione di dati e indicatori grafici in modo esaustivo le principali minacce rilevate dalla piattaforma del servizio.
- **Technical Report** un rapporto tecnico con tutte le indicazioni necessarie per la comprensione dei problemi riscontrati, per la loro classificazione in termini di severità e per l'identificazione delle misure più idonee da adottare per la loro risoluzione. Tale rapporto fornirà il dettaglio delle principali vulnerabilità/minacce riscontrate.

Incident Response
L'identificazione di eventuali incidenti ossia la fase in cui un attacco o una presunta violazione viene individuata e circoscritta. In particolare, gli eventi rilevati dai dispositivi di sicurezza verranno classificati come sotto:

- **Livello High;** Grave impatto sull'operatività e conseguente livello di compromissione di servizi e/o sistemi dell'Amministrazione. L'incidente presenta almeno una tra le seguenti condizioni:
    - Impossibilità tecnica di fornire uno o più servizi classificati come critici dall'Amministrazione;
    - Estesa infezione virale in grado di compromettere uno o più sistemi e di propagarsi nella rete;
    - Compromissione di sistemi o di reti in grado di permettere accessi incontrollati a informazioni riservate;
    - Violazione dei siti web;
    - Rilevanti perdite di operatività per clienti interni (dipendenti- collaboratori) ed esterni (cittadini-partner-fornitori);
    - Frode o attività criminale che coinvolga servizi forniti dall'Amministrazione;
    - Perdita di immagine e/o reputazione.
- **Livello Medium**; I servizi e/o sistemi sono parzialmente interrotti o seriamente degradati. L'incidente presenta una tra le seguenti condizioni:
    - compromissione di server e degrado delle prestazioni;
    - attacchi che provocano il funzionamento parziale o intermittente della rete/sistemi/applicazioni;
    - impossibilità tecnica di fornire servizi classificati dall'Amministrazione come non critici;
    - parziale perdita di operatività per un gruppo di clienti interni o esterni;
- **Livello Low;** Modesto impatto sull'operatività e relativi ambienti per l'erogazione dei servizi. L'incidente presenta una tra le seguenti condizioni:
    - informazione (o segnalazione) del rischio di contaminazioni da virus;
    - informazione (o segnalazione) del rischio di intrusione da parte di un attaccante;
    - parziale perdita di operatività per un numero ristretto di clienti interni o esterni.

Il livello di allarme di una severity/minaccia sarà determinato dal personale del SOC attraverso un approccio qualitativo sulla base dei seguenti elementi:

- Categoria e livello di gravità della severity/minaccia (severità);
- Criticità delle risorse IT coinvolte (se disponibili le informazioni).

I valori associati a ciascuno dei due elementi di sicurezza sono assegnati dagli operatori e analisti del SOC sulla base delle informazioni acquisite (eventi pervenuti attraverso la piattaforma SIEM, analisi preliminare effettuata dalle fonti informative, ecc.) e delle specifiche competenze in materia di gestione degli incidenti di sicurezza.
A titolo di esempio si riporta la matrice di correlazione tra il livello di vulnerabilità/minaccia, il relativo livello di gravità e la criticità delle risorse IT coinvolte.

<table>
<tr><th>Minaccia / Classe di Gravità</th><th>Valore Asset</th><th>Tipologia notifica</th><th>Report</th><th>Raccolta monitoraggio e correlazione Log</th></tr>
<tr><td rowspan="2">Livello Low / Avviso</td><td>Non critico</td><td>n/a</td><td rowspan="3">Reporting periodico mensile</td><td rowspan="4">24x7</td></tr>
<tr><td>Critico</td><td>n/a</td></tr>
<tr><td rowspan="2">Livello Medium / importante</td><td>Non critico</td><td>n/a</td></tr>
<tr><td>Critico</td><td>Tramite mail</td></tr>
<tr><td rowspan="2">Livello High / Critico</td><td>Non critico</td><td>Tramite mail</td><td rowspan="2">Report di dettaglio on-demand N.B.D.</td></tr>
<tr><td>Critico</td><td>Tramite mail e/o contatto telefonico</td></tr>
</table>

Le estrazioni di log e analisi su dati storici possono essere richieste nella finestra 8x5 (Festivi esclusi).
I report saranno consegnati con le modalità concordate.

