VERBALE SEDUTA RISERVATA

OGGETTO: verbale seconda seduta riservata del 24 novembre 2023 della commissione tecnica per l'AS sull'AQ ID 2174 per il progetto indicato.

PROGETTO: Avviso 3/2022 della Agenzia per la Cybersicurezza Nazionale - Piano Nazionale di Ripresa e Resilienza (PNRR) Missione 1 – Componente 1 – Investimento 1.5 "Cybersecurity" finanziato dall'Unione europea – Next generation EU – Progetto Framework & Tools - CUP H16G22000340006. Adesione all'Accordo Quadro Consip per la fornitura di prodotti per la gestione degli eventi di sicurezza e degli accessi, per la protezione dei canali e-mail, web e dati ed erogazione di servizi connessi per le Pubbliche Amministrazioni (ID 2174 - Cybersicurezza 1). Appalto per la fornitura di prodotti di Cybersecurity: strumenti SWG e WAF – CIG A01FDC90F5

L'anno 2023 e questo giorno 24 del mese di novembre, alle ore 09:00 in Firenze, tramite seduta telematica, in esecuzione delle Determinazioni n. 8594/2023 e della 9552/2023 di cui alla procedura negoziata n. 3815049 /2023 sul Mercato Elettronico per la Pubblica Amministrazione (MEPA) si riunisce, in seduta riservata, la Commissione tecnica nominata con Determinazione n. 9553 del 21/11/2023 e così composta:

- **Luca Bertelli**, Dirigente del Servizio Sicurezza, Infrastruttura e Architettura IT dell'Ente – Direzione Sistemi Informativi – in qualità di RUP e di Presidente della Commissione;
- **Marco Mencacci**, Dirigente del Servizio Sviluppo Infrastrutture Tecnologiche – Direzione Sistemi Informativi – in qualità di membro;
- **Avvisano Edoardo**, Istruttore Informatico della E.Q. Data Center, Sistemi e Cloud – Direzione Sistemi Informativi – in qualità di membro.

Il RUP informa che il Concorrente ha fornito, tramite scambio PEC avvenute in soccorso procedimentale, il chiarimento richiesto e ha così risolto l'ambiguità presente nell'offerta tecnica come rilevata nel precedente verbale: il prodotto offerto dal Concorrente è afferente alla fascia 3, cioè quella rispondente fino a 10.000 utenti. La PEC di richiesta è il protocollo generale n° 376221 del 23/11/2023 e la PEC di risposta del concorrente è il protocollo generale n° 376896 del 23/11/2023 (si sono scordati gli allegati) e n° 376906 del 23/11/2023 (PEC completa).

Si riprende, pertanto, dalla lettura dell'offerta tecnica con il controllo e riscontro del rispetto dei **requisiti minimi obbligatori**, come richiesti dal Capitolato Tecnico all'articolo 4, per capire se il Concorrente ha presentato un'offerta tecnica congrua.

Si riporta una tabella dei requisiti obbligatori con una colonna compilata quanto riscontrato nell'offerta tecnica presentata dal Concorrente, indicando se il riscontro, in base alla documentazione presentata, sia

Positivo oppure Negativo e prevedendo la possibilità di integrare con delle note sintetiche a completamento della valutazione, se ritenuto opportuno dalla Commissione.

Per quanto non dettagliato, completo o sufficientemente esaustivo in offerta tecnica, la Commissione decide di ricorrere ai dati presenti nel datasheet ufficiale del produttore Stormshield per l'apparato SN6100, per il modulo Log Supervisor e il Barracuda BWF964D offerti in gara.

REQUISITI OBBLIGATORI DEL PRODOTTO OFFERTO	RISCONTRO
Secure Web Gateway (SWG) – Stormshield SN6100 NB: informazioni presenti nel capitolo 2 dell'offerta tecnica e nei datasheet già indicati	
SWG_3 (fascia 3): fino a 10.000 utenti	Positivo (in base all'esito del soccorso procedimentale)
Configurazione in alta affidabilità	Positivo (paragrafo 2.2)
Ciascuna appliance: • 8 interfacce 10/100/1000 base T • 8 interfacce SFP complete di relativo Transceiver 1000 Base LX • 14 interfacce di tipo SFP/SFP+ (1/10 Gbps) equipaggiate con moduli SFP Fibra ottica SR 10/1 Gbps autosense • Possibilità di equipaggiare moduli con ciascuno 2 porte da 40 Gbps • Doppio SSD almeno da 1 TB in RAID 1 • Funzionalità di Breach fighter (sandboxing) e advanced antivirus • Mandatorio disporre di un'interfaccia IPMI per la gestione remota dell'hardware, questa funzione è indispensabile per ottenere una gestione completa dell'hardware da remoto, monitorare le componenti e controllare completamente l'appliance (control, reboot, interruption, etc.). Questa interfaccia deve essere operativa a prescindere dallo stato del firewall e della relativa configurazione.	Positivo
Performance Minime: • Firewall throughput (1518 byte UDP) 170 Gbps • Firewall throughput (IMIX**) 53.3 Gbps • IPS throughput (1518 byte UDP) 68 Gbps • IPS throughput (1 MByte HTTP files) 27 Gbps • Antivirus throughput 12.5 Gbps	Positivo
VPN • IPSec throughput - AES-GCM 20 Gbps • IPSec throughput - AES256/SHA2 12.3 Gbps • Max number of IPSec VPN tunnels 10,000 • Max number of SSL VPN (Portal mode) 2,048 • Number of simultaneous SSL VPN clients 500	Positivo
NETWORK CONNECTIVITY • Concurrent connections 20,000,000 New connections per second 250,000 • Number of main gateways (max)/backup (max) 64/64	Positivo
Struttura modulare con almeno 7 slot: • 10/100/1000 interfaces 8-64 • 10 Gb copper interfaces 0-32	Positivo

• 1 Gb fiber interfaces 0-64 • 10 Gb fiber interfaces 2-34 • 40 Gb fiber interfaces 0-16	
SYSTEM • Number of rules (recommended / specific configuration) 8192 / 32768 • Max Number of static routes 10240	Positivo
REDUNDANCY • High Availability (Active/Passive) • Redundant SSD RAID 1 • Redundant power supply (hot swappable) • Redundant ventilation (hot swappable)	Positivo
HARDWARE • MTBF non inferiore a 20 anni a 25 gradi centigradi • Compliance CE/FCC/CB • Certificazione Europea ANSSI e BSI	Positivo
USAGE CONTROL • Firewall/IPS/IDS mode • Identity-based firewall • Application detection and management • Microsoft Services Firewall • Industrial firewall/IPS/IDS • Industrial application control • Detection and control of the use of mobile terminals • Application inventory • Vulnerability detection • Geolocation (countries, continents) • Dynamic Host Reputation • URL filtering (embedded database or cloud mode) • Transparent authentication (Active Directory, SSO Agent, SSL, SPNEGO) • Multiuser authentication in cookie mode (Citrix-TSE) • Guest and sponsorship mode authentication, webservices	Positivo
PROTECTION FROM THREATS • Intrusion detection and prevention • Protocols autodetection and compliancy check • Application inspection • Protection from denial of service attacks (DoS) • Protection from SQL injections • Protection from Cross-Site Scripting (XSS) • Protection from malicious Web2.0 code and scripts (Clean & Pass) • Trojan detection • Detection of interactive connections (botnets, Command&Control) • Protection from data evasion • Advanced management of fragmentation • Automatic reaction to attack (notification, quarantine, block, QOS, dump) • Antispam and antiphishing: • reputationbased analysis, heuristic engine • Embedded antivirus (HTTP, SMTP, POP3, FTP) • SSL decryption and inspection - VoIP protection (SIP)	Positivo

• Collaborative security: IP reputation, cloud based Sandbox on the European territory (option) • Traffic Geolocalization	
CONFIDENTIALITY • Site-to-site or nomad IPSec VPN • Remote SSL VPN access in multi-OS tunnel mode (Windows, Android, iOS, etc.) • SSL VPN agent with automatic configuration (Windows) • Support for Android/ iPhone IPSec VPN	Positivo
NETWORK – INTEGRATION • IPv4 e IPv6 • NAT, PAT, transparent (bridge)/routed/hybrid modes • Dynamic routing (RIP - OSPF - BGP) - Multiple link management (balancing, failover) • Multi-level internal or external PKI management • Multi-domain authentication (including internal LDAP) • Explicit proxy • Policy-based routing (PBR) • QoS management • DHCP client/relay/server • NTP client • DNS proxy-cache • HTTP proxy • LACP management che dovrà esser consentito in caso di aggregazione di interfacce indispensabile per l'associazione allo stack degli switch di core presenti • Spanning-tree management (RSTP/ MSTP) • SD-WAN • Multifactor Authentication (MFA)	Positivo
MANAGEMENT • Web-based management • Interface with privacy mode (GDPR compliant) • Object-oriented security policy • Contextual security policy • Real-time configuration helper • Rule counter • Multiple installation wizards • Global/local security policy • Embedded log reporting and analysis tools • Interactive and customizable reports • Support for multiple syslog server UDP/TCP/TLS - SNMP v1, v2c, v3 agent - IPFIX • Automated configuration backup • Open API • Script recording	Positivo
LOG SERVER (RIDONDATO) n. 2 istanze licenziate e contemporanee di Log Supervisor, installabile su piattaforma vmWare, con certificazione EAL3+ che deve garantire: • Advance log analysis • Compliance years of legal archive • Report manual & automatic	Positivo

• Central Log Management	
LOG MANAGEMENT • Event collection via syslog (TCP & UDP) • Secure collection via syslog-TLS • Syslog Forwarder function • Events Per Second (EPS): 10,000+ • Normalisation and native indexing of SNS & SES logs • Log management over multiple years (1+ years) • Number of firewalls: 500+	Positivo
SEARCH TYPES • Simple search • Multicriteria advanced search (log type, time, etc.) • Predefined searches • Results displayed as raw logs, normalised logs and graphical logs • Enrichment with external sources (CSV, IPtoHost, LDAP, GeoIP) • Navigation through time (minutes, hours, days, specific time range) • Search history • Results exported in CSV format	Positivo
ALERTS AND INCIDENT MANAGEMENT • Automatic generation based on pre-established rules • Management of alert criticality (4 levels) • Incidents assigned to administrators for resolution, with resolution tracking REPORTS • Manual or automatic generation (hour, day, week or month) • Customised layout or predefined templates • Report format: PDF, HTML, XLS, DOCX, CSV • Reports sent by email	Positivo
Prodotto deve risultare non soggetto a legge federale USA Cloud ACT e Patriot ACT, o di qualsiasi altro ente non espressamente autorizzato	Positivo (azienda multinazionale con sede legale in Francia)
Requisiti di cui alla pagina 10 del Capitolato Tecnico	Positivo (NB: questi requisiti sono un approfondimento e un maggior dettaglio tecnico di quanto già riportato come requisiti e caratteristiche nei punti precedenti)
Web Application Firewall (WAF) – Barracuda BWF964D NB: informazioni presenti nel capitolo 3 dell'offerta tecnica e sul datasheet indicato	
WAF_2 (fascia 2): fino a 5 Gbps di throughput HTTP	Positivo
Funzionalità di bilanciamento di livello 7 (modello ISO/OSI) delle Applicazioni	Positivo
Configurazione in alta affidabilità	Positivo
Protezione SIA dagli "OWASP Top 10 Web Application Risks" SIA dagli "OWASP Top 10 API Security Risks" (questa nuova catalogazione elaborata da OWASP è molto importante perché rappresenta una nuova e pericolosa categoria di attacchi di nuova generazione focalizzati sulle API, ormai dominanti negli applicativi Web di	Positivo (presente nel paragrafo 3.1 dell'offerta tecnica)

nuova generazione	
Disponibilità sia di funzionalità di API Discovery (JSON e XML), che di funzionalità di API Security nella soluzione (JSON e XML)	Positivo
Protezione BOT avanzata, quindi non solo legata a Database di BOT conosciuti, ma anche alla disponibilità di un ambiente di Intelligenza Artificiale/Machine Learning nel cloud del Vendor	Positivo
Protezione non solo da attacchi DDOS di tipo Applicativo, ma anche da attacchi DDOS di tipo Volumetrico	Positivo
Protezione completa in relazione all'Upload di file verso gli applicativi Web, vale a dire disponibilità sia di una protezione Antivirus/Antimalware "signature" based, sia di un ambiente di Advanced Threat Protection basato su Sandbox nel cloud del Vendor	Positivo
Utilizzo delle Smart Signatures sviluppate dal Vendor. Tali signatures vengono raggruppate in "gruppi" per consentire una significativa ottimizzazione della memoria e velocità di rilevamento rispetto alle signatures "statiche". Ogni signature all'interno di un gruppo ha la capacità di rilevare gli attacchi trovati in 40 signatures standard, e questo è un netto vantaggio se comparato con la tipica sicurezza basata su firma disponibile con altri WAF, in cui ogni firma è specifica per una vulnerabilità o un attacco e la loro corrispondenza richiede molto tempo	Positivo
Pieno supporto per l'Identity e l'Access Control; quindi, supporto non solo di utenti/gruppi locali, ma soprattutto supporto LDAP/AD. Radius, Kerberos v5, SMS Passcode, OKTA, SAML, Azure AD, DUO, RSA Secure ID, OpenID Connect, JWT arrivando fina al supporto MFA	Positivo
Disponibilità di un tool gratuito ed integrato per fare dei Vulnerability Scanner, da poter usare anche come Automatic Remediation Service	Positivo
Virtual Patching integrabile con più di 20 differenti Vulnerability Scanners	Positivo
Pieno supporto della Client-Site Protection per la difesa contro gli attacchi alla Supply Chain delle aziende	Positivo
Protezione sia dal furto di informazioni relative alla struttura degli applicativi Web (Website Cloaking) sia dal furto di dati sensibili (Outbound Data Theft Protection)	Positivo
Possibilità non solo di bloccare attacchi geograficamente identificati (Geo IP), ma anche categorizzati all'interno di DataBase costantemente aggiornati (nodi TOR, per esempio, piuttosto che Proxies pubblici, etc.)	Positivo
Completo supporto di funzionalità di Application Delivery Control; nella fattispecie supporto di TLS/SSL Offloading, Load Balancing, Content Routing, Caching e Compressione, supporto di soluzioni di HSM come Gemalto, supporto IPv6, supporto FTP/S, Website e URL Translation	Positivo
Possibilità di esportazione dei log tramite Syslog e piena integrazione con le più diffuse piattaforme SIEM/SOAR (Splunk, ARCsight, Azure Sentinel, RSA enVision, IBM Qradar, Symantec, Sumologic, Loggly, Azure Event Hub ed altre ancora)	Possibilità
La soluzione WAF deve essere disponibile per l'installazione on-prem, sia in modalità HW-based che Virtual-based e, nell'ottica di possibili progetti futuri, deve essere anche disponibile sui più diffusi Cloud pubblici come AWS, Google Cloud e Microsoft Azure oltre ad essere disponibile in modalità WAF-as-a-Service (su Cloud del produttore stesso)	Possibilità
La soluzione deve essere riconosciuta come "Strong-Performer" dal Forrester Wave dedicato alle soluzioni WAF	Possibilità

Si procede adesso con la valutazione delle caratteristiche migliorative e l'assegnazione dei punteggi della tipologia 'D' (discrezionali) e 'T' (tabellari) come già indicato nel primo verbale riservato del 23/11/2023 utilizzando come strumento di supporto gli schemi allegati al presente verbale.

A conclusione delle valutazioni, al termine delle operazioni il punteggio tecnico finale attribuito per caratteristiche migliorative dell'Appalto Specifico all'unica offerta presentata risulta il seguente:

Telecom SpA: **29,2000** punti (ventinove virgola due).

Dell'allegato di supporto all'Appalto Specifico previsto dall'Accordo Quadro ID 2174, si riporta sotto lo schema sintetico della componente tecnica ovverosia il punteggio assegnato dalla Commissione e i punti ereditati dall'AQ stesso, precisando che Fastweb e Vodafone non hanno presentato alcuna offerta per questo Appalto Specifico, ma il documento previsto all'AQ non è modificabile; quindi, sono riportate anche le righe per queste due aziende. Come riportato nello schema sottostante, complessivamente il concorrente ha conseguito **59,2194** punti tecnici (cinquantanove,2194).

Componente Tecnica

Punteggio Tecnico dell'AS - PT AS	39
Punteggio Tecnico massimo ereditabile - PT ER	31
Parametro K	1,0164
Punteggi tecnici ereditati dalla fase di AQ	
RTI Fastweb	29,6472
RTI Telecom	30,0194
RTI Vodafone	25,1192
Punteggi tecnici assegnati dall'Amministrazione in AS (arrotondati alla 4 cifra decimale)	
RTI Fastweb	0
RTI Telecom	29,2
RTI Vodafone	0
Punteggi tecnici complessivi di AS	
RTI Fastweb	29,6472
RTI Telecom	59,2194
RTI Vodafone	25,1192

La Commissione rimanda al RUP le successive azioni per la conclusione della procedura.

Alle 11.30 la Commissione termina la seduta.

Letto, approvato e sottoscritto.

LUCA BERTELLI
Comune di Firenze
27.11.2023 12:14:10
GMT+01:00

Il Presidente	Commissario	Commissario
FIRMATO DIGITALMENTE		
Luca Bertelli	Marco Mencacci	Edoardo Avvisano

NB: la Commissione concorda che i due commissari firmano la versione cartacea del presente verbale, la stessa sarà poi scansionata formato PDF e firmata digitalmente dal solo Presidente.