Classificazione documento: Ambito pubblico

Gara a procedura aperta per l'affidamento di un Accordo Quadro avente ad oggetto la fornitura di soluzioni per protezione e resilienza delle reti e dei sistemi informativi ed erogazione di servizi connessi per le pubbliche amministrazioni (ID 2733)

Il presente errata corrige sarà visibile su: www.consip.it, www.acquistinretepa.it e www.mef.gov.it

***

ERRATA CORRIGE

A. Modifiche al Capitolato Tecnico Generale:

A.1) Al paragrafo 9.1 «Responsabile Unico delle Attività Contrattuali (RUAC)», la previsione:

"*Il profilo professionale minimo per la figura del RUAC dovrà corrispondere al profilo Security Principal presente nel rispettivo Capitolato Tecnico Speciale del Lotto di riferimento*."

deve intendersi sostituita dalla seguente:

"Il profilo professionale della figura del RUAC dovrà corrispondere al profilo Security Principal presente nel rispettivo Capitolato Tecnico Speciale del Lotto di riferimento, con esclusivo riferimento alle caratteristiche relative al titolo di studio e all'anzianità lavorativa."

A.2) Modifica al paragrafo 11 "Prescrizioni relative alla cybersicurezza"

Al paragrafo 11 "Prescrizioni relative alla cybersicurezza" del Capitolato Tecnico Generale, nella tabella relativa al Lotto 4, con riferimento al prodotto "Security Orchestration, Automation and Response - SOAR", la previsione:

"*Categoria 4, 19*"

deve intendersi sostituita dalla seguente:

"*Categoria 5, 19*".

A.3) Modifica al paragrafo 6.3 "Service Desk"

Al paragrafo 6.3 "Service Desk" del Capitolato Tecnico Generale, le previsioni:

"*attivo con operatore nella fascia oraria Lun-Ven 9.00 – 18.00 per quanto attiene le richieste di cui al precedente punto a) e b);*

attivo con operatore nella fascia oraria relativa al profilo di servizio eventualmente contrattualizzato dall'Amministrazione Contraente (cfr. paragrafo 2.2.4 del Capitolato Tecnico Speciale relativo ai lotti 2, 3 e 4) per quanto attiene le richieste di cui al precedente punto c) e d)."

devono intendersi sostituite dalle seguenti:

"*attivo con operatore nella fascia oraria Lun-Ven 9.00 – 18.00 per quanto attiene le richieste di cui ai precedenti punti a), b) e c);*

attivo con operatore nella fascia oraria relativa al profilo di servizio eventualmente contrattualizzato dall'Amministrazione Contraente (cfr. paragrafo 2.2.4 del Capitolato Tecnico Speciale relativo ai lotti 2, 3 e 4) per quanto attiene le richieste di cui al precedente punto d)."

B. Modifiche al Capitolato Tecnico Speciale Lotti 2, 3, 4:

B.1) Al paragrafo 2.1.1.1, Tabella 1, con riferimento al prodotto WAAP in formato Cloud/SaaS, la metrica:

"*Classi di richieste o N. applicazioni*"

deve intendersi sostituita dalla seguente:

"Classi di richieste mensili o N. applicazioni."

B.2) Al par. 2.1.3.2 in tabella 7

- si intendono eliminati i seguenti requisiti:

~~*"Dashboard di monitoraggio in tempo reale con funzionalità drill-down almeno per: Attacchi, Sessioni, dati Geografici di accesso."*~~

~~*"Funzionalità di Data Loss Prevention."*~~

~~*"Ispezione del traffico FTP e delle versioni sicure da esso derivanti."*~~

- con riferimento al requisito:

"*Possibilità di interrogare la base dati della soluzione tramite API*."

si precisa che, per mero refuso, il requisito è stato riportato due volte nella medesima tabella. La presente correzione è pertanto volta esclusivamente a eliminare la duplicazione, restando fermo e invariato il requisito nella restante occorrenza.

B.3) Al paragrafo 2.2.1.2 - Collaudo iniziale e Verifica di conformità in corso di esecuzione, con riferimento alle forniture erogate in formato Cloud/SaaS, la previsione:

"*le stesse, e la rispettiva remunerazione, decorreranno dalla rispettiva "Data di Accettazione della Fornitura" conseguente al Collaudo iniziale di cui al presente paragrafo, e avranno una durata di 36 mesi*"

deve intendersi sostituita dalla seguente:

"le stesse, e la rispettiva remunerazione, decorreranno dalla rispettiva "Data di Accettazione della Fornitura" conseguente al Collaudo iniziale di cui al presente paragrafo *e avranno la durata determinata dall'Amministrazione, fino a un massimo di 36 mesi.*"

B.4) Al paragrafo 2.2.3 - Servizio di monitoraggio e aggiornamento software/firmware (incluso nella fornitura), la previsione:

"*Gli aggiornamenti di firmware/software dovranno essere garantiti dal Fornitore all'Amministrazione per la durata di 36 mesi, decorrenti dalla data di accettazione della fornitura del rispettivo prodotto. Si intendono incluse nel servizio tutte le eventuali nuove minor release e le licenze/subscription che garantiscano il corretto funzionamento del prodotto per 36 mesi dalla "Data di accettazione" della fornitura del rispettivo prodotto*."

deve intendersi sostituita dalla seguente:

"Per i prodotti offerti in formato Appliance Fisica, gli aggiornamenti firmware/software dovranno essere garantiti per 36 mesi decorrenti dalla Data di Accettazione della relativa fornitura. Si intendono incluse nel servizio tutte le eventuali nuove minor release e le licenze/subscription necessarie a garantire il corretto funzionamento del prodotto per il medesimo periodo.

Per i prodotti offerti negli ulteriori formati tecnologici, gli aggiornamenti firmware/software dovranno essere garantiti per l'intera durata della relativa fornitura, fino a un massimo di 36 mesi, decorrenti dalla Data di Accettazione della fornitura del rispettivo prodotto.

Si intendono incluse nel servizio tutte le eventuali nuove minor release e le licenze/subscription necessarie a garantire il corretto funzionamento del prodotto per l'intera durata della relativa fornitura."

B.5) Al par. 2.2.6.2 la previsione:

- "*8 ore lavorative complessive nella fascia oraria Lun-Sab 20.00-7.00 o la domenica o nei giorni festivi (fascia straordinaria)*."

  d**eve intendersi sostituita come segue**:

- "*8 ore lavorative complessive nella fascia oraria Lun-Sab 20.00-**8.00** o la domenica o nei giorni festivi (fascia straordinaria)*."

B.6) Al paragrafo 2.1.5.5 «Requisiti della eXtended Detection and Response (XDR)», nella Tabella 21 – Requisiti funzionali minimi per tutte le fasce di XDR, la previsione:

"*La soluzione deve consentire la rilevazione e il blocco di minacce sulla base di signature note (signature based).*"

deve intendersi integrata come segue:

"La soluzione deve consentire la rilevazione e il blocco di minacce sulla base di signature note (signature based). *Il requisito può essere soddisfatto anche mediante le funzionalità oggetto dei criteri migliorativi XDR 5.7, 5.10 e 5.12, ove offerte, purché le stesse, singolarmente oppure in combinazione, consentano la rilevazione e il blocco delle minacce note.*"

B.7) Al paragrafo 2.1.5.1 «Requisiti dell'Endpoint Protection Platform (EPP)/Endpoint Detection & Response (EDR)», nella Tabella 17 – Requisiti funzionali minimi per tutte le fasce di EPP/EDR, la previsione:

"*Presenza di un set di signature già presenti sulla soluzione per permettere la protezione fin dal primo utilizzo*."

deve intendersi integrata come segue:

"Presenza di un set di signature già presenti sulla soluzione per permettere la protezione fin dal primo utilizzo. *Il requisito può essere soddisfatto anche mediante le funzionalità oggetto dei criteri migliorativi EPP/EDR 1.11 e 1.12, ove offerte, purché le stesse, singolarmente oppure in combinazione, consentano l'identificazione e la classificazione delle minacce e risultino disponibili e attive fin dalla prima installazione dell'agent*."

B.8) Al paragrafo 2.1.5.2 «Requisiti della Server Protection Platform (SPP)», nella Tabella 18 – Requisiti funzionali minimi per tutte le fasce di SPP, la previsione:

"*Funzionalità Antimalware signature based e tramite sistemi di analisi comportamentale*."

deve intendersi integrata come segue:

"Funzionalità Antimalware signature based e tramite sistemi di analisi comportamentale. *Il requisito può essere soddisfatto anche mediante le funzionalità oggetto dei criteri migliorativi SPP 2.2 e 2.7, ove offerte, purché le stesse, singolarmente oppure in combinazione, consentano l'identificazione, la rilevazione e il blocco delle minacce note, unitamente all'analisi comportamentale.*"

B.9) Al paragrafo 2.1.3.7 «Requisiti dell'Anti-Advanced Persistent Threat (Anti-APT)», nella Tabella 12 – Requisiti funzionali minimi per tutte le fasce di Anti-APT, la previsione:

«*Permettere di operare in modalità interattiva*.»

deve intendersi integrata come segue:

«Permettere di operare in modalità interattiva *e/o automatizzata*.»

B.10) Al paragrafo 2.1.3.7 «Requisiti dell'Anti-Advanced Persistent Threat (Anti-APT)», nella Tabella 12 – Requisiti funzionali minimi per tutte le fasce di Anti-APT, la previsione:

"*Possibilità di confrontare le firme dei malware in analisi con quelle presenti nella propria base dati al fine di identificare casistiche già note*."

deve intendersi integrata come segue:

"Possibilità di confrontare le firme dei malware in analisi con quelle presenti nella propria base dati al fine di identificare casistiche già note. *Il requisito può essere soddisfatto anche mediante le funzionalità oggetto dei criteri migliorativi Anti-APT 7.5 e 7.6, ove offerte, purché le stesse, singolarmente oppure in combinazione, consentano di identificare casistiche già note*."

B.11) Modifica ai requisiti minimi comuni dei prodotti

Al paragrafo 2.1.2 "Requisiti minimi comuni", punto 4, del Capitolato Tecnico Speciale Lotti 2, 3 e 4, la previsione:

"*prevedere la possibilità di disabilitare, da parte dell'Amministratore di sistema, qualsiasi servizio o funzionalità, documentato dal Produttore, in grado di comunicare verso reti esterne e/o interne anche per funzioni gestionali e/o di aggiornamento/manutenzione;*"

deve intendersi integrata dalla seguente:

" ad eccezione delle comunicazioni strettamente necessarie all'erogazione e al funzionamento del prodotto secondo il formato tecnologico offerto. Le comunicazioni non disabilitabili devono essere debitamente documentate dal Produttore, con indicazione della relativa finalità;"

B.12) Modifiche agli indicatori IQ09, IQ10 e IQ11

B.12.1) Indicatore IQ09 - Tempestività di risposta al disservizio

Al paragrafo 3.9 "IQ09 - Tempestività di risposta al disservizio" del Capitolato Tecnico Speciale Lotti 2, 3 e 4, nella tabella relativa all'indicatore, la previsione:

"*Unità di misura: Percentuale*"

deve intendersi sostituita dalla seguente:

"*Unità di misura: Ore*".

Restano invariate le ulteriori previsioni relative all'indicatore IQ09.

B.12.2) Indicatore IQ10 - Tempestività del tempo di intervento

Al paragrafo 3.10 "IQ10 - Tempestività del tempo di intervento" del Capitolato Tecnico Speciale Lotti 2, 3 e 4, nella tabella relativa all'indicatore, la previsione:

"Unità di misura: Percentuale"

deve intendersi sostituita dalla seguente:

"Unità di misura: Ore".

Restano invariate le ulteriori previsioni relative all'indicatore IQ10.

B.12.3) Indicatore IQ11 - Tempestività del tempo di ripristino del servizio

Al paragrafo 3.11 "IQ11 - Tempestività del tempo di ripristino del servizio" del Capitolato Tecnico Speciale Lotti 2, 3 e 4 sono apportate le seguenti modifiche.

- La previsione:

  "Unità di misura: Percentuale"

  deve intendersi sostituita dalla seguente:

  "Unità di misura: Ore".

- La formula:

  "TRIPR_SER = (TRS_XX - VTRS_XX) / VTRS_XX"

  deve intendersi sostituita dalla seguente:

  "TRIPR_SER = TRS_XX - VTRS_XX".

  Gli eventuali valori negativi di TRIPR_SER sono assunti pari a zero.

- La previsione relativa alle azioni contrattuali:

  "Per ogni rilievo eccedente il valore di soglia si applicherà la penale "Tempo di ripristino del servizio", pari allo 0,6‰ (zerovirgolasei per mille) dell'importo del Contratto Esecutivo."

  deve intendersi sostituita dalla seguente:

  "*Per ogni ora di ritardo nel ripristino del servizio rispetto al tempo massimo applicabile, determinata secondo le regole di arrotondamento previste dal presente indicatore, si applicherà la penale "Tempo di ripristino del servizio", pari allo 0,6‰ (zerovirgolasei per mille) dell'importo del Contratto Esecutivo*."

Restano ferme le ulteriori previsioni relative all'indicatore IQ11.

B.13) Modifica all'indicatore IQ01 - Rispetto di una scadenza contrattuale

Al paragrafo 3.1 "IQ01 - Rispetto di una scadenza contrattuale" del Capitolato Tecnico Speciale Lotti 2, 3 e 4, nella sezione "Dati da rilevare", dalla previsione **deve intendersi modificato come segue:**

"*L'indicatore viene calcolato come sommatoria degli eventi rilevati nel periodo di misurazione ~~(mensile)~~*."

B.14) Modifica all'indicatore IQ08 - Percentuale di chiamate in ingresso perse per il servizio di Service Desk

Al paragrafo 3.8 "IQ08 - Percentuale di chiamate in ingresso perse per il servizio di Service Desk" del Capitolato Tecnico Speciale Lotti 2, 3 e 4, nella sezione "Frequenza di misurazione", la previsione:

"*Trimestrale*"

deve intendersi sostituita dalla seguente:

"*Mensile*".

B.15) Modifica all'indicatore IQ12 - Tempo di disponibilità dei prodotti Cloud/SaaS

Al paragrafo 3.12 "IQ12 - Tempo di disponibilità dei prodotti Cloud/SaaS" del Capitolato Tecnico Speciale Lotti 2, 3 e 4, nella sezione "Eccezioni", la previsione:

"*Nessuna*"

deve intendersi sostituita dalla seguente:

"La misura del valore di soglia è effettuata al netto dei fermi programmati."

B.16) Al paragrafo 2.1.5.3 «Requisiti della Security Information and Event Management (SIEM)», nella Tabella 19 – Requisiti funzionali minimi per tutte le fasce di SIEM, si intende eliminato il seguente requisito:

"Possibilità di mappare gli alert di sicurezza con il framework MITRE ATT&CK o tassonomia cyber dell'ACN."

Al paragrafo 2.1.5.5 «Requisiti della eXtended Detection and Response (XDR)», nella Tabella 21 – Requisiti funzionali minimi per tutte le fasce di XDR, si intende eliminato il seguente requisito:

"Capacità di mapping delle tecniche e tattiche di attacco, mettendole in relazione al MITRE ATT&CK e/o alla tassonomia personalizzabile dalla PA (ACN)."

I predetti requisiti sono indicati, con formulazione invariata, tra i corrispondenti requisiti migliorativi, secondo quanto previsto al punto C.6, lettere b) e c), della presente Errata Corrige.

C. <u>Modifiche al Capitolato d'Oneri:</u>

C.1) Al par. 15 "Offerta tecnica", sono apportate le seguenti modifiche:

- nella tabella viene inserito il seguente riferimento:

"***Ove formulata offerta per la premialità per la tutela della sicurezza nazionale****: Allegato n. 18 – Dichiarazione uso di tecnologie di cybersicurezza*"

- **deve intendersi modificato come segue**:

3. ove sia stata formulata offerta per il criterio relativo alla "Premialità per la tutela della sicurezza nazionale", per ciascun Lotto per il quale si presenta offerta deve essere prodotta la dichiarazione di cui all'Allegato 18 – "Dichiarazione uso di tecnologie di cybersicurezza", firmata digitalmente con le modalità previste per l'Offerta Tecnica. La dichiarazione dovrà avere contenuto conforme all'Allegato 18."

Classificazione documento: Ambito pubblico

C.2) Il par. 19 “Svolgimento operazioni di gara”

“*i)* *verifica tecnica delle offerte dei Lotti 2,3 e 4*”

deve intendersi così modificato:

“***i)*** *verifica tecnica delle offerte dei Lotti 2,3 e 4 e verifica documentale per tutti i Lotti*”

C.3) Al par 17.1.1 Lotto 1, sono apportate le seguenti modifiche:

- il subcriterio 7.1

SLA approvazione documenti - ID 7.1

deve intendersi modificato come segue

SLA sostituzione del personale - ID 7.1

C.4) Al par 17.1.2 Lotto 2, il subcriterio 2.2 **deve intendersi integrato come segue:**

“Presenza della funzionalità di CDN *oppure web Caching configurabile direttamente sulla soluzione offerta”*

C.5) Modifiche ai criteri relativi all’acquisizione e all’utilizzo degli Indicatori di Compromissione.

- Al paragrafo 17.1.3, con riferimento al Lotto 3, criterio di valutazione NAC 1.3, la previsione:

  “Possibilità di importare liste dinamiche di Indicatori di Compromissione, quali indirizzi IP, domini, URL e ulteriori indicatori pertinenti, provenienti da fonti proprietarie o da terze parti qualificate, tra cui almeno MISP ACN, tramite protocolli standard STIX/TAXII, nonché, ove disponibili, ulteriori API documentate.”

  deve intendersi sostituita dalla seguente:

  “Capacità della soluzione NAC di acquisire e utilizzare automaticamente informazioni relative a minacce, compromissioni o vulnerabilità associate agli endpoint, provenienti da fonti proprietarie o da componenti dell’ecosistema di sicurezza dell’Amministrazione, mediante protocolli standard e/o API documentate, al fine di applicare dinamicamente policy di accesso e azioni di contenimento.”

- Ai paragrafi 17.1.2 e 17.1.4, con riferimento ai criteri di valutazione riportati nella seguente tabella:

Lotto	Tipologia di prodotto	Criterio
Lotto 2	NGFW	NGFW - ID 1.1
Lotto 2	WAAP	WAAP - ID 2.5
Lotto 2	SWG	SWG - ID 3.6
Lotto 2	SEG	SEG - ID 6.1
Lotto 2	Anti-APT	Anti-APT - ID 7.5
Lotto 4	EPP/EDR	EPP/EDR - ID 1.11
Lotto 4	SPP	SPP - ID 2.2
Lotto 4	SIEM	SIEM - ID 3.4
Lotto 4	SOAR	SOAR - ID 4.2
Lotto 4	XDR	XDR - ID 5.10

  la previsione:

"*Possibilità di importare liste dinamiche di Indicatori di Compromissione, quali indirizzi IP, domini, URL e ulteriori indicatori pertinenti, provenienti da fonti proprietarie o da terze parti qualificate, tra cui almeno MISP ACN, tramite protocolli standard STIX/TAXII, nonché, ove disponibili, ulteriori API documentate*."

deve intendersi sostituita dalla seguente:

"Possibilità di importare liste dinamiche di Indicatori di Compromissione, quali indirizzi IP, domini, URL e ulteriori indicatori pertinenti, provenienti da fonti proprietarie o da terze parti qualificate, tra cui almeno MISP ACN, mediante protocolli standard, quali STIX/TAXII, oppure tramite API, connettori o ulteriori modalità di integrazione documentate e interoperabili."

- Al paragrafo 17.1.3, con riferimento al Lotto 3, criterio di valutazione IAM - ID 2.6, la previsione:

"*La soluzione deve garantire la capacità di utilizzare, nei controlli IAM, indicatori di compromissione (IOC) provenienti da fonti qualificate, incluse piattaforme basate su MISP e tassonomie riconosciute (es. TC ACN), per il tramite di componenti di sicurezza integrabili (es. SIEM/TIP/NGFW) che supportano gli standard STIX per la rappresentazione dei dati di CTI e TAXII 2.x per la distribuzione automatizzata*."

deve intendersi sostituita dalla seguente:

"*La soluzione deve garantire la capacità di utilizzare, nei controlli IAM, Indicatori di Compromissione (IoC) provenienti da fonti qualificate, incluse piattaforme basate su MISP e tassonomie riconosciute, quali, a titolo esemplificativo, TC ACN, per il tramite di componenti di sicurezza integrabili, quali SIEM, TIP e NGFW, che supportano protocolli standard, quali STIX per la rappresentazione dei dati di CTI e TAXII 2.x per la distribuzione automatizzata, oppure tramite API, connettori o ulteriori modalità di integrazione documentate e interoperabili*."

- Al paragrafo 17.1.3, con riferimento al Lotto 3, criterio di valutazione PAM - ID 3.3, la previsione:

"*La soluzione deve garantire la capacità di utilizzare, nei controlli PAM, indicatori di compromissione (IOC) provenienti da fonti qualificate, incluse piattaforme basate su MISP e tassonomie riconosciute (es. TC ACN), per il tramite di componenti di sicurezza integrabili (es. SIEM/TIP/NGFW) che supportano gli standard STIX per la rappresentazione dei dati di CTI e TAXII 2.x per la distribuzione automatizzata*."

deve intendersi sostituita dalla seguente:

"*La soluzione deve garantire la capacità di utilizzare, nei controlli PAM, Indicatori di Compromissione (IoC) provenienti da fonti qualificate, incluse piattaforme basate su MISP e tassonomie riconosciute, quali, a titolo esemplificativo, TC ACN, per il tramite di componenti di sicurezza integrabili, quali SIEM, TIP e NGFW, che supportano protocolli standard, quali STIX per la rappresentazione dei dati di CTI e TAXII 2.x per la distribuzione automatizzata, oppure tramite API, connettori o ulteriori modalità di integrazione documentate e interoperabili*."

C.6) Modifica dei criteri relativi al mapping delle tecniche e tattiche di attacco

Al paragrafo 17.1.4 «Lotto 4» del Capitolato d'Oneri, nella «Tabella dei criteri discrezionali (D) e tabellari (T) di valutazione dell'offerta tecnica – Lotto 4», sono apportate le seguenti modifiche.

a) Sostituzione dei requisiti migliorativi relativi a EPP/EDR, SPP e SOAR

Con riferimento ai seguenti criteri tabellari:

- EPP/EDR – ID 1.7;
- SPP – ID 2.3;
- SOAR – ID 4.8,

la previsione:

"Presenza di una funzionalità di mapping delle tecniche e tattiche di attacco, mettendole in relazione con la tassonomia ACN."

deve intendersi sostituita dalla seguente:

"Presenza di una funzionalità di mapping delle tecniche e tattiche di attacco, mettendole in relazione con il framework MITRE ATT&CK."

b) Con riferimento al criterio tabellare SIEM – ID 3.7, la previsione:

"Presenza di una funzionalità di mapping delle tecniche e tattiche di attacco, mettendole in relazione con la tassonomia ACN."

deve intendersi sostituita dalla seguente previsione, già contenuta tra i requisiti minimi del prodotto SIEM e trasferita tra i requisiti migliorativi:

"Possibilità di mappare gli alert di sicurezza con il framework MITRE ATT&CK o tassonomia cyber dell'ACN."

c) Con riferimento al criterio tabellare XDR – ID 5.9, la previsione:

"Presenza di una funzionalità di mapping delle tecniche e tattiche di attacco, mettendole in relazione con la tassonomia ACN."

deve intendersi sostituita dalla seguente previsione, già contenuta tra i requisiti minimi del prodotto XDR e trasferita tra i requisiti migliorativi:

"Capacità di mapping delle tecniche e tattiche di attacco, mettendole in relazione al MITRE ATT&CK e/o alla tassonomia personalizzabile dalla PA (ACN)."

Restano invariati i punteggi attribuiti ai predetti criteri, i punteggi massimi dei relativi criteri di valutazione e la numerazione dei successivi subcriteri.

C.7) Modifiche ai Paragrafi 17.1.2, 17.1.3 e 17.1.4

C.7.1) Nei paragrafi 17.1.2, 17.1.3 e 17.1.4, con riferimento ai criteri discrezionali indicati di seguito:

Lotto 2

- 1.9 – Machine Learning e Artificial Intelligence – NGFW;
- 2.1 – Machine Learning e Artificial Intelligence – WAAP;
- 3.10 – Machine Learning e Artificial Intelligence – SWG;
- 5.5 – Supporto alla Reportistica per Compliance Normativa – CASB;
- 5.6 – Machine Learning e Artificial Intelligence – CASB;
- 6.6 – Machine Learning e Artificial Intelligence – SEG;
- 7.6 – Machine Learning e Artificial Intelligence – Anti-APT.

Lotto 3

- 1.6 – Machine Learning e Artificial Intelligence – NAC;
- 1.8 – Controllo della postura di sicurezza dei dispositivi – NAC;
- 3.6 – Supporto nella gestione della compliance normativa – PAM;
- 3.7 – Efficacia nella gestione degli accessi privilegiati – PAM;
- 4.3 – Valutazione del rischio della perdita di dati – DLP;
- 4.5 – Gestione policy e supporto alla compliance aziendale – DLP;
- 4.6 – Machine Learning e Artificial Intelligence – DLP.

Lotto 4

- 1.12 – Machine Learning e Artificial Intelligence – EPP/EDR;
- 2.7 – Machine Learning e Artificial Intelligence – SPP;

- 3.6 – Produzione di reportistica per la compliance aziendale – SIEM;
- 3.8 – Machine Learning e Artificial Intelligence – SIEM;
- 4.11 – Machine Learning e Artificial Intelligence – SOAR;
- 5.11 – Supporto nella gestione degli incidenti – XDR;
- 5.12 – Machine Learning e Artificial Intelligence – XDR.

La relativa articolazione nella colonna «Descrizione sintetica del subcriterio», recante le distinte indicazioni:

"[Prodotto] - ID [x.x] - Brand 1"

"[Prodotto] - ID [x.x] - Brand 2"

"[Prodotto] - ID [x.x] - Brand n"

con i corrispondenti punteggi frazionati riportati nella colonna «Valore singolo requisito»,

deve intendersi sostituita dalla seguente:

"[Prodotto] - ID [x.x]~~ – Brand 1~~".

Nella colonna «Valore singolo requisito» deve intendersi riportato il medesimo valore complessivo indicato, per il relativo subcriterio, nella colonna «Punti D max».

È eliminata, pertanto, l'attribuzione di autonomi sottopunteggi riferiti a «Brand 1», «Brand 2», ecc., restando invariato il punteggio discrezionale massimo complessivamente previsto per ciascun subcriterio.

C.7.2) Integrazione e coordinamento delle descrizioni dei subcriteri

Nella descrizione dei subcriteri di cui al precedente punto C.7.1), la richiesta di descrizione delle caratteristiche tecniche delle soluzioni offerte deve intendersi riferita a ciascun Brand offerto:

"*Si chiede di descrivere* […]"

oppure

«*Descrivere* […]»

deve intendersi integrata come segue:

"*Si chiede di descrivere, per ogni Brand offerto*, […]"

oppure

«*Descrivere, per ogni Brand offerto*, […]».

a) Criteri relativi alle tecniche di Machine Learning e Artificial Intelligence

Con riferimento ai seguenti subcriteri:

- Lotto 2: 1.9 – NGFW; 2.1 – WAAP; 3.10 – SWG; 5.6 – CASB; 6.6 – SEG; 7.6 – Anti-APT;
- Lotto 3: 1.6 – NAC; 4.6 – DLP;
- Lotto 4: 1.12 – EPP/EDR; 2.6 – SPP; 3.8 – SIEM; 4.11 – SOAR; 5.12 – XDR;

la previsione:

"*Sarà valutata, nel complesso, l'efficacia del prodotto e la capacità dello stesso di assicurare […]*"

deve intendersi sostituita dalla seguente:

"*Sarà valutata, nel complesso, l'efficacia dei prodotti e la capacità degli stessi di assicurare […]*".

b) Subcriterio 1.8 – NAC, Lotto 3

La previsione:

"*Sarà valutato il prodotto nel suo complesso in termini di […]*"

deve intendersi modificata come segue:

"*Saranno valutati i prodotti nel loro complesso in termini di […]*".

c) **Subcriterio 3.6 – PAM, Lotto 3**

La previsione:

"Il prodotto sarà valutato nel suo complesso in termini di […]"

deve intendersi modificata come segue:

"*I prodotti saranno valutati nel loro complesso in termini di […]*".

d) **Subcriterio 3.7 – PAM, Lotto 3**

Con riferimento al subcriterio 3.7 – «Efficacia nella gestione degli accessi privilegiati – PAM», la previsione:

"*La soluzione sarà valutata nel suo complesso in termini di […]*"

deve intendersi modificata come segue:

"*Le soluzioni saranno valutate nel loro complesso in termini di […]*".

e) **Subcriterio 4.3 – DLP, Lotto 3**

La previsione:

"*Le funzionalità saranno valutate […]*"

deve intendersi modificata come segue:

"*Saranno valutati i prodotti […]*".

f) **Subcriterio 4.5 – DLP, Lotto 3**

La previsione:

"*Sarà valutata […]*"

deve intendersi modificata come segue:

"Saranno valutati i prodotti nel loro complesso in termini di […]".

g) **Subcriterio 5.5 – CASB, Lotto 2, e subcriterio 3.6 – SIEM, Lotto 4**

La previsione:

"*Saranno valutate le funzionalità e la reportistica nel loro complesso […]*"

deve intendersi modificata come segue:

"*Saranno valutate nel loro complesso le funzionalità e la reportistica dei prodotti […]*".

h) **Subcriterio 5.11 – XDR, Lotto 4**

La previsione riferita al singolo sistema:

"*Sarà valutato il sistema XDR nel suo complesso, in termini di […]*"

deve intendersi modificata come segue

"*Saranno valutati i sistemi XDR nel loro complesso, in termini di […]*".

Nel medesimo subcriterio, i successivi riferimenti al singolare devono essere coordinati come segue:

- "efficacia del sistema" → "*efficacia dei sistemi*";

C.7.3) Integrazione del paragrafo 17.2

Al paragrafo 17.2 «Metodo di attribuzione del coefficiente per il calcolo del punteggio dell'offerta tecnica», nella sezione dedicata ai criteri discrezionali, dopo la disciplina relativa al confronto a coppie, è inserito il seguente testo:

"Con riferimento ai criteri discrezionali dei Lotti 2, 3 e 4 articolati in subcriteri riferiti ai Brand offerti, nell'espressione delle preferenze nell'ambito del confronto a coppie, la Commissione formulerà un giudizio comparativo complessivo, tenendo conto delle caratteristiche tecniche e qualitative delle soluzioni riferite ai singoli Brand e del livello complessivo con cui l'offerta risponde agli elementi di valutazione previsti dal criterio.

Ad esempio: se A e B offrono entrambi X, Y e Z e differiscono soltanto sugli altri brand, per i brand X, Y e Z, in quanto coincidenti, il percorso valutativo sarà il medesimo e il confronto si concentrerà sugli elementi effettivamente differenzianti tra le due offerte.".

C.8) Modifica al criterio SIEM – ID 3.2

Al paragrafo 17.1.4 del Capitolato d'Oneri, nella "Tabella dei criteri discrezionali (D) e tabellari (T) di valutazione dell'offerta tecnica – Lotto 4", con riferimento al criterio SIEM – ID 3.2, la previsione:

"*Presenza di una funzionalità di monitoraggio delle configurazioni. Il sistema deve poter collezionare le configurazioni degli apparati di rete, identificarne i cambiamenti, e fornire una funzionalità di comparazione delle varie revisioni*."

deve intendersi sostituita dalla seguente:

"Presenza di una funzionalità di monitoraggio delle configurazioni al fine di identificarne i cambiamenti."

D. <u>Modifica allo Schema di offerta economica</u>

D.1) Allegato 17C – Tabella di Offerta economica Lotto 4

Nel foglio "Prezzi unitari offerti", nella sezione relativa al prodotto XDR:

- per il formato Appliance Virtuale, la dicitura

  Prezzo offerto - AV [Euro/anno]

  deve intendersi sostituita dalla seguente:

  Prezzo offerto - AV [Euro **per endpoint**/anno];
- per il formato Cloud/SaaS, la dicitura

  Prezzo offerto - Cloud/SaaS [Euro server/anno]

  deve intendersi sostituita dalla seguente:

  Prezzo offerto - Cloud/SaaS [Euro per endpoint/anno]

D.2) Allegato 17C – Tabella di Offerta Economica Lotto 4

Nel foglio "Prezzi unitari offerti", nella sezione relativa al prodotto SOAR in formato Cloud/SaaS, la dicitura:

Cloud/SaaS [Euro server/anno]

deve intendersi sostituita dalla seguente:

Cloud/SaaS [Euro ad anno]

Classificazione documento: Ambito pubblico

E. Modifica all'Allegato 16 – Modello di declaratoria per le verifiche tecniche

E.1) Nella sezione «Verifiche tecniche specifiche – Lotto 2 – WAAP», Tabella 7 – Requisiti migliorativi WAAP, la previsione:

"Presenza della funzionalità di CDN."

deve intendersi sostituita dalla seguente:

"Presenza della funzionalità di CDN oppure Web Caching configurabile direttamente sulla soluzione offerta."

E.2) Nella sezione «Verifiche tecniche specifiche – Lotto 2 – WAAP», Tabella 6 – Requisiti minimi WAAP,

- si intendono eliminati i seguenti requisiti:

"Dashboard di monitoraggio in tempo reale con funzionalità drill-down almeno per: Attacchi, Sessioni, dati Geografici di accesso."

"Funzionalità di Data Loss Prevention."

"Ispezione del traffico FTP e delle versioni sicure da esso derivanti."

- con riferimento al requisito:

"Possibilità di interrogare la base dati della soluzione tramite API."

si intende eliminata una delle due occorrenze duplicate, restando fermo il requisito riportato nella medesima tabella**.**

E.3) Modifiche relative all'acquisizione e all'utilizzo degli Indicatori di Compromissione

- Nella sezione «Verifiche tecniche specifiche – Lotto 3 – NAC», Tabella 19 – Requisiti migliorativi NAC, la previsione:

  "*Possibilità di importare liste dinamiche di Indicatori di Compromissione, quali indirizzi IP, domini, URL e ulteriori indicatori pertinenti, provenienti da fonti proprietarie o da terze parti qualificate, tra cui almeno MISP ACN, tramite protocolli standard STIX/TAXII, nonché, ove disponibili, ulteriori API documentate*."

  deve intendersi sostituita dalla seguente:

  "Capacità della soluzione NAC di acquisire e utilizzare automaticamente informazioni relative a minacce, compromissioni o vulnerabilità associate agli endpoint, provenienti da fonti proprietarie o da componenti dell'ecosistema di sicurezza dell'Amministrazione, mediante protocolli standard e/o API documentate, al fine di applicare dinamicamente policy di accesso e azioni di contenimento."

- Con riferimento ai capitoli, alle sezioni e alle tabelle riportati di seguito:

Capitolo	Sezione	Tabella	Criterio corrispondente
Verifiche tecniche specifiche – Lotto 2	NGFW	Tabella 5 – Requisiti migliorativi NGFW	NGFW - ID 1.1
Verifiche tecniche specifiche – Lotto 2	WAAP	Tabella 7 – Requisiti migliorativi WAAP	WAAP - ID 2.5
Verifiche tecniche specifiche – Lotto 2	SWG	Tabella 9 – Requisiti migliorativi SWG	SWG - ID 3.6
Verifiche tecniche specifiche – Lotto 2	SEG	Tabella 15 – Requisiti migliorativi SEG	SEG - ID 6.1

Verifiche tecniche specifiche – Lotto 2	Anti-APT	Tabella 17 – Requisiti migliorativi Anti-APT	Anti-APT - ID 7.5
Verifiche tecniche specifiche – Lotto 4	EPP/EDR	Tabella 27 – Requisiti migliorativi EPP/EDR	EPP/EDR - ID 1.11
Verifiche tecniche specifiche – Lotto 4	SPP	Tabella 29 – Requisiti migliorativi SPP	SPP - ID 2.2
Verifiche tecniche specifiche – Lotto 4	SIEM	Tabella 31 – Requisiti migliorativi SIEM	SIEM - ID 3.4
Verifiche tecniche specifiche – Lotto 4	SOAR	Tabella 33 – Requisiti migliorativi SOAR	SOAR - ID 4.2
Verifiche tecniche specifiche – Lotto 4	XDR	Tabella 35 – Requisiti migliorativi XDR	XDR - ID 5.10

la previsione:

"*Possibilità di importare liste dinamiche di Indicatori di Compromissione, quali indirizzi IP, domini, URL e ulteriori indicatori pertinenti, provenienti da fonti proprietarie o da terze parti qualificate, tra cui almeno MISP ACN, tramite protocolli standard STIX/TAXII, nonché, ove disponibili, ulteriori API documentate*."

deve intendersi sostituita dalla seguente:

"*Possibilità di importare liste dinamiche di Indicatori di Compromissione, quali indirizzi IP, domini, URL e ulteriori indicatori pertinenti, provenienti da fonti proprietarie o da terze parti qualificate, tra cui almeno MISP ACN, mediante protocolli standard, quali STIX/TAXII, oppure tramite API, connettori o ulteriori modalità di integrazione documentate e interoperabili*."

- Nel capitolo Verifiche tecniche specifiche – Lotto 3, sezione IAM, Tabella 21 – Requisiti migliorativi IAM, con riferimento al requisito corrispondente al criterio di valutazione IAM - ID 2.6, la previsione:

  "*La soluzione deve garantire la capacità di utilizzare, nei controlli IAM, indicatori di compromissione (IOC) provenienti da fonti qualificate, incluse piattaforme basate su MISP e tassonomie riconosciute (es. TC ACN), per il tramite di componenti di sicurezza integrabili (es. SIEM/TIP/NGFW) che supportano gli standard STIX per la rappresentazione dei dati di CTI e TAXII 2.x per la distribuzione automatizzata*."

  deve intendersi sostituita dalla seguente:

  "*La soluzione deve garantire la capacità di utilizzare, nei controlli IAM, Indicatori di Compromissione (IoC) provenienti da fonti qualificate, incluse piattaforme basate su MISP e tassonomie riconosciute, quali, a titolo esemplificativo, TC ACN, per il tramite di componenti di sicurezza integrabili, quali SIEM, TIP e NGFW, che supportano protocolli standard, quali STIX per la rappresentazione dei dati di CTI e TAXII 2.x per la distribuzione automatizzata, oppure tramite API, connettori o ulteriori modalità di integrazione documentate e interoperabili."*

- Nel capitolo Verifiche tecniche specifiche – Lotto 3, sezione PAM, Tabella 23 – Requisiti migliorativi PAM, con riferimento al requisito corrispondente al criterio di valutazione PAM - ID 3.3, la previsione:

  "*La soluzione deve garantire la capacità di utilizzare, nei controlli PAM, indicatori di compromissione (IOC) provenienti da fonti qualificate, incluse piattaforme basate su MISP e tassonomie riconosciute (es. TC ACN), per il tramite di componenti di sicurezza integrabili (es. SIEM/TIP/NGFW) che supportano gli standard STIX per la rappresentazione dei dati di CTI e TAXII 2.x per la distribuzione automatizzata*."

  deve intendersi sostituita dalla seguente:

> *"La soluzione deve garantire la capacità di utilizzare, nei controlli PAM, Indicatori di Compromissione (IoC) provenienti da fonti qualificate, incluse piattaforme basate su MISP e tassonomie riconosciute, quali, a titolo esemplificativo, TC ACN, per il tramite di componenti di sicurezza integrabili, quali SIEM, TIP e NGFW, che supportano protocolli standard, quali STIX per la rappresentazione dei dati di CTI e TAXII 2.x per la distribuzione automatizzata, oppure tramite API, connettori o ulteriori modalità di integrazione documentate e interoperabili."*

E.4) Nella sezione Verifiche tecniche specifiche – Lotto 4 - XDR, Tabella 34 – Requisiti minimi XDR, la previsione:

"*La soluzione deve consentire la rilevazione e il blocco di minacce sulla base di signature note (signature based*)."

deve intendersi integrata come segue:

*"*La soluzione deve consentire la rilevazione e il blocco di minacce sulla base di signature note (signature based). *Il requisito può essere soddisfatto anche mediante le funzionalità oggetto dei criteri migliorativi XDR 5.7, 5.10 e 5.12, ove offerte, purché le stesse, singolarmente oppure in combinazione, consentano la rilevazione e il blocco delle minacce note."*

E.5) Nella sezione «Verifiche tecniche specifiche – Lotto 4 – EPP/EDR», Tabella 26 – Requisiti minimi EPP/EDR, la previsione:

"*Presenza di un set di signature già presenti sulla soluzione per permettere la protezione fin dal primo utilizzo*."

deve intendersi integrata come segue:

"Presenza di un set di signature già presenti sulla soluzione per permettere la protezione fin dal primo utilizzo. *Il requisito può essere soddisfatto anche mediante le funzionalità oggetto dei criteri migliorativi EPP/EDR 1.11 e 1.12, ove offerte, purché le stesse, singolarmente oppure in combinazione, consentano l'identificazione e la classificazione delle minacce e risultino disponibili e attive fin dalla prima installazione dell'agent.*"

E.6) Nella sezione «Verifiche tecniche specifiche – Lotto 4 – SPP», Tabella 28 – Requisiti minimi SPP, la previsione:

"*Funzionalità Antimalware signature based e tramite sistemi di analisi comportamentale*."

deve intendersi integrata come segue:

"Funzionalità Antimalware signature based e tramite sistemi di analisi comportamentale. *Il requisito può essere soddisfatto anche mediante le funzionalità oggetto dei criteri migliorativi SPP 2.2 e 2.7, ove offerte, purché le stesse, singolarmente oppure in combinazione, consentano l'identificazione, la rilevazione e il blocco delle minacce note, unitamente all'analisi comportamentale.*"

E.7) Nella sezione Verifiche tecniche specifiche – Lotto 2 – Anti-APT, Tabella 16 – Requisiti minimi Anti-APT, la previsione:

"*Permettere di operare in modalità interattiva*."

deve intendersi sostituita dalla seguente:

"Permettere di operare in modalità interattiva *e/o automatizzata*."

E.8) Modifiche ai requisiti relativi al mapping delle tecniche e tattiche di attacco

Nelle sezioni «Verifiche tecniche specifiche – Lotto 4» dell'Allegato 16 – Modello di declaratoria per le verifiche tecniche sono apportate le seguenti modifiche:

a) nelle tabelle dei requisiti migliorativi EPP/EDR, SPP e SOAR, la previsione:

"Presenza di una funzionalità di mapping delle tecniche e tattiche di attacco, mettendole in relazione con la tassonomia ACN."

deve intendersi sostituita dalla seguente:

"Presenza di una funzionalità di mapping delle tecniche e tattiche di attacco, mettendole in relazione con il framework MITRE ATT&CK."

b) nella Tabella 30 – Requisiti minimi SIEM, si intende eliminato il requisito:

"Possibilità di mappare gli alert di sicurezza con il framework MITRE ATT&CK o tassonomia cyber dell'ACN."

Il medesimo requisito, con formulazione invariata, è inserito nella Tabella 31 – Requisiti migliorativi SIEM.

c) nella Tabella 34 – Requisiti minimi XDR, si intende eliminato il requisito:

"Capacità di mapping delle tecniche e tattiche di attacco, mettendole in relazione al MITRE ATT&CK e/o alla tassonomia personalizzabile dalla PA (ACN)."

Il medesimo requisito, con formulazione invariata, è inserito nella Tabella 35 – Requisiti migliorativi XDR.

E.9) Nella sezione «Verifiche tecniche specifiche – Lotto 2 – Anti-APT», Tabella 16 – Requisiti minimi Anti-APT, la previsione:

"*Possibilità di confrontare le firme dei malware in analisi con quelle presenti nella propria base dati al fine di identificare casistiche già note*."

deve intendersi integrata come segue:

"Possibilità di confrontare le firme dei malware in analisi con quelle presenti nella propria base dati al fine di identificare casistiche già note. *Il requisito può essere soddisfatto anche mediante le funzionalità oggetto dei criteri migliorativi Anti-APT 7.5 e 7.6, ove offerte, purché le stesse, singolarmente oppure in combinazione, consentano di identificare casistiche già note."*

E.10) Nella sezione relativa al Lotto 4 – SIEM dell'Allegato 16 – Modello di declaratoria per le verifiche tecniche, con riferimento al requisito migliorativo SIEM corrispondente al criterio ID 3.2, la previsione:

"*Presenza di una funzionalità di monitoraggio delle configurazioni. Il sistema deve poter collezionare le configurazioni degli apparati di rete, identificarne i cambiamenti, e fornire una funzionalità di comparazione delle varie revisioni*."

deve intendersi sostituita dalla seguente:

"*Presenza di una funzionalità di monitoraggio delle configurazioni al fine di identificarne i cambiamenti*."

E.11) Nell'Allegato 16 - Modello di declaratoria per le verifiche tecniche, alla tabella 1 – Requisiti Comuni la previsione:

"*prevedere la possibilità di disabilitare, da parte dell'Amministratore di sistema, qualsiasi servizio o funzionalità, documentato dal Produttore, in grado di comunicare verso reti esterne e/o interne anche per funzioni gestionali e/o di aggiornamento/manutenzione*;"

deve intendersi integrata dalla seguente:

"ad eccezione delle comunicazioni strettamente necessarie all'erogazione e al funzionamento del prodotto secondo il formato tecnologico offerto. Le comunicazioni non disabilitabili devono essere debitamente documentate dal Produttore, con indicazione della relativa finalità;"

E.12) Nella sezione "Verifiche tecniche specifiche - Lotto 4 - SPP", Tabella 29 - Requisiti migliorativi SPP, la previsione:

"*Implementazione di una funzionalità di monitoraggio completo delle attività dei server, che consenta la registrazione e l'analisi di tutte le operazioni eseguite, inclusi, ma non limitati a, attività di networking, modifiche a file e registri, per una tracciabilità dettagliata e una valutazione accurata del comportamento dei server*"

deve intendersi sostituita dalla seguente:

"*Presenza di una funzionalità di analisi di tutte le attività che vengono eseguite sui server, tenendo traccia delle attività di networking, modifiche a file e registri, etc…"*

F. <u>Modifiche agli allegati agli Schemi di relazione tecnica</u>

Classificazione documento: Ambito pubblico

F.1) Allegato 3C.1 – Prodotti offerti Lotto 3.xlsx

Nel foglio «Prodotti offerti Lotto 3», al rigo 52, nelle celle D52, E52 e F52, la dicitura:

"*Appliance Virtuale*"

deve intendersi sostituita dalla seguente:

"*Appliance fisica*".

G. <u>Pubblicazione documenti</u>

Si rende noto che:

- il Capitolato Tecnico Speciale è stato sostituito dal documento "ID 2733 Capitolato Tecnico Speciale Lotti 2 3 4_New";
- il Capitolato Tecnico Generale è stato sostituito dal documento "ID 2733 - Capitolato Tecnico Generale_New";
- il Capitolato d'Oneri è stato sostituito dal documento "ID 2733 - Capitolato d'Oneri_New";
- l'Allegato 16 - Modello di declaratoria per le verifiche tecniche è stato sostituito dal documento "ID 2733 - Allegato 16 - Modello di declaratoria per le verifiche tecniche_New";
- l'Allegato 17C - Tabella di Offerta Economica Lotto 4 è stato sostituito dal documento "ID 2733 - Allegato 17C - Tabella di Offerta Economica Lotto 4_New";
- l'Allegato 3C.1 - Prodotti offerti Lotto 3 è stato sostituito dal documento "ID 2733 - Allegato 3C.1 - Prodotti offerti Lotto 3_New".

Consip S.p.A.

Avv. Marco Reggiani

(Amministratore Delegato e Direttore Generale)