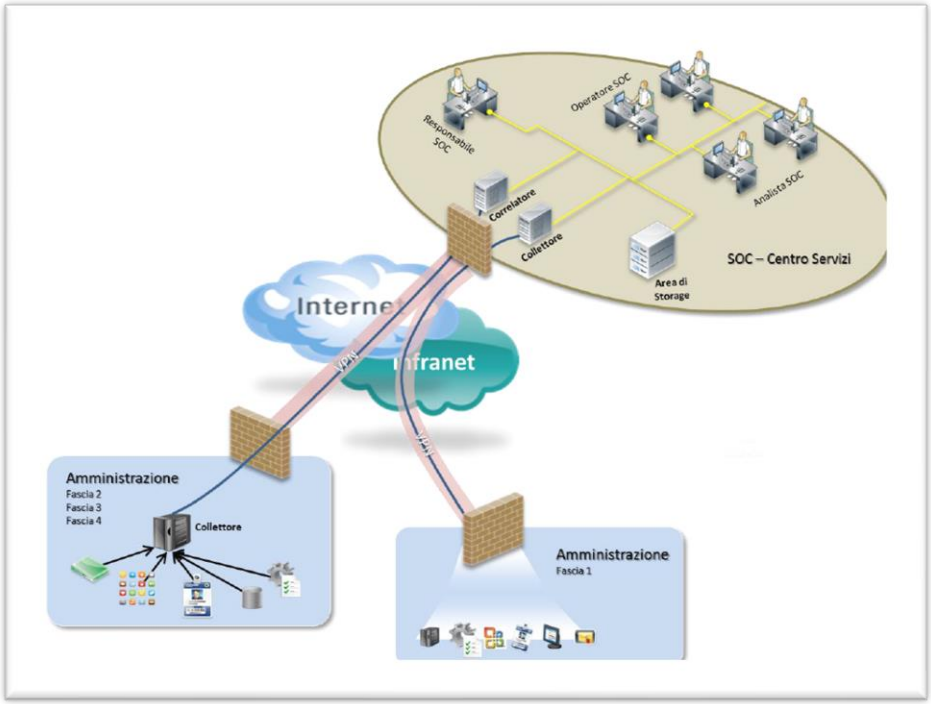
Log Management
L'elemento di servizio Log Management prevede:

- La raccolta dei dati registrati nei log dei dispositivi controllati;
- La possibilità di conservare i file di log nel formato RAW;
- La conservazione dei log relativi ad eventi correlati in modo da preservarne la disponibilità e l'integrità, in accordo ai requisiti imposti dal testo unico sulla privacy e successive modificazioni;
- La conservazione dei dati delle Amministrazioni per almeno 180 giorni, con conseguente applicazione delle politiche di rotazione e cancellazione sicura dei dati anteriori al periodo definito;
- L'attività di gestione della piattaforma (Configuration & change management, fault management);
- Un insieme standard di report;
- La possibilità di estrarre i log in modalità concordate con l'Amministrazione.

Soluzione Tecnologica

Per il Servizio di Monitoraggio (SOC) si utilizza una piattaforma centralizzata di Security Information and Event Management (SIEM). Tale piattaforma consiste in un sistema che associa eventi, minacce e rischi per fornire un potente sistema di intelligence per la sicurezza, risposte rapide in caso di necessità, una ininterrotta gestione dei log.
La soluzione è intrinsecamente scalabile e modulare e si presenta sotto forma di appliance, con alcune componenti virtualizzabili.
L'architettura prevista si articola nelle seguenti componenti:

- Console di Gestione che compone il Layer Application e Presentation installato presso il Centro Servizi ad uso del team specialistico di monitoraggio;
- Sistema di Correlazione e Log Management (Correlatore)che compone il Layer di Data Collecting e Storage installato presso il Centro Servizi;
- Sistema di Raccolta Log (Collettore) che compone il Layer di Data Collecting and Forwarding.



Gli eventi sono raccolti dal cluster di Collettori che integrano anche la funzione di Real Time Correlation. La raccolta degli eventi, tipicamente avviene in modalità “agent-less”. Dal momento che i Collettori vengono proposti in una configurazione di cluster in HA, viene garantita la continuità dei servizi di raccolta dei log e della correlazione in tempo reale in caso di fault del Collettore primario.
Prima di effettuare qualunque elaborazione dei log, il Collettore li firma digitalmente, li comprime, ne effettua un hash e li invia verso l’infrastruttura del centro servizi che ha il compito di mantenere i file di log “raw” inalterati per il tempo di “retention” specificato. Tale tempo di retention può essere diverso e configurato ad hoc a seconda dei casi da gestire, o più precisamente a seconda delle normative cui rispondere. La piattaforma effettua l’archiviazione dei log raw sullo storage. In seguito i log vengono analizzati localmente, normalizzati, indicizzati ed inviati alla piattaforma di analisi.
Nel fare questo i log vengono anche aggregati: questa fase consente di raggruppare più eventi uguali tra loro verificatisi in un intervallo di tempo prefissato in modo da ridurre lo spazio occupato da essi all’interno del database. Come conseguenza dell’operazione di aggregazione, nel DB verranno conservate le seguenti informazioni: time stamp del primo evento aggregato, numero complessivo di eventi verificatisi nell’intervallo di aggregazione, time stamp e dati contenuti nell’ultimo evento aggregato.
Si ribadisce che le elaborazioni effettuate dal Collettore sui log sono “successive” al loro processamento (firma digitale, compressione ed hashing) per l’invio ai successivi moduli che deve mantenere i raw log “originali ed inalterabili nel tempo”. Le soluzioni proposte prevedono i moduli Collettori in cluster HA. Si ricorda che tali Collettori sono le componenti cui è demandata la raccolta dei log e, eventualmente, la correlazione degli eventi in real time. Questa configurazione consente di ottenere un meccanismo di alta affidabilità sia per parte di raccolta dei log che per quella di correlazione degli eventi in tempo reale.
Il processo di switch-over tra un Collettore e l’altro può essere causato da un fault del Collettore Primario, oppure può essere iniziato manualmente. Nel primo caso è compito del Secondario rilevare il fault del Primario. Per quanto riguarda la Console di Gestione, è implementata una configurazione ridondata in cui una seconda appliance contiene un backup completo di tutti i dati e di tutti i settaggi della console principale.
Il Primario contiene i dati “master” e il Secondario li duplica automaticamente all’interno del proprio database. In caso di failover, lo switch è manuale e richiede di effettuare il login sulla Console secondaria e di “Promuovere” il medesimo al ruolo di Console Primaria.

Sistemi soggetti al monitoraggio

Verranno sottoposti a monitoraggio i sistemi indicati dall'Amministrazione fino al raggiungimento nel numero di EPS contrattualizzato. L'eventuale superamento del numero degli EPS dovrà essere soggetto a fattibilità da parte del Centro Servizi e ad una successiva valutazione commerciale.

3 Offerta economica

Le condizioni economiche corrispondono a quelle in vigore per il contratto SPC Cloud Lotto 2.

Nello specifico:

- Componente VA: Canone annuo 16.794,00€
- Componente Database Security: Canone annuo 18.375,00€
- Componente Servizio di Monitoraggio: Canone annuo 102.328,44€

FASTWEB
un passo avanti

INFORMAZIONI E CONTATTI

E-mail
Email Editabile

Grandi Aziende Fastweb
fastweb.it/grandi-aziende/

Riepilogo offerta economica

Stazione Appaltante: ARES - Azienda Regionale della Salute

Oggetto procedura: Servizi di gestione delle identità digitali e sicurezza ICT di ARES Sardegna per un periodo massimo di 12 mesi

Protocollo: 5AF- SPC CLOUD

Ragione sociale del Concorrente: Fastweb Spa

Partita IVA: 12878470157

Codice fiscale: 12878470157

Data creazione offerta: 14/06/2024 16:55

Codice	Descrizione	Base asta	Base asta non ribassabile	Quantità prodotto	Offerta €	Componente VA: Canone annuo	Componente Database Security: Canone annuo	Componente Servizio di Monitoraggio: Canone annuo
1	Servizi di Vulnerability Assessment e Servizi di Monitoraggio per 12 mesi	138500.00			137497.44			
1	Servizi di Vulnerability Assessment e Servizi di Monitoraggio per 12 mesi	138500.00		1.00	137497.44	16794.00	18375.00	102328.44