ALLEGATO 16

MODELLO DI DECLARATORIA PER LE VERIFICHE TECNICHE

Gara europea 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 (ed. 1) – suddivisa in 4 Lotti - per le pubbliche amministrazioni ai sensi dell'art. 59, comma 4, lett. A), del d.lgs. 36/2023

ID 2733

Classificazione Consip: distribuzione ristretta

Sommario

PREMESSA **4**

MODELLO DI DECLARATORIA PER LE VERIFICHE TECNICHE **4**

CONTENUTO DEL MODELLO DI DECLARATORIA PER LE VERIFICHE TECNICHE **6**

VERIFICHE TECNICHE SPECIFICHE - LOTTO 2 **10**

NGFW 10
WAAP 12
SWG 14
ZTNA 17
CASB 20
SEG 22
Anti APT 25

VERIFICHE TECNICHE SPECIFICHE - LOTTO 3 **27**

NAC 27
IAM 29
PAM 31
DLP 33

VERIFICHE TECNICHE SPECIFICHE - LOTTO 4 **35**

EPP/EDR 35
SPP 38
SIEM 39
SOAR 42
XDR 45

Indice delle tabelle

Tabella 1 - Requisiti Comuni a tutti i prodotti (Lotti 2, 3, 4) 7
Tabella 2 - Requisiti DNSH Scheda 3 comuni a tutti i prodotti - Appliance Fisiche 8
Tabella 3 - Requisiti minimi DNSH Scheda 6 comuni a tutti i prodotti erogati in SaaS 9
Tabella 4 – Requisiti minimi NGFW 11
Tabella 5 - Requisiti migliorativi NGFW 12
Tabella 6 – Requisiti minimi WAAP 13
Tabella 7 - Requisiti migliorativi WAAP 14
Tabella 8 - Requisiti minimi SWG 16
Tabella 9 - Requisiti migliorativi SWG 17
Tabella 10 - Requisiti minimi ZTNA 18
Tabella 11 - Requisiti migliorativi ZTNA 19
Tabella 12 - Requisiti minimi CASB 21
Tabella 13 - Requisiti migliorativi CASB 21
Tabella 14 - Requisiti minimi SEG 23
Tabella 15 - Requisiti migliorativi SEG 24
Tabella 16 - Requisiti minimi ANTI-APT 26
Tabella 17 - Requisiti migliorativi ANTI-APT 27
Tabella 18 - Requisiti minimi NAC 28
Tabella 19 - Requisiti migliorativi NAC 29
Tabella 20 - Requisiti minimi IAM 30
Tabella 21 - Requisiti migliorativi IAM 30
Tabella 22 - Requisiti minimi PAM 32
Tabella 23 - Requisiti migliorativi PAM 32
Tabella 24 - Requisiti minimi DLP 33
Tabella 25 - Requisiti migliorativi DLP 34
Tabella 26 - Requisiti minimi EPP/EDR 36
Tabella 27 - Requisiti migliorativi EPP/EDR 37
Tabella 28 - Requisiti minimi SPP 38
Tabella 29 - Requisiti migliorativi SPP 39
Tabella 30 - Requisiti minimi SIEM 40
Tabella 31 - Requisiti migliorativi SIEM 41
Tabella 32 - Requisiti minimi SOAR 43
Tabella 33 - Requisiti migliorativi SOAR 44
Tabella 34 - Requisiti minimi XDR 46
Tabella 35 - Requisiti migliorativi XDR 47

PREMESSA

Il presente modello dovrà essere compilato, ai fini dell'espletamento delle verifiche tecniche, per ciascun Lotto, secondo il format di seguito indicato.

Si precisa che:

I. il concorrente, per ogni singolo brand, per ciascuna soluzione offerta e per ogni singolo requisito di ogni singola tabella, dovrà indicare in modo chiaro e inequivocabile il/i documento/i prodotto/i a comprova ai sensi del paragrafo 21 BIS.3 del Capitolato d'Oneri e, ove pertinente, del relativo numero di pagina da cui risulti il rispetto del relativo requisito minimo e/o migliorativo eventualmente offerto;

II. le tabelle dovranno essere compilate distintamente per ciascun brand offerto e per ciascun formato tecnologico previsto dalla documentazione di gara per lo specifico prodotto e concretamente oggetto dell'offerta (Appliance Fisica, Appliance Virtuale e Cloud/SaaS), con una compilazione distinta per ogni soluzione proposta;

III. qualora, nell'ambito del medesimo brand, siano offerte soluzioni afferenti a diversi formati tecnologici, dovrà essere compilata una distinta tabella per ciascuna soluzione offerta;

IV. la compilazione dovrà riguardare sia le soluzioni offerte ai fini del soddisfacimento del numero minimo richiesto dal Capitolato Tecnico Speciale, sia le eventuali soluzioni aggiuntive offerte ai fini dell'attribuzione dei punteggi migliorativi;

V. con riferimento alle tabelle contenenti requisiti applicabili esclusivamente a determinati formati tecnologici, ivi inclusi, ove pertinenti, i Requisiti Comuni e i Requisiti DNSH, la relativa tabella dovrà essere compilata e ripetuta per ciascun brand, formato tecnologico e soluzione cui i requisiti risultino applicabili; non dovranno essere compilate le tabelle relative a formati tecnologici non pertinenti rispetto alla soluzione offerta;

VI. l'intestazione di ciascuna tabella dovrà riportare chiaramente:

- Lotto;
- Brand;
- Formato tecnologico (AF, AV, Cloud/SaaS);

VII. il campo "Nota/e" delle tabelle potrà essere compilato laddove ritenuto utile e/o necessario;

VIII. tutti i documenti sopra indicati dovranno essere allegati in formato PDF;

IX. In ogni caso, la compilazione del Modello dovrà consentire l'univoca riconducibilità di ciascun requisito oggetto di verifica al relativo Lotto, brand, formato tecnologico e specifica soluzione offerta.

Per comodità di lettura, nelle sottostanti tabelle evidenziate in grigio sono riportati i campi che devono essere compilati.

MODELLO DI DECLARATORIA PER LE VERIFICHE TECNICHE

Il sottoscritto _____, nato a _____ il _____C.F._____, domiciliato per la carica presso la sede societaria ove appresso, nella sua qualità di _____ e legale rappresentante avente i

poteri necessari per impegnare la _____ nella presente procedura, con sede in _____, Via _____, iscritta al Registro delle Imprese di ___ al n. ___, codice fiscale n. _____ CCNL applicato _____ Settore _____, che partecipa alla presente iniziativa nella seguente forma _____

ai sensi e per gli effetti dell'art. 76 D.P.R. 445/2000 consapevole della responsabilità e delle conseguenze civili e penali previste in caso di dichiarazioni mendaci e/o formazione od uso di atti falsi e/o in caso di esibizione di atti contenenti dati non più corrispondenti a verità;

DICHIARA

- che tutti i documenti allegati alla presente dichiarazione sono conformi agli originali e che tutti i requisiti minimi e migliorativi sotto riportati, cui i documenti allegati alla presente dichiarazione si riferiscono, erano sussistenti alla data della sottoscrizione dell'offerta;
- di aver preso visione delle disposizioni del Regolamento (UE) 2024/2847 (Cyber Resilience Act) e, pur nel periodo transitorio antecedente alla sua piena applicazione, si impegna, per tutta la durata dell'esecuzione contrattuale, ad adottare e mantenere misure tecniche e organizzative coerenti con i requisiti essenziali di cybersicurezza previsti dal medesimo Regolamento, con particolare riferimento ai requisiti di cui all'Allegato I del CRA;
- di impegnarsi, infine, ad adeguare tempestivamente prodotti, servizi, processi e misure di sicurezza alle disposizioni del Regolamento (UE) 2024/2847 che diverranno applicabili nel corso dell'esecuzione contrattuale, senza ulteriori oneri per l'Amministrazione.

CONTENUTO DEL MODELLO DI DECLARATORIA PER LE VERIFICHE TECNICHE

TABELLA REQUISITI COMUNI A TUTTI I LOTTI (CFR. PAR. 2.1.2 CTS 2B)				
AMBITO	**REQUISITI COMUNI**	**DOCUMENTO/I COMPROVANTE/I IL REQUISITO**	**PAGINA/E**	**NOTE**
Prodotti	Disponibili sul mercato al momento della scadenza per la presentazione dell'offerta. Pertanto, tutti i prodotti proposti devono essere già commercializzati o commercializzabili al momento di presentazione dell'offerta e non saranno accettati prototipi			
	Per i prodotti dotati di hardware dedicato, essere nuovi di fabbrica e non ricondizionati, per cui il numero di matricola, corrispondente ai dispositivi forniti, non dovrà mai essere stato precedentemente oggetto di fatturazione verso un cliente			
	Non prevedere servizi e funzionalità, che non siano esplicitamente riportati nella documentazione tecnica e nella manualistica del Produttore, in grado di comunicare verso reti esterne e/o interne			
	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, 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			
	Per i prodotti dotati di hardware dedicato, provvisti di regolare marcatura "CE", a garanzia della conformità dei prodotti alla normativa dell'Unione applicabile alla specifica merceologia			
	Per i prodotti dotati di hardware dedicato: essere conformi alla normativa vigente, nazionale ed europea, che regolamenta la loro produzione, commercializzazione ed utilizzo e rispettare, ciascuna per le singole specifiche caratteristiche, le seguenti prescrizioni in materia di sicurezza: - Decreto Legislativo del 19 maggio 2016 n. 86 e s.m.i., "attuazione della direttiva 2014/35/UE concernente l'armonizzazione delle legislazioni degli Stati membri relative alla messa a disposizione sul mercato del materiale elettrico destinato ad essere adoperato entro taluni limiti di tensione"; - D. Lgs. 4 marzo 2014, n. 27 e s.m.i., "attuazione della direttiva 2011/65/UE sulla restrizione dell'uso di determinate sostanze pericolose nelle apparecchiature elettriche ed elettroniche" (RoHS); - D. Lgs. 18 maggio 2016, n. 80 e s.m.i., "modifiche al decreto legislativo 6 novembre 2007, n. 194, di attuazione della direttiva 2014/30/UE del Parlamento europeo e del Consiglio, del 26 febbraio 2014, concernente l'armonizzazione delle legislazioni degli Stati membri relative alla compatibilità elettromagnetica";			

TABELLA REQUISITI COMUNI A TUTTI I LOTTI (CFR. PAR. 2.1.2 CTS 2B)				
AMBITO	**REQUISITI COMUNI**	**DOCUMENTO/I COMPROVANTE/I IL REQUISITO**	**PAGINA/E**	**NOTE**
	- D. Lgs, n. 49/2014 così come modificato da ultimo D.Lgs. n. 11 del 3 settembre 2020 e s.m.i., "Attuazione degli articoli 2 e 3 della direttiva (UE) 2018/849 relativa a pile e accumulatori e ai rifiuti di pile e accumulatori e sui rifiuti di apparecchiature elettriche ed elettroniche. Inoltre: • l'offerente • oppure, se diverso dall'offerente, il produttore, così come definito all'art. 4, lett. g), del D.Lgs. 49/2014; • oppure, sempre se diverso dall'offerente, il distributore, così come definito all'art. 4, lett. h), del D.Lgs. 49/2014; dovrà essere in possesso dell'iscrizione al Registro nazionale dei soggetti obbligati al finanziamento dei sistemi di gestione dei RAEE, istituito e funzionante ai sensi del regolamento 25 settembre 2007, n. 185.			

Tabella 1 - Requisiti Comuni a tutti i prodotti (Lotti 2, 3, 4)

APPLIANCE FISICHE				
AMBITO	**REQUISITI MINIMI – DNSH – SCHEDA 3**	**DOCUMENTO/I COMPROVANTE/I IL REQUISITO**	**PAGINA/E**	**NOTE**
DNSH	(1) Iscrizione alla piattaforma RAEE in qualità di produttore e/o distributore e/o fornitore			
	(2) Etichetta ambientale di tipo I, secondo la UNI EN ISO 14024, ad esempio TCO Certified, EPEAT 2018, Blue Angel, TÜV Green Product Mark o etichetta equivalente			
	(3) Etichetta EPA ENERGY STAR			
	(3.1) Dichiarazione del produttore che attesti che il consumo tipico di energia elettrica (Etec), calcolato per ogni dispositivo offerto, non superi il TEC massimo necessario (Etec-max) in linea con quanto descritto nell'Allegato III dei criteri GPP UE			
	(4) Per i server e prodotti di archiviazioni dati, conformità alla seguente normativa: ecodesign (Regolamento (EU) 2019/424			
	(7) Rispetto della seguente normativa: REACH (Regolamento (CE) n.1907/2006); RoHS (Direttiva 2011/65/EU e ss.m.i.); Compatibilità elettromagnetica (Direttiva 2014/30/UE e ss.m.i.)			

	(8) Indicazione delle limitazioni delle caratteristiche di pericolo dei materiali che si prevede utilizzare (Art. 57, Regolamento CE 1907/2006, REACH) .			

Tabella 2 - Requisiti DNSH Scheda 3 comuni a tutti i prodotti - Appliance Fisiche

In riferimento alla precedente tabella, si precisa che:

- qualora in possesso dei requisiti di cui ai punti (1) e (2) non è necessario possedere anche i requisiti di cui ai punti successivi;
- in assenza di un'etichetta ambientale di tipo I, secondo la UNI EN ISO 14024 (punto 2), allora si ha l'obbligo possedere i requisiti di cui a tutti i punti successivi: (3), (4), (7) e (8), con la precisazione che in assenza dei requisiti al punto (3) si ha l'obbligo di rispondere al punto (3.1);
- i requisiti di cui ai punti (1) e (7) sono comunque già previsti in via obbligatoria al precedente paragrafo 2.1.2 del capitolato tecnico speciale lotti 2, 3, 4;
- la numerazione non prevede i nn. (5) e (6), in quanto trattasi di requisiti della Scheda n. 3 non pertinenti con la merceologia oggetto della presente iniziativa.

CLOUD SAAS – SERVIZI INFORMATICI DI HOSTING E CLOUD – REGIME 2				
AMBITO	**REQUISITI MINIMI – DNSH – SCHEDA 6**	**DOCUMENTO/I COMPROVANTE/I IL REQUISITO**	**PAGINA/E**	**NOTE**
DNSH	(1) Certificazione di sistema di gestione ambientale di tipo ISO 14001 o EMAS rilasciata sotto accreditamento.			
	(2) Comunicazione del calcolo della media ponderata del potenziale di riscaldamento globale, anche per l'inventario dei refrigeranti utilizzati nei siti o per fornire il servizio, e dimostrazione dell'aderenza al metodo descritto nell'allegato IV del regolamento (UE) n. 517/2014, oppure sistema di gestione dell'energia (norma ISO 50001) o sistema di gestione ambientale (sistema EMAS o norma ISO 14001) che riportino l'uso di refrigeranti.			
	(3) Svolgimento degli studi di fattibilità per l'implementazione e il rispetto di tutte le "pratiche attese" incluse nella versione più recente del codice di condotta europeo sull'efficienza energetica dei centri dati e hanno attuato tutte le pratiche attese a cui è stato assegnato il valore massimo di 5.			
	(4) Adesione dei data center che ospitano i servizi di hosting e cloud alle pratiche raccomandate contenute nel CEN-CENELEC documento CLC TR50600-99-1 "Data centre facilities and infrastructures- Part 99-1 : Recommended practices for energy management".			
	(5) Rispetto di tutti i Criteri dell'UE applicabili in materia di appalti pubblici verdi per i centri dati, le sale server e servizi cloud e fornite le relative prove di verifica.			

CLOUD SAAS – SERVIZI INFORMATICI DI HOSTING E CLOUD – REGIME 2				
AMBITO	**REQUISITI MINIMI – DNSH – SCHEDA 6**	**DOCUMENTO/I COMPROVANTE/I IL REQUISITO**	**PAGINA/E**	**NOTE**
	(6) Possesso per i data center che ospitano i servizi di hosting e cloud di un piano di gestione dei rifiuti.			
	(7) Conformità alla seguente normativa: ecodesign (Regolamento (EU) 2019/424) considerato che la conformità alle normative può essere dimostrata anche tramite il sistema di gestione ISO 30134:2016 certificato da organismi di certificazione accreditati.			
	(8) Conformità delle apparecchiature dei data center alla seguente normativa: REACH (Regolamento (CE) n.1907/2006); RoHS (Direttiva 2011/65/EU e ss.m.i.); compatibilità elettromagnetica (Direttiva 2014/30/UE). La conformità alla norma RoHS può essere dimostrata applicando la norma EN IEC 63000:2018.			

Tabella 3 - Requisiti minimi DNSH Scheda 6 comuni a tutti i prodotti erogati in SaaS

In riferimento alla precedente tabella, si precisa che:

- qualora in possesso del requisito di cui al punto (1), non è necessario possedere anche i requisiti di cui ai punti successivi;
- qualora non in possesso del requisito (1), dovranno essere posseduti i requisiti di cui ai punti:
  - (2);
  - almeno uno tra (3), (4) e (5);
  - (6);
  - (7);
  - (8);

  Solamente nel caso in cui sia posseduto il requisito di cui al punto (5), non sarà necessario comprovare anche il possesso di cui ai precedenti punti (7) e (8).

VERIFICHE TECNICHE SPECIFICHE - LOTTO 2
NGFW

LOTTO 2 - TABELLA REQUISITI MINIMI NGFW BRAND K-ESIMO (DOVE K=1,2,3,4,5)				
AMBITO	**REQUISITI MINIMI**	**DOCUMENTO/I COMPROVANTE/I IL REQUISITO**	**PAGINA/E**	**NOTE**
NGFW	Funzionalità di network firewall (statefull inspection, policy enforcement, packet filtering, DNAT e SNAT, VPN IPSEC client to site e site to site, VPN TLS).			
	Funzionalità di intrusion prevention system per il rilevamento, blocco e tracciamento delle minacce, attraverso l'adozione di meccanismi di ispezione dei malware di tipo signature based, anomaly detection (es. individuazione delle anomalie nei protocolli comunemente utilizzati nell'ambito delle reti IP), analisi euristica o comportamentale (adottata per riconoscere minacce per le quali non sono state già definite le firme), con possibilità di creare anche signature personalizzate per contrastare attacchi ancora non censiti.			
	WEB/URL Filtering statico e dinamico, con possibilità di controllare le statistiche sulla navigazione, di bloccare l'accesso a particolari siti e creare anche categorie personalizzate.			
	Funzionalità anti-malware sia su base firma che su base comportamentale.			
	Funzionalità di anti-botnet.			
	Deep packet inspection per scansionare l'intero payload dei pacchetti.			
	TLS/SSL inspection per l'ispezione del traffico cifrato.			
	SSH inspection.			
	Controllo delle applicazioni con blocco dell'esecuzione in funzione della configurazione impostata dall'Amministratore di Sistema.			
	QoS bandwidth management con la possibilità di impostare una larghezza di banda minima garantita e un limite massimo di larghezza di banda per il traffico insieme ad un valore di priorità.			
	Trasmissione di eventi e log al SIEM o ad altro strumento di raccolta log, ove disponibile, dell'Amministrazione.			
	Produzione di report personalizzabili di sintesi (executive summary) e di dettaglio (technical report), al fine di certificare la compliance a determinati standard o per consentire analisi sul livello di protezione delle applicazioni.			
	Supporto IPv6.			
	Supporto per configurazione in alta affidabilità.			

LOTTO 2 - TABELLA REQUISITI MINIMI NGFW BRAND K-ESIMO (DOVE K=1,2,3,4,5)				
AMBITO	**REQUISITI MINIMI**	**DOCUMENTO/I COMPROVANTE/I IL REQUISITO**	**PAGINA/E**	**NOTE**
	Funzionalità di accesso selettivo alle applicazioni con modello Zero Trust basata su identificazione dei dispositivi client e autenticazione degli utenti.			
	Analisi del traffico su base geolocalizzazione degli IP e possibilità di filtraggio/blocco.			

Tabella 4 – Requisiti minimi NGFW

LOTTO 2 - TABELLA REQUISITI MIGLIORATIVI NGFW BRAND K-ESIMO (DOVE K=1,2,3,4,5)				
AMBITO	**REQUISITI MIGLIORATIVI**	**DOCUMENTO/I COMPROVANTE/I IL REQUISITO**	**PAGINA/E**	**NOTE**
NGFW	~~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~~. 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.			
	Presenza della funzionalità di DNS Filter (filtraggio su base categorizzazione dei domini e reputazione) per proteggere i client dall'accesso a domini compromessi.			
	Disponibilità di usufruire di un database dinamico di mappatura IP/porta/protocollo dei servizi cloud, aggiornato direttamente dal vendor, che può essere utilizzato sia in ambito policy che in ambito routing.			
	Ai fini dell'interconnessione con Public Cloud e la gestione di ambienti ibridi, possibilità di supportare almeno due tra le seguenti tecnologie: AWS, Azure, Oracle, Google.			
	Ai fini dell'integrazione con ambienti SDN, possibilità di supportare almeno due tra le seguenti tecnologie: Open stack, Cisco ACI, vmware NSX/ESXi, Kubernetes.			
	Presenza della funzionalità di gestione della sicurezza per i dispositivi IOT, garantendo almeno la scansione dei dispositivi, il controllo delle vulnerabilità e malware e l'aggiornamento delle policy di sicurezza.			

LOTTO 2 - TABELLA REQUISITI MIGLIORATIVI NGFW BRAND K-ESIMO (DOVE K=1,2,3,4,5)				
AMBITO	**REQUISITI MIGLIORATIVI**	**DOCUMENTO/I COMPROVANTE/I IL REQUISITO**	**PAGINA/E**	**NOTE**
	Capacità di intercettare, analizzare e indirizzare le richieste DNS mediante funzionalità integrate nella soluzione NGFW oppure mediante componenti con essa integrate o interoperabili, garantendo la gestione centralizzata e l'applicazione delle relative policy di sicurezza.			
	Possibilità di integrazione con soluzioni di terze parti, anche non previste nativamente, attraverso utilizzo di protocolli standard e/o API documentate.			
	Funzionalità di anti-spam.			

Tabella 5 - Requisiti migliorativi NGFW

WAAP

LOTTO 2 - TABELLA REQUISITI MINIMI WAAP BRAND K-ESIMO (DOVE K=1,2, 3, 4)				
AMBITO	**REQUISITI MINIMI**	**DOCUMENTO/I COMPROVANTE/I IL REQUISITO**	**PAGINA/E**	**NOTE**
WAAP	Capacità di protezione dagli attacchi applicativi almeno OWASP TOP 10 (ultima versione disponibile alla data di presentazione offerta).			
	~~Ispezione del traffico FTP e delle versioni sicure da esso derivanti.~~			
	Ispezione Traffico HTTP/HTTPS.			
	Protezione delle API web che utilizzano formati strutturati quali JSON e XML, mediante l'analisi dei dati veicolati da questi formati.			
	Controllo dell'IP Reputation.			
	Mitigazione degli attacchi tramite reti di bot.			

LOTTO 2 - TABELLA REQUISITI MINIMI WAAP BRAND K-ESIMO (DOVE K=1,2, 3, 4)				
AMBITO	**REQUISITI MINIMI**	**DOCUMENTO/I COMPROVANTE/I IL REQUISITO**	**PAGINA/E**	**NOTE**
	Possibilità di definire BlackList e Whitelist di accesso, anche basandosi sulla georeferenziazione degli IP address.			
	Capacità di rilevamento e mitigazione di attacchi DDOS di tipo applicativo.			
	SSL Offloading.			
	Supporto del protocollo IPV6.			
	Supporto per configurazione in alta affidabilità.			
	~~Dashboard di monitoraggio in tempo reale con funzionalità drill-down almeno per: Attacchi, Sessioni, dati Geografici di accesso~~.			
	Funzionalità di reportistica attraverso dashboard e API che consenta: – il monitor in real-time; – la realizzazione di report tramite template predefiniti o personalizzabili; – la possibilità di esportare i report.			
	Fornire funzionalità di Virtual Patching.			
	Supporto standard PCI DSS.			
	~~Funzionalità di Data Loss Prevention.~~			
	Possibilità di interrogare la base dati della soluzione tramite API.			
	Funzionalità di bilanciamento di livello 7 (modello ISO/OSI) delle Applicazioni.			
	~~Possibilità di interrogare la base dati della soluzione tramite API.~~			
	Implementazione di regole e policy personalizzate su base richiesta della PA.			

Tabella 6 – Requisiti minimi WAAP

LOTTO 2 - TABELLA REQUISITI MIGLIORATIVI WAAP BRAND K-ESIMO (DOVE K=1,2,3,4)				
AMBITO	**REQUISITI MIGLIORATIVI**	**DOCUMENTO/I COMPROVANTE/I IL REQUISITO**	**PAGINA/E**	**NOTE**
WAAP	Presenza della funzionalità di CDN oppure web Caching configurabile direttamente sulla soluzione offerta			
	Presenza della funzionalità di API Discovery & Protection.			
	Possibilità di integrazione con soluzioni di terze parti, anche non previste nativamente, attraverso utilizzo di protocolli standard e/o API documentate.			
	~~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~~. 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.			
	Presenza di una dashboard di monitoraggio in tempo reale con funzionalità drill-down almeno per: Attacchi, Sessioni, dati Geografici di accesso.			
	Presenza della funzionalità di Data Loss Prevention.			

Tabella 7 - Requisiti migliorativi WAAP

SWG

LOTTO 2 - TABELLA REQUISITI MINIMI SWG BRAND K-ESIMO (DOVE K=1,2,3,4)				
AMBITO	**REQUISITI MINIMI**	**DOCUMENTO/I COMPROVANTE/I IL REQUISITO**	**PAGINA/E**	**NOTE**
SWG	Funzionalità: – proxy del traffico in modalità trasparente ed esplicita; – capacità di filtraggio delle URL;			

LOTTO 2 - TABELLA REQUISITI MINIMI SWG BRAND K-ESIMO (DOVE K=1,2,3,4)				
AMBITO	**REQUISITI MINIMI**	**DOCUMENTO/I COMPROVANTE/I IL REQUISITO**	**PAGINA/E**	**NOTE**
	– capacità di filtraggio dei contenuti; – capacità di filtraggio dei protocolli, tra cui HTTP/HTTPS/FTP/FTPS/SFTP; – capacità di filtraggio delle applicazioni.			
	Definizione criteri di sicurezza/filtraggio per utente e/o gruppi e definizione di blacklist/whitelist.			
	La soluzione dovrà supportare il reindirizzamento esplicito del traffico verso il servizio SWG mediante PAC file o mediante meccanismi equivalenti di traffic steering nativamente supportati dalla soluzione. Qualora venga utilizzato un PAC file, dovranno essere previsti: - meccanismi di limitazione degli accessi in scrittura; - trasmissione protetta mediante HTTPS. Qualora vengano adottati meccanismi alternativi al PAC file, il Fornitore dovrà garantire un livello di sicurezza almeno equivalente per quanto riguarda la protezione dell'integrità della configurazione e delle informazioni utilizzate per il reindirizzamento del traffico.			
	Web/URL Filtering basato su un insieme ampio e articolato di categorie predefinite (almeno 80), con possibilità di definire categorie personalizzate e di classificare o riclassificare tempestivamente URL e domini in funzione dell'evoluzione delle minacce.			
	Identificazione dei comportamenti potenzialmente pericolosi, blocco dei siti potenzialmente malevoli o categorizzati come tali e blocco dei file in base all'estensione.			
	Presenza di un database di identificativi degli attacchi e delle categorie dei siti (es. SaaS, Piattaforme Streaming, etc...). Questo deve poter essere costantemente aggiornabile anche in base a richieste specifiche della PA.			
	Funzionalità di protezione Anti Malware, WEB/IP reputation e anti-botnet sul traffico gestito.			
	Identificazione attacchi di tipo zero-day.			
	Applicazione delle policy definite anche ai dispositivi offnet. Per tale funzionalità potrà essere previsto l'utilizzo di agent da installare sui dispositivi remoti e che supporti i principali Sistemi Operativi (Windows, MacOS, iOS, Android).			

LOTTO 2 - TABELLA REQUISITI MINIMI SWG BRAND K-ESIMO (DOVE K=1,2,3,4)				
AMBITO	**REQUISITI MINIMI**	**DOCUMENTO/I COMPROVANTE/I IL REQUISITO**	**PAGINA/E**	**NOTE**
	Supporto di alcuni dei principali meccanismi di autenticazione e federazione delle identità, quali Kerberos, LDAP, integrazione con Active Directory, SAML, OIDC, OAUTH2.Supporto di alcuni dei principali meccanismi di autenticazione quali: Kerberos, NTLM, LDAP, AD, SAML.			
	Funzionalità di reportistica attraverso dashboard e API che consenta: – il monitor in real-time; – la realizzazione di report tramite template predefiniti o personalizzabili; – la possibilità di esportare i report.			
	Supporto del protocollo IPv6.			
	Supporto per configurazione in alta affidabilità.			
	Funzionalità di SSL/TLS Inspection.			
	Console di gestione centralizzata per configurazione e implementazione delle policy e controllo degli agent.			

Tabella 8 - Requisiti minimi SWG

LOTTO 2 - TABELLA REQUISITI MIGLORATIVI SWG BRAND K-ESIMO (DOVE K=1,2,3,4)				
AMBITO	**REQUISITI MIGLIORATIVI**	**DOCUMENTO/I COMPROVANTE/I IL REQUISITO**	**PAGINA/E**	**NOTE**
SWG	Possibilità di reindirizzare il traffico verso il Secure Web Gateway in modalità trasparente mediante, a titolo esemplificativo e non esaustivo, protocolli e meccanismi quali WCCP opportunamente autenticato, tunnel IPsec o soluzioni di instradamento basate su policy (Policy Based Routing - PBR), idonei a garantire la sicurezza, l'affidabilità e la continuità operativa del reindirizzamento del traffico.			
	Presenza di una funzionalità di file reputation.			
	Presenza di una funzionalità di DLP nell'ispezione del traffico verso server (HTTP POST): identificazione di parole chiave o pattern di dati e possibilità di effettuare fingerprinting di file/cartelle.			

LOTTO 2 - TABELLA REQUISITI MIGLORATIVI SWG BRAND K-ESIMO (DOVE K=1,2,3,4)				
AMBITO	**REQUISITI MIGLIORATIVI**	**DOCUMENTO/I COMPROVANTE/I IL REQUISITO**	**PAGINA/E**	**NOTE**
	Possibilità di configurare delle eccezioni relativamente al traffico da non intercettare in modalità SSL/TLS inspection.			
	Supporto del protocollo ICAP per l'integrazione con Server ICAP.			
	~~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~~. 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.			
	Possibilità di reindirizzamento del traffico mediante feature di Remote Browser Isolation (RBI).			
	Possibilità di configurazione di eccezioni a livello di traffic steering (es. split tunneling VPN) sulla base di differenti parametri (categoria, applicazioni custom, reti sorgenti, etc...).			
	Possibilità di integrazione con soluzioni di terze parti, anche non previste nativamente, attraverso utilizzo di protocolli standard e/o API documentate.			

Tabella 9 - Requisiti migliorativi SWG

ZTNA

LOTTO 2 - TABELLA REQUISITI MINIMI ZTNA BRAND K-ESIMO (DOVE K=1,2,3)				
AMBITO	**REQUISITI MINIMI**	**DOCUMENTO/I COMPROVANTE/I IL REQUISITO**	**PAGINA/E**	**NOTE**
ZTNA	Garantire in modo trasparente l'accesso alle sole risorse aziendali a cui l'utente è stato autorizzato, su base profilatura.			
	Garantire almeno un metodo di autenticazione forte (SAML, MFA, etc…).			

LOTTO 2 - TABELLA REQUISITI MINIMI ZTNA BRAND K-ESIMO (DOVE K=1,2,3)				
AMBITO	**REQUISITI MINIMI**	**DOCUMENTO/I COMPROVANTE/I IL REQUISITO**	**PAGINA/E**	**NOTE**
	Supporto dei protocolli: FTP, SSH, RDP, SSL, HTTP/HTTPS, etc…).			
	Monitorare e valutare la postura dell'end-point sulla base di specifici criteri anche richiedibili dalla PA (a titolo esemplificativo: tipo e versione Sistema Operativo, tipo e versione del browser, anti-virus aggiornato, geolocalizzazione).			
	Possibilità sia di installazione di agent su dispositivo, sia la possibilità di accesso clientless (agentless) via browser.			
	Supporto dei principali Sistemi Operativi (Windows, Linux, macOS).			
	Funzionalità di reportistica che consentano: - il monitor in real-time attraverso dashboard; - la realizzazione di report attraverso template predefiniti o personalizzabili; - la possibilità di esportare i report.			
	Supporto del protocollo IPv6.			
	La soluzione deve garantire la gestione delle policy di accesso alle risorse aziendali (infrastrutture, dati e applicazioni), personalizzabili in base alle esigenze della PA, in contesti on-prem, cloud e ibridi.			
	Supporto per configurazioni in alta affidabilità.			
	Fornire meccanismi di protezione dalle minacce (malware, phishing, zero-day, etc…).			

Tabella 10 - Requisiti minimi ZTNA

LOTTO 2 - TABELLA REQUISITI MIGLIORATIVI ZTNA BRAND K-ESIMO (DOVE K=1,2,3)				
AMBITO	**REQUISITI MIGLIORATIVI**	**DOCUMENTO/I COMPROVANTE/I IL REQUISITO**	**PAGINA/E**	**NOTE**
ZTNA	Possibilità di permettere l'analisi comportamentale.			
	Possibilità di impedire movimenti laterali.			
	Possibilità di integrazione con soluzioni di terze parti, anche non previste nativamente, attraverso utilizzo di protocolli standard e/o API documentate.			

LOTTO 2 - TABELLA REQUISITI MIGLIORATIVI ZTNA BRAND K-ESIMO (DOVE K=1,2,3)				
AMBITO	**REQUISITI MIGLIORATIVI**	**DOCUMENTO/I COMPROVANTE/I IL REQUISITO**	**PAGINA/E**	**NOTE**
	Presenza di funzionalità di Data Loss Prevention (DLP).			

Tabella 11 - Requisiti migliorativi ZTNA

CASB

LOTTO 2 - TABELLA REQUISITI MINIMI CASB BRAND K-ESIMO (DOVE K=1,2,3)				
AMBITO	**REQUISITI MINIMI**	**DOCUMENTO/I COMPROVANTE/I IL REQUISITO**	**PAGINA/E**	**NOTE**
CASB	Garantire almeno un metodo di autenticazione forte basato su SAML o altro metodo di riconoscimento (MFA).			
	Monitorare la postura di sicurezza dei dispositivi connessi permettendo il blocco degli accessi in situazioni di potenziale compromissione.			
	Funzionalità di Data Loss Prevention (DLP).			
	Monitoraggio degli utenti connessi alle applicazioni SaaS indipendentemente dai dispositivi utilizzati.			
	Monitoraggio continuo e analisi del comportamento utente anche in base a dati storici ad esso relativo (geolocalizzazione, IP, fasce orarie, etc…).			
	Garantire la gestione delle policy di accesso alle applicazioni cloud aziendali predefinite e personalizzabili in base alle esigenze della PA (es. geolocalizzazione, IP, fasce orarie, permessi di accesso alle risorse, etc…) in maniera trasparente per l'end user.			
	Supporto per configurazioni in alta affidabilità.			
	Supporto del protocollo IPv6.			
	Possibilità di installazione di agent su dispositivo e la possibilità di accesso clientless (agentless) via browser per supportare architetture BYOD.			
	Funzionalità di reportistica che consentano: - il monitor in real-time attraverso dashboard; - la realizzazione di report attraverso template predefiniti o personalizzabili (C-level, Compliance, Alert, Shadow IT, etc...); - la possibilità di esportare i report.			
	Analisi del contenuto e delle attività svolte sulle applicazioni SaaS, incluse Microsoft 365 OneDrive, Sharepoint, Teams, permettendo la rilevazione di minacce.			

LOTTO 2 - TABELLA REQUISITI MINIMI CASB BRAND K-ESIMO (DOVE K=1,2,3)				
AMBITO	**REQUISITI MINIMI**	**DOCUMENTO/I COMPROVANTE/I IL REQUISITO**	**PAGINA/E**	**NOTE**
	Rilevazione di tutte le applicazioni cloud aziendali, permettendo l'identificazione di Shadow IT.			
	Implementazione di meccanismi di allarmistica per segnalare eventi potenzialmente pericolosi (comportamenti anomali, dispositivi compromessi, applicazioni non autorizzate, etc…) permettendo la configurazione dei parametri da parte della PA.			
	Meccanismi di protezione dalle minacce (malware, phishing, zero-day, etc…).			
	Accesso alle risorse aziendali sulla base della profilatura utente.			

Tabella 12 - Requisiti minimi CASB

LOTTO 2 - TABELLA REQUISITI MIGLIORATIVI CASB BRAND K-ESIMO (DOVE K=1,2,3)				
AMBITO	**REQUISITI MIGLIORATIVI**	**DOCUMENTO/I COMPROVANTE/I IL REQUISITO**	**PAGINA/E**	**NOTE**
CASB	Presenza di funzionalità di Deep Packet Inspection (DPI).			
	Presenza di una funzionalità di definizione ed implementazione di policy adattative e dinamiche sulla base della postura dei dispositivi e del comportamento utente.			
	Presenza di una funzionalità di analisi del contenuto dello storage di infrastrutture IaaS di tipo Azure, AWS, GCP.			
	Possibilità di integrazione con soluzioni di terze parti, anche non previste nativamente, attraverso utilizzo di protocolli standard e/o API documentate.			

Tabella 13 - Requisiti migliorativi CASB

SEG

LOTTO 2 - TABELLA REQUISITI MINIMI SEG BRAND K-ESIMO (DOVE K=1,2,3,4)				
AMBITO	**REQUISITI MINIMI**	**DOCUMENTO/I COMPROVANTE/I IL REQUISITO**	**PAGINA/E**	**NOTE**
SEG	Supporto al Mail Transfer Agent.			
	Funzionalità di protezione a più livelli per l'individuazione dello SPAM e la rilevazione di minacce attraverso più meccanismi quali l'analisi approfondita del contenuto delle email e il filtraggio delle URL presenti nel corpo del messaggio.			
	Funzionalità di anti-virus, anti-phishing, anti-BEC, anti-spoofing, Cousin Domain Detection, anti-spam e anti-malware in grado di identificare virus, worms, ransomware attraverso il riconoscimento di signature e analisi euristica dei contenuti.			
	Protezione da email massive e di marketing.			
	Protezione realtime attraverso API o SMTP relay.			
	Identificazione di attacchi di tipo zero-day.			
	Blocco email in base alla lingua utilizzata o specifici charset.			
	Rimozione, tramite l'analisi del contenuto dell'email e degli allegati, di file malevoli. Identificazione, tramite analisi di tipo true file type, della tipologia di file e inclusione URLs potenzialmente pericolosi.			
	Trattamento delle email per quali è stato identificato un virus/malware con varie opzioni quali l'invio di una notifica, la quarantena, l'eliminazione del messaggio, l'inserimento in white/black list.			
	Supporto dei filtri basati sulla reputazione dell'indirizzo IP di provenienza e/o URL.			
	Ispezione sulla posta in uscita e in ingresso.			
	Crittografia dei messaggi in uscita con protocollo SSL/TLS.			
	Supporto dell'autenticazione tramite LDAP/AD.			
	Aggiornamenti costanti delle signature attraverso feed di threat intelligence.			
	Possibilità di bloccare allegati e/o contenuti attivi nelle mail (es. MACRO). La soluzione deve segnalare all'amministrazione/utente l'avvenuto blocco.			

LOTTO 2 - TABELLA REQUISITI MINIMI SEG BRAND K-ESIMO (DOVE K=1,2,3,4)				
AMBITO	**REQUISITI MINIMI**	**DOCUMENTO/I COMPROVANTE/I IL REQUISITO**	**PAGINA/E**	**NOTE**
	La soluzione deve avere funzionalità di reportistica che consentano: - il monitor in real-time attraverso dashboard; - la realizzazione di report attraverso template predefiniti e personalizzabili; - la possibilità di esportare i report.			
	Supporto del protocollo IPv6.			
	Supporto per configurazione in alta affidabilità.			
	Supporto dei protocolli SPF, DKIM o in alternativa del protocollo DMARC.			
	Cifratura automatica dei messaggi in uscita per i quali risultano verificate delle politiche di identificazione configurabili (policy based encryption).			
	Identificazione di immagini potenzialmente dannose.			
	Creazione di regole di spam personalizzate.			
	Identificazione di testo nascosto all'interno di immagini presenti nelle email.			
	Possibilità di interrogare la base-dati della soluzione tramite API.			
	Funzionalità di Data Loss Prevention nell'ispezione delle mail in uscita almeno attraverso l'identificazione di parole chiave o pattern di dati.			
	Supporto alla segnalazione delle mail sospette di spam attraverso meccanismi di semplificazione della segnalazione da parte degli utenti.			

Tabella 14 - Requisiti minimi SEG

LOTTO 2 - TABELLA REQUISITI MIGLIORATIVI SEG BRAND K-ESIMO (DOVE K=1,2,3,4)				
AMBITO	**REQUISITI MIGLIORATIVI**	**DOCUMENTO/I COMPROVANTE/I IL REQUISITO**	**PAGINA/E**	**NOTE**
SEG	~~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~~. 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.			
	Possibilità di gestione e analisi sicura dei QR Code contenuti nel corpo mail o negli allegati, allo scopo di identificare gli URL ad essi associati ed effettuare azioni diverse in base alla categoria a cui gli stessi URL appartengono.			
	Supporto allo standard ARC (Authenticated Received Chain), come ulteriore livello di sicurezza relativo alla verifica del mittente.			
	Possibilità di integrazione con soluzioni di terze parti, anche non previste nativamente, attraverso utilizzo di protocolli standard e/o API documentate.			
	Possibilità di supporto del protocollo di sicurezza DANE (DNS-based Authentication of Named Entities) per rafforzare le misure di verifica sui mittenti e contribuire alla mitigazione degli attacchi di tipo man-in-the-middle.			

Tabella 15 - Requisiti migliorativi SEG

Anti APT

LOTTO 2 - TABELLA REQUISITI MINIMI ANTI-APT BRAND K-ESIMO (DOVE K=1,2,3)				
AMBITO	**REQUISITI MINIMI**	**DOCUMENTO/I COMPROVANTE/I IL REQUISITO**	**PAGINA/E**	**NOTE**
ANTI-APT	Supportare ambienti di analisi basati su Sistemi Operativi Windows, MacOS e Unix-based.			
	Rilevazione in ambiente isolato: – mediante analisi comportamentale di malware, minacce zero-day e APT; – mediante analisi del traffico di comunicazioni C&C, botnet, worm.			
	Supporto di almeno le seguenti tipologie di file: .zip, .gz, .bz2, .exe, .dll, .bat, .pdf, .jar, .doc, .docx, .xls, .xlsx, .ppt, .pptx., .iso, .img.			
	Permettere la personalizzazione degli ambienti di analisi al fine di garantire le stesse caratteristiche (configurazioni, drivers, applicazioni installate, etc…) dell'ambiente di esercizio.			
	Permettere di operare in modalità interattiva e/o automatizzata.			
	Raccolta di screenshot di ciò che accade all'interno dell'ambiente d'analisi durante la detonazione di una sample, integrandoli nei report d'analisi.			
	Integrazione di regole di pattern detection, quali YARA rules, personalizzate e definite dalla PA a seconda delle necessità.			
	Estrazione di IoC, IoA, identificati durante l'esecuzione dell'analisi, permettendone l'export nei formati standard (STIX).			
	Parallelizzare più macchine virtuali per l'analisi contemporanea di più sample.			
	Funzionalità di reportistica che consentano: - il monitor in real-time attraverso dashboard; - la realizzazione di report attraverso template predefiniti o personalizzabili; - la possibilità di esportare i report che contengano tutte le attività svolte e i relativi risultati sia in termini di scoring che di indicatori quali, a titolo esemplificativo: o URLs estratti; o Processi creati a runtime; o Connessioni realizzate verso l'esterno (possibile C&C), movimento laterale, botnet, worm; o tentativi di Privilege Escalation;			

LOTTO 2 - TABELLA REQUISITI MINIMI ANTI-APT BRAND K-ESIMO (DOVE K=1,2,3)				
AMBITO	**REQUISITI MINIMI**	**DOCUMENTO/I COMPROVANTE/I IL REQUISITO**	**PAGINA/E**	**NOTE**
	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.			
	Meccanismi di notifica (email, trouble-ticket, etc…) quando il risultato dell'analisi evidenzia comportamenti pericolosi.			
	Deve essere possibile gestire la configurazione della soluzione via GUI (Graphical User Interface) o CLI (Command Line Interface).			
	Supporto del protocollo IPv6.			
	Supporto a configurazione in alta affidabilità.			

Tabella 16 - Requisiti minimi ANTI-APT

LOTTO 2 - TABELLA REQUISITI MIGLIORATIVI ANTI-APT BRAND K-ESIMO (DOVE K=1,2,3)				
AMBITO	**REQUISITI MIGLIORATIVI**	**DOCUMENTO/I COMPROVANTE/I IL REQUISITO**	**PAGINA/E**	**NOTE**
ANTI-APT	Possibilità di supportare ambienti di analisi OT e ICS.			
	Presenza di tecniche anti evasive che siano in grado di trattare malware progettati per riconoscere l'esecuzione in ambiente di analisi (ad esempio rimanendo latenti fino a quando non siano effettuate operazioni che indichino l'effettiva presenza di un utente reale come l'esecuzione di un click del mouse, etc...).			
	Presenza della funzionalità di analisi dell'intero ciclo di vita di un malware, riconducendolo alla tassonomia definita MITRE ATT&CK.			
	Presenza di funzionalità di integrazione con soluzioni di terze parti, anche non previste nativamente, attraverso utilizzo di protocolli standard, API documentate al fine di permettere l'analisi delle sample ritenute sospette inviate dalle soluzioni stesse.			
	~~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~~.			

LOTTO 2 - TABELLA REQUISITI MIGLIORATIVI ANTI-APT BRAND K-ESIMO (DOVE K=1,2,3)				
AMBITO	**REQUISITI MIGLIORATIVI**	**DOCUMENTO/I COMPROVANTE/I IL REQUISITO**	**PAGINA/E**	**NOTE**
	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.			

Tabella 17 - Requisiti migliorativi ANTI-APT

VERIFICHE TECNICHE SPECIFICHE - LOTTO 3
NAC

LOTTO 3 - TABELLA REQUISITI MINIMI NAC BRAND K-ESIMO (DOVE K=1,2,3,4)				
AMBITO	**REQUISITI MINIMI**	**DOCUMENTO/I COMPROVANTE/I IL REQUISITO**	**PAGINA/E**	**NOTE**
NAC	Discovery degli endpoint connessi alle reti aziendali e aggiornamento dell'inventario dei dispositivi connessi, siano essi Personali, aziendali, sistemi IoT, etc...			
	Controllo degli accessi in base alle policy di sicurezza.			
	Gestione accessi Guest.			
	Profilatura degli endpoint di rete indipendentemente dalla modalità di accesso alla rete.			
	Supporto standard 802.1x, MAC Authentication, Web Authentication.			
	Integrazione con sistemi di Identity Management esterni: Radius/LDAP/Active Directory. Inoltre deve permettere l'utilizzo della Multi-Factor Authentication.			
	Assegnazione dinamica della VLAN in base a parametri di autenticazione o profilatura.			
	Isolamento di endpoint di rete non autorizzati.			
	Gestione delle regole e policy da una dashboard centralizzata.			
	Funzionalità di BYOD (Bring Your Own Device) almeno per endpoint Android e iOS.			

LOTTO 3 - TABELLA REQUISITI MINIMI NAC BRAND K-ESIMO (DOVE K=1,2,3,4)				
AMBITO	**REQUISITI MINIMI**	**DOCUMENTO/I COMPROVANTE/I IL REQUISITO**	**PAGINA/E**	**NOTE**
	Funzionalità di check compliance con agent su endpoint Windows, MacOS e Linux, con possibilità di verifica della presenza di software installati e/o file sul sistema operativo e/o software antivirus.			
	Visibilità dispositivi IoT.			
	Funzionalità di reportistica che consentano: - il monitor in real-time attraverso dashboard; - la realizzazione di report attraverso template predefiniti o personalizzabili; - la possibilità di esportare i report.			
	Supporto del protocollo IPv6.			
	Supporto per configurazione in alta affidabilità.			
	Funzionalità Radius Server.			
	Profilatura degli endpoint basata su tecniche agent-less.			
	Implementazione di strategia Role Based Access Control e Least Privilege.			
	Funzionalità di creazione livelli di segmentazione della rete al fine di definire regole puntuali e adattate al segmento.			
	Valutazione della postura di sicurezza dei dispositivi aziendali e degli endpoint prima di permettere l'accesso alla rete.			

Tabella 18 - Requisiti minimi NAC

LOTTO 3 - TABELLA REQUISITI MIGLIORATIVI NAC BRAND K-ESIMO (DOVE K=1,2,3,4)				
AMBITO	**REQUISITI MIGLIORATIVI**	**DOCUMENTO/I COMPROVANTE/I IL REQUISITO**	**PAGINA/E**	**NOTE**
NAC	Possibilità di configurare risposte automatiche ad eventi di rete specifici al fine di contenere il propagarsi degli attacchi			
	Presenza di una funzionalità di analisi dinamica dei comportamenti dei vari dispositivi connessi, utilizzando tecniche automatizzate per classificarli.			
	~~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.~~			

	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.			
	Presenza di funzionalità di integrazione con soluzioni di terze parti, anche non previste nativamente, attraverso utilizzo di protocolli standard e/o API documentate.			
	Possibilità di gestire switch attraverso l'utilizzo del solo protocollo SNMP.			
	Presenza di una funzionalità di supporto protocollo TACACS+ (RFC 8907) per gestione utenti amministrativi.			
	Presenza di una funzionalità che consenta di implementare strategie Zero Trust per garantire la sicurezza della rete aziendale.			

Tabella 19 - Requisiti migliorativi NAC

IAM

LOTTO 3 - TABELLA REQUISITI MINIMI IAM BRAND K-ESIMO (DOVE K=1,2,3,4)				
AMBITO	**REQUISITI MINIMI**	**DOCUMENTO/I COMPROVANTE/I IL REQUISITO**	**PAGINA/E**	**NOTE**
IAM	Automazione dei processi di creazione, aggiornamento periodico e rimozione delle identità e delle utenze.			
	Definizione e gestione dei profili e dei ruoli, specificando per ogni risorsa i privilegi d'accesso.			
	Garantire la definizione di policy granulari basate su attributi e informazioni di contesto.			
	Integrazione nativa con sistemi SSO fornendo l'accesso attraverso diverse applicazioni e servizi definibili dalla PA.			
	Supporto alla Multi Factor Authentication.			
	Funzionalità di offuscamento delle informazioni relative a login falliti e/o errori (dove risiede l'errore, etc...).			
	Funzionalità di definizione del ciclo di vita delle password utente (durata della password, regole di costruzione, riutilizzo, etc...).			
	Le password devono essere conservate e trasmesse in maniera sicura attraverso protocolli specifici e crittografia.			
	Garantire policy di accesso da remoto granulari per ogni singolo utente (VPN, etc...).			
	Implementazione di misure di logging dettagliate di tutti i tentativi di autenticazione e attività utente.			
	Permettere il blocco automatico dell'accesso dopo un numero di tentativi falliti personalizzabile.			
	Permettere la personalizzazione delle attività di reset, sblocco e richieste d'accesso self-service anche in base al profilo/ruolo utente.			

	Gestione centralizzata di policy, gestione degli accessi e monitoring dello stato del sistema			
	Motore di analisi del rischio per valutazione del contesto (geolocalizzazione, device, storico degli accessi).			

Tabella 20 - Requisiti minimi IAM

LOTTO 3 - TABELLA REQUISITI MIGLIORATIVI IAM BRAND K-ESIMO (DOVE K=1,2,3,4)				
AMBITO	**REQUISITI MIGLIORATIVI**	**DOCUMENTO/I COMPROVANTE/I IL REQUISITO**	**PAGINA/E**	**NOTE**
IAM	Presenza di una funzionalità di Risk Based Authentication per modulare dinamicamente l'autenticazione in funzione del rischio.			
	Presenza di una funzionalità di supporto per scenari “mobile” di registrazione del dispositivo, autenticazione e autorizzazione anche adoperando notifiche push.			
	Presenza di una funzionalità di verifica real time dell'attendibilità della sorgente che ha scatenato l'evento relativo al cambiamento dell'identità sui sistemi connessi.			
	Possibilità di definire dei workflow di gestione delle utenze.			
	Presenza di funzionalità di integrazione con soluzioni di terze parti, anche non previste nativamente, attraverso utilizzo di protocolli standard e/o API documentate.			
	~~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.~~ 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.			

Tabella 21 - Requisiti migliorativi IAM

PAM

LOTTO 3 - TABELLA REQUISITI MINIMI PAM BRAND K-ESIMO (DOVE K=1,2,3)				
AMBITO	**REQUISITI MINIMI**	**DOCUMENTO/I COMPROVANTE/I IL REQUISITO**	**PAGINA/E**	**NOTE**
PAM	Gestione delle password di accesso attraverso l'utilizzo di una "cassaforte" elettronica in grado di generare password sicure in maniera dinamica.			
	Garantire la protezione delle password salvate attraverso protocolli sicuri di encryption.			
	Supporto gestione delle chiavi SSH.			
	Isolamento delle sessioni privilegiate.			
	Monitoraggio delle sessioni privilegiate in real time.			
	Tracciatura e registrazione delle attività dell'utente durante la sessione privilegiata, al fine di effettuare audit sulle attività effettuate (Capability to monitor, record, and control privileged sessions in real-time).			
	Possibilità di limitare l'accesso in base all'orario			
	Funzionalità di reportistica e logging che consentano: - il tracciamento di tutte le attività privilegiate; - il monitor in real-time attraverso dashboard; - la realizzazione di report attraverso template predefiniti e personalizzabili; - la possibilità di esportare i report.			
	Discovery automatico degli account privilegiati.			
	Supporto all'autenticazione di terze parti (ad es. fornitori, consulenti) che accedono da remoto.			
	Possibilità di utilizzare una password in real-time senza che l'utente conosca mai la password utilizzata.			
	Supporto IPv6.			
	Supporto alta affidabilità.			
	Possibilità di definire dei workflow per la gestione del processo autorizzativo degli accessi per gli account privilegiati.			
	Possibilità di effettuare un'analisi di dettaglio delle minacce informatiche per identificare, segnalare e bloccare attività privilegiate anomale, anche in funzione del loro grado di criticità.			
	Possibilità di limitare l'accesso sulla base della localizzazione dell'utente.			
	Gestione delle password anche per Machine to Machine e Application to Application.			

LOTTO 3 - TABELLA REQUISITI MINIMI PAM BRAND K-ESIMO (DOVE K=1,2,3)				
AMBITO	**REQUISITI MINIMI**	**DOCUMENTO/I COMPROVANTE/I IL REQUISITO**	**PAGINA/E**	**NOTE**
	Permettere di definire policy basate sul Least Privilege, gestendole su base ruoli, utenti o gruppi.			
	Garantire la corretta protezione sia delle password, sia delle sessioni (encryption, hashing, etc…).			
	Funzionalità di cambio password amministrativa automatico dopo ogni singolo utilizzo.			

Tabella 22 - Requisiti minimi PAM

LOTTO 3 - TABELLA REQUISITI MIGLIORATIVI PAM BRAND K-ESIMO (DOVE K=1,2,3)				
AMBITO	**REQUISITI MIGLIORATIVI**	**DOCUMENTO/I COMPROVANTE/I IL REQUISITO**	**PAGINA/E**	**NOTE**
PAM	Presenza di funzionalità di integrazione con soluzioni di terze parti, anche non previste nativamente, attraverso utilizzo di protocolli standard e/o API documentate			
	Possibilità di supporto a dispositivi iOS e Android.			
	~~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.~~ 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.			
	Possibilità di configurare regole d'accesso e assegnazione dei privilegi basata sulla geolocalizzazione.			
	Presenza di funzionalità di gestione centralizzata di tutte le policy di rilascio dei privilegi, permettendo inoltre la completa supervisione del processo.			
	Presenza di una funzionalità di richiesta delle credenziali privilegiate per mezzo di autenticazione forte.			

Tabella 23 - Requisiti migliorativi PAM

DLP

LOTTO 3 - TABELLA REQUISITI MINIMI DLP BRAND K-ESIMO (DOVE K=1,2,3)				
AMBITO	**REQUISITI MINIMI**	**DOCUMENTO/I COMPROVANTE/I IL REQUISITO**	**PAGINA/E**	**NOTE**
DLP	Compatibilità con dispositivi di vario genere (dispositivi fissi, mobili o personali) e indipendente dal Sistema Operativo adoperato (Windows, Linux, MacOS).			
	Funzionalità di Data Discovery.			
	Sulla base della classificazione delle informazioni e delle policy aziendali, garantire la corretta protezione dei dati gestiti dagli endpoint, a riposo o in transito (encryption, hashing, etc…).			
	Consentire il blocco automatico di attività che violino le policy aziendali.			
	Identificazione di dispositivi di memoria di massa connessi agli endpoint ed impedire che questi vengano adoperati impropriamente (estrazione dati aziendali protetti, copia di documenti non protetti adeguatamente, etc…).			
	Funzionalità di reportistica che consentano: - il monitor in real-time attraverso dashboard; - la realizzazione di report attraverso template predefiniti e personalizzabili; - la possibilità di esportare i report.			
	Supporto protocollo IPv6.			
	Supporto alta affidabilità.			
	Possibilità di interrogare la base dati della soluzione tramite API.			
	Presenza di meccanismi di notifica immediata, tramite mail o strumento definito dalla PA, all'utente e alla struttura decisa dalla PA, nel momento in cui si rilevano attività che contravvengono alle policy definite (es. invio di file classificati verso l'esterno dell'azienda o account personali non autorizzati).			

Tabella 24 - Requisiti minimi DLP

LOTTO 3 - TABELLA REQUISITI MIGLIORATIVI DLP BRAND K-ESIMO (DOVE K=1,2,3)				
AMBITO	**REQUISITI MIGLIORATIVI**	**DOCUMENTO/I COMPROVANTE/I IL REQUISITO**	**PAGINA/E**	**NOTE**
DLP	Presenza di una funzionalità di rilevazione testo per immagini OCR: possibilità di analizzare il contenuto informativo all'interno di file immagine o documenti, bloccandone l'eventuale trasmissione sia per email, canali web che per invii tra endpoint.			
	Presenza di una funzionalità di implementazione policy che consentano di prevenire l'invio di dati verso IP appartenenti ad area geografiche considerate rischiose.			
	Presenza di una funzionalità di content inspection, quali ad esempio pattern matching, ricerca di parole chiave etc…, che permettano una più accurata disamina dei contenuti che richiedono protezione.			
	Presenza di funzionalità di integrazione con soluzioni di terze parti, anche non previste nativamente, attraverso utilizzo di protocolli standard e/o API documentate.			

Tabella 25 - Requisiti migliorativi DLP

VERIFICHE TECNICHE SPECIFICHE - LOTTO 4

EPP/EDR

LOTTO 4 - TABELLA REQUISITI MINIMI EPP/EDR BRAND K-ESIMO (DOVE K=1,2,3)				
AMBITO	**REQUISITI MINIMI**	**DOCUMENTO/I COMPROVANTE/I IL REQUISITO**	**PAGINA/E**	**NOTE**
EPP/EDR	Protezione di tutti i Sistemi Operativi principalmente in uso, quali Windows, MacOS.			
	Implementazione di misure di analisi continue, inclusa l'analisi statica dei file, per l'identificazione di attività anomale o maliziose sugli endpoint.			
	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.			
	La soluzione deve effettuare: - il blocco di azioni dannose; - la gestione della quarantena dei file; - la pulizia dell'endpoint in seguito al rilevamento di malware.			
	Protezione del traffico in entrata e in uscita dagli endpoint, comprensivo di controllo delle applicazioni, delle porte e dei protocolli utilizzati al fine di prevenire attacchi e intrusioni contro gli endpoint.			
	Capacità di impostare regole per limitare o bloccare l'accesso a supporti removibili collegati all'endpoint.			
	Capacità di definire policy di sicurezza attraverso le quali sia consentita l'esecuzione dei soli programmi autorizzati.			
	Presenza di funzionalità di reportistica attraverso dashboard e API che consentano: - il monitor in real-time attraverso dashboard; - la realizzazione di report attraverso template predefiniti o personalizzabili; - la possibilità di esportare i report.			
	Supporto del protocollo IPv6.			

LOTTO 4 - TABELLA REQUISITI MINIMI EPP/EDR BRAND K-ESIMO (DOVE K=1,2,3)				
AMBITO	**REQUISITI MINIMI**	**DOCUMENTO/I COMPROVANTE/I IL REQUISITO**	**PAGINA/E**	**NOTE**
	Supporto configurazione in alta affidabilità.			
	Installazione Agent attraverso sistemi centralizzati di distribuzione. Il sistema centralizzato deve permettere l'enforcing delle policy di sicurezza su tutti gli endpoint.			
	Permettere il blocco preventivo dell'accesso a siti maliziosi o l'apertura di allegati o file sconosciuti.			
	La soluzione EPP/EDR deve garantire la visibilità e il controllo delle periferiche collegate agli endpoint, assicurando meccanismi di monitoraggio, applicazione di policy di sicurezza, rilevazione di utilizzi anomali e registrazione degli eventi ai fini di audit e investigazione.			
	Riduzione dell'impatto sulle performance dei sistemi, garantendo un utilizzo ottimale delle risorse a disposizione.			

Tabella 26 - Requisiti minimi EPP/EDR

LOTTO 4 - TABELLA REQUISITI MIGLIORATIVI EPP/EDR BRAND K-ESIMO (DOVE K=1,2,3)				
AMBITO	**REQUISITI MIGLIORATIVI**	**DOCUMENTO/I COMPROVANTE/I IL REQUISITO**	**PAGINA/E**	**NOTE**
EPP/EDR	Presenza di protezione sistemi Unix-based.			
	Presenza di protezione dispositivi mobili (Android, iOS).			
	Presenza di una funzionalità di identificazione del comportamento utente, rilevando e segnalando eventuali discostamenti da quest'ultimo.			
	Presenza di una funzionalità di analisi di tutte le attività che vengono eseguite sugli endpoint, tenendo traccia delle attività di networking, modifiche a file e registri, etc…			
	Presenza di una funzionalità di visualizzazione scanner-less sulle vulnerabilità e conseguente associazione di un fattore di rischio ad uno specifico endpoint.			
	Possibilità di protezione da attacchi di tipo file-less, memory injection e obfuscated malware attraverso meccanismi di manipolazione della memoria utilizzata dai processi.			

LOTTO 4 - TABELLA REQUISITI MIGLIORATIVI EPP/EDR BRAND K-ESIMO (DOVE K=1,2,3)				
AMBITO	**REQUISITI MIGLIORATIVI**	**DOCUMENTO/I COMPROVANTE/I IL REQUISITO**	**PAGINA/E**	**NOTE**
	~~Presenza di funzionalità di mapping delle tecniche e tattiche di attacco, mettendole in relazione con la tassonomia ACN.~~ Presenza di una funzionalità di mapping delle tecniche e tattiche di attacco, mettendole in relazione con il framework MITRE ATT&CK.			
	Presenza di strumenti di investigazione (dashboards) sulla base di records storici per analizzare la timeline di un attacco e sulla base di system snapshot per analizzare lo stato attuale dell'endpoint.			
	Presenza di funzionalità di sicurezza volte a garantire la privacy di tutte le informazioni utente presenti sul dispositivo, implementando anche l'encryption dei dati considerati privati.			
	Presenza di funzionalità di integrazione con soluzioni di terze parti, anche non previste nativamente, attraverso utilizzo di protocolli standard e/o API documentate.			
	~~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~~. 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.			
	Presenza di una funzionalità che consenta la rappresentazione degli attacchi in modo dettagliato e comprensibile per l'operatore. L'EPP dovrà fornire una alberatura completa dei processi, dei tipi di attacco, la data di rilevamento, la famiglia di malware e le tecniche utilizzate, facilitando l'analisi dell'infezione ed il livello di rischio per la PA.			

Tabella 27 - Requisiti migliorativi EPP/EDR

SPP

LOTTO 4 - TABELLA REQUISITI MINIMI SPP BRAND K-ESIMO (DOVE K=1,2)				
AMBITO	**REQUISITI MINIMI**	**DOCUMENTO/I COMPROVANTE/I IL REQUISITO**	**PAGINA/E**	**NOTE**
SPP	Supporto ai principali Sistemi Operativi, siano essi Windows-based o Linux-Based.			
	Supporto agli ambienti di virtualizzazione, ad esempio VMWare, Microsoft Hyper-V etc… (per tutti gli ambienti offerti, il Fornitore dovrà indicare in offerta l'elenco delle versioni supportate).			
	Garantire protezione contro attacchi di livello applicativo, inclusi attacchi botnet, DDoS e altre minacce che mirano a sfruttare vulnerabilità applicative per compromettere la disponibilità, l'integrità o la riservatezza dei dati e dei servizi.			
	Funzionalità di reportistica e logging che consentano: - il monitor in real-time attraverso dashboard; - la realizzazione di report attraverso template predefiniti; - la possibilità di esportare i report.			
	Supporto del protocollo IPv6.			
	Supporto alta affidabilità.			
	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.			
	Protezione di tutti i dati memorizzati nel Server, garantendo la protezione contro attacchi tipici delle basi dati.			
	Funzionalità di protezione dei file di sistema critici e delle chiavi di registro da manomissioni, autorizzando le modifiche solo in accordo alle policy definite.			
	Riduzione all'impatto sulle performance dei sistemi, garantendo un utilizzo ottimale delle risorse a disposizione.			

Tabella 28 - Requisiti minimi SPP

LOTTO 4 - TABELLA REQUISITI MIGLIORATIVI SPP BRAND K-ESIMO (DOVE K=1,2)				
AMBITO	**REQUISITI MIGLIORATIVI**	**DOCUMENTO/I COMPROVANTE/I IL REQUISITO**	**PAGINA/E**	**NOTE**
SPP	Presenza di una funzionalità di monitoring e analisi del traffico contro anomalie e possibili pericoli.			
	~~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~~. 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.			
	~~Presenza di funzionalità di mapping delle tecniche e tattiche di attacco, mettendole in relazione con la tassonomia ACN.~~ Presenza di una funzionalità di mapping delle tecniche e tattiche di attacco, mettendole in relazione con il framework MITRE ATT&CK.			
	~~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.~~ 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…			
	Presenza di una funzionalità di investigazione sulla base di records storici per analizzare la timeline di un attacco e sulla base di system snapshot per analizzare lo stato attuale del server.			
	Presenza di funzionalità di integrazione con soluzioni di terze parti, anche non previste nativamente, attraverso utilizzo di protocolli standard e/o API documentate.			

Tabella 29 - Requisiti migliorativi SPP

SIEM

LOTTO 4 - TABELLA REQUISITI MINIMI SIEM BRAND K-ESIMO (DOVE K=1,2,3,4)				
AMBITO	**REQUISITI MINIMI**	**DOCUMENTO/I COMPROVANTE/I IL REQUISITO**	**PAGINA/E**	**NOTE**
SIEM	Capacità di raccogliere i log/eventi generati dagli apparati, dai sistemi e dalle applicazioni, standardizzando i formati di log per l'analisi e la correlazione.			
	Acquisizione dei log/eventi in real time tramite parser completi già disponibili nativamente nella soluzione.			
	Funzionalità di sviluppo parser di normalizzazione ad hoc per sorgenti non disponibili nativamente.			
	Identificazione e correlazione degli eventi per effettuale la detection delle anomalie e dei potenziali incidenti di sicurezza.			
	Garantire la compressione e memorizzazione dei log/eventi, garantendone l'integrità e l'indicizzazione, consentendo anche l'impostazione della retention (di almeno 12 mesi).			
	Implementazione di regole di correlazione personalizzabili, tenendo in considerazione anche eventi provenienti da differenti sorgenti.			
	Prevedere la possibilità di assegnazione di ruoli interni al SIEM, permettendo l'assegnazione della gestione e risoluzione di particolari incidenti/eventi a personale specifico.			
	Funzionalità di reportistica che consenta: - il monitor in real-time attraverso dashboard; - la realizzazione di report attraverso template predefiniti; - la possibilità di esportare i report; - la realizzazione di report personalizzati.			
	Supporto Protocollo IPv6.			
	Supporto per configurazione in alta affidabilità.			
	Funzionalità di ticketing, il sistema deve fornire la funzionalità integrata di ticketing (gestione dei ticket) e la possibilità di integrarsi con sistemi esterni di gestione di ticketing.			
	Prioritizzazione degli incidenti per severità e impatto, con livelli adattabili e personalizzabili al contesto della PA.			
	~~Possibilità di mappare gli alert di sicurezza con il framework MITRE ATT&CK o tassonomia cyber dell'ACN.~~			
	Supporto modalità multi-tenancy.			

Tabella 30 - Requisiti minimi SIEM

LOTTO 4 - TABELLA REQUISITI MIGLIORATIVI SIEM BRAND K-ESIMO (DOVE K=1,2,3,4)				
AMBITO	**REQUISITI MIGLIORATIVI**	**DOCUMENTO/I COMPROVANTE/I IL REQUISITO**	**PAGINA/E**	**NOTE**
SIEM	Presenza di una funzionalità di allarmistica e segnalazione tramite differenti mezzi, quali ad esempio mail, ticketing, soluzione personalizzata della PA, etc..			
	Presenza di una funzionalità di monitoraggio delle configurazioni~~. Il sistema deve poter collezionare le configurazioni degli apparati di rete,~~ al fine di identificarne i cambiamenti~~, e fornire una funzionalità di comparazione delle varie revisioni~~.			
	Presenza di una funzionalità di creazione dashboard personalizzabili dalla PA per la visualizzazione di metriche e trend di attacco rilevanti			
	~~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~~. 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.			
	Presenza di funzionalità di integrazione con soluzioni di terze parti, anche non previste nativamente, attraverso utilizzo di protocolli standard e/o API documentate.			
	~~Presenza di funzionalità di mapping delle tecniche e tattiche di attacco, mettendole in relazione con la tassonomia ACN.~~ Possibilità di mappare gli alert di sicurezza con il framework MITRE ATT&CK o tassonomia cyber dell'ACN.			

Tabella 31 - Requisiti migliorativi SIEM

SOAR

LOTTO 4 - TABELLA REQUISITI MINIMI SOAR BRAND K-ESIMO (DOVE K=1,2,3)				
AMBITO	**REQUISITI MINIMI**	**DOCUMENTO/I COMPROVANTE/I IL REQUISITO**	**PAGINA/E**	**NOTE**
SOAR	Orchestrazione del processo di risposta agli incidenti di sicurezza informatici attraverso l'impiego di playbook standardizzati e automatizzati.			
	Il SOAR deve: - permettere la creazione, gestione ed esecuzione di workflow automatizzati (playbook) per gestire la fase di incident response; - includere playbook predefiniti out-of-the-box.			
	Capacità di mettere in relazione nuovi incidenti di sicurezza con incidenti già risolti, di identificare investigazioni duplicate, al fine di ridurre i tempi di indagine.			
	Permettere la realizzazione di workflow più o meno complessi, includendo la possibilità di realizzare operazioni condizionali o decisionali.			
	Funzionalità di confronto degli Indicatori di Compromissione raccolti con gli incidenti in analisi.			
	Raccolta di informazioni dettagliate di tutte le attività svolte all'interno dell'indagine effettuata e di tutti gli incidenti.			
	Supporto protocollo IPv6.			
	Supporto implementazione in alta affidabilità.			
	Disponibilità di dashboard e reportistica per ricavare ed evidenziare le metriche/livelli di servizio più significativi relativi alle procedure di incident response, misurare la loro efficacia e l'efficacia delle misure di sicurezza adottate. Possibilità di esportare la reportistica e di realizzare dei report personalizzati.			
	La soluzione deve poter implementare l'import e l'export di Indicatori di Compromissione, anche attraverso task automatizzati o periodici.			
	Funzionalità di interfaccia grafica per la creazione dei playbook.			
	Funzionalità di gestione degli incidenti; la soluzione deve disporre di un sistema di incident management integrato che permetta di assegnare le attività a specifici utenti della piattaforma, tracciandone le attività.			

LOTTO 4 - TABELLA REQUISITI MINIMI SOAR BRAND K-ESIMO (DOVE K=1,2,3)				
AMBITO	**REQUISITI MINIMI**	**DOCUMENTO/I COMPROVANTE/I IL REQUISITO**	**PAGINA/E**	**NOTE**
	Funzionalità di creazione di diversi utenti con ruoli differenziati in modo da definire la visibilità e l'accesso a specifiche aree e /o informazioni del sistema.			
	Implementazione di Multi Factor Authentication e l'integrazione con sistemi di gestione delle identità aziendali.			
	Presenza di dashboard predefinite che supportino gli analisti nella visualizzazione e gestione degli incidenti di sicurezza. Queste dashboard devono fornire una rappresentazione chiara degli indicatori di compromissione (IoC) e delle metriche chiave relative agli incidenti.			
	Possibilità di definire dashboard specifiche per ogni categoria di incidente definita, in modo da mettere in evidenza solo le informazioni rilevanti per tale categoria.			
	Capacità del SOAR di estrarre contenuti da file, binari ed email in maniera indipendente.			
	Supporto modalità multi-tenancy.			

Tabella 32 - Requisiti minimi SOAR

LOTTO 4 - TABELLA REQUISITI MIGLIORATIVI SOAR BRAND K-ESIMO (DOVE K=1,2,3)				
AMBITO	**REQUISITI MIGLIORATIVI**	**DOCUMENTO/I COMPROVANTE/I IL REQUISITO**	**PAGINA/E**	**NOTE**
SOAR	Presenza di funzionalità di integrazione con soluzioni di terze parti, anche non previste nativamente, attraverso utilizzo di protocolli standard e/o API documentate.			
	~~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~~. 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.			

LOTTO 4 - TABELLA REQUISITI MIGLIORATIVI SOAR BRAND K-ESIMO (DOVE K=1,2,3)				
AMBITO	**REQUISITI MIGLIORATIVI**	**DOCUMENTO/I COMPROVANTE/I IL REQUISITO**	**PAGINA/E**	**NOTE**
	Presenza di funzionalità di comunicazione e collaborazione che consentano la condivisione delle informazioni fra gli analisti di sicurezza.			
	Presenza di funzionalità di debug dei playbook e ripresa della routine dal punto di interruzione in modo da evidenziarne eventuali errori, la soluzione deve essere in grado di far ripartire il playbook dal punto in cui è stato rilevato l'errore.			
	Presenza di funzionalità “training” con procedure automatizzate dove eseguire scenari preconfigurati e dati emulati senza impatto sull'ambiente di produzione.			
	Presenza di funzionalità di prioritizzazione degli incidenti anche in maniera automatica secondo criteri specificati dalla PA.			
	Presenza di funzionalità di intervento manuale all'interno di un workflow automatizzato secondo logiche prefissate dalla PA.			
	~~Presenza di funzionalità di mapping delle tecniche e tattiche di attacco, mettendole in relazione con la tassonomia ACN.~~ Presenza di una funzionalità di mapping delle tecniche e tattiche di attacco, mettendole in relazione con il framework MITRE ATT&CK.			
	Presenza di funzionalità di compliance con le normative e regolamentazioni sulla privacy dei dati, fornendo inoltre la possibilità di gestione sicura dei dati sensibili.			
	Presenza di funzionalità di creazione e personalizzazione di dashboard in base alle esigenze specifiche della Pubblica Amministrazione (PA), tra cui la possibilità di aggiungere, rimuovere e modificare widget e visualizzazioni per adattarsi ai flussi di lavoro e alle priorità dell’organizzazione.			

Tabella 33 - Requisiti migliorativi SOAR

XDR

LOTTO 4 - TABELLA REQUISITI MINIMI XDR BRAND K-ESIMO (DOVE K=1,2,3)				
AMBITO	**REQUISITI MINIMI**	**DOCUMENTO/I COMPROVANTE/I IL REQUISITO**	**PAGINA/E**	**NOTE**
XDR	Supporto ai principali Sistemi Operativi, siano essi Windows-based o Linux-Based.			
	Capacità di utilizzare la rete degli agent installati come sensore per rilevare comportamenti dannosi e correlare tali informazioni su più origini di telemetria con dati storici e in tempo reale.			
	Capacità di analizzare gli eventi correlati per determinare gli incidenti e richiedere l'intervento dell'analista solamente laddove necessario (attività bloccanti, decision making, etc…).			
	Funzionalità di integrazione Nativa con soluzioni di sicurezza dello stesso vendor.			
	Capacità di raccogliere e analizzare dati, in maniera centralizzata, da molteplici fonti, arricchendo le informazioni disponibili sull'XDR e migliorandone le capacità di rilevazione e risposta agli incidenti.			
	Presenza di agent per gestire almeno sistemi Windows e Linux-based.			
	Capacità di assegnazione ruoli e privilegi differenti quali ad esempio Amministratore, Analista, etc con differenti livelli di accesso agli incidenti e alle risorse.			
	Individuazione anomalie e generazione di alert tramite detection rules personalizzabili. Dovrà permettere di inoltrare queste ultime a sistemi di log management tramite protocolli sicuri (quali TLS, etc...).			
	Funzionalità di analisi dei dati storici necessari per la ricostruzione della timeline di un attacco e confrontare lo stato passato "sicuro" con quello attuale dell'endpoint.			
	Funzionalità di distribuzione automatica degli aggiornamenti di tutti gli agent.			
	Il sistema deve essere capace di identificare e rispondere automaticamente agli incidenti di sicurezza meno complessi e che la PA ritenga essere automaticamente risolvibili, riducendo i tempi di risposta e di potenziale danno, ma anche fornire agli analisti tutte le informazioni necessarie per una risoluzione manuale efficace, fornendo la visualizzazione dettagliata degli eventi, strumenti di analisi avanzata e suggerimenti basati sulle best practice.			
	~~Capacità di mapping delle tecniche e tattiche di attacco, mettendole in relazione al MITRE ATT&CK e/o alla tassonomia personalizzabile dalla PA (ACN).~~			

LOTTO 4 - TABELLA REQUISITI MINIMI XDR BRAND K-ESIMO (DOVE K=1,2,3)				
AMBITO	**REQUISITI MINIMI**	**DOCUMENTO/I COMPROVANTE/I IL REQUISITO**	**PAGINA/E**	**NOTE**
	Riduzione all'impatto sulle performance dei sistemi, garantendo un utilizzo ottimale delle risorse a disposizione.			
	Funzionalità di reportistica e logging che consentano: - il monitor in real-time attraverso dashboard; - la realizzazione di report attraverso template predefiniti; - la possibilità di esportare i report.			
	Capacità di assegnare la priorità agli incidenti in base al rischio e all'impatto per concentrare gli analisti su ciò che deve essere affrontato con urgenza.			
	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.			
	Funzionalità di creazione di regole di gestione (anche per singolo endpoint/asset) che la PA vuole tenere sotto controllo.			
	Supporto modalità multi-tenancy.			

Tabella 34 - Requisiti minimi XDR

LOTTO 4 - TABELLA REQUISITI MIGLIORATIVI XDR BRAND K-ESIMO (DOVE K=1,2,3)				
AMBITO	**REQUISITI MIGLIORATIVI**	**DOCUMENTO/I COMPROVANTE/I IL REQUISITO**	**PAGINA/E**	**NOTE**
XDR	Presenza di funzionalità di integrazione con soluzioni di terze parti, anche non previste nativamente, attraverso utilizzo di protocolli standard e/o API documentate.			
	Presenza di funzionalità di identificazione e analisi degli asset coinvolti in un incidente di sicurezza, indipendentemente dalla loro natura, siano essi dispositivi, utenti, dati o interazioni tra applicazioni, processi, servizi in esecuzione con le altre risorse.			
	Presenza di funzionalità di raccolta e analisi dei dati relativi al traffico in rete e tra gli endpoint, mediante tecniche di behavioral analysis, al fine di arricchire le informazioni ottenute tramite gli incidenti.			

LOTTO 4 - TABELLA REQUISITI MIGLIORATIVI XDR BRAND K-ESIMO (DOVE K=1,2,3)				
AMBITO	**REQUISITI MIGLIORATIVI**	**DOCUMENTO/I COMPROVANTE/I IL REQUISITO**	**PAGINA/E**	**NOTE**
	Possibilità di integrazione con soluzioni di raccolta logging native di almeno un cloud service provider, ad es. AWS, GCP, Azure.			
	Presenza di funzionalità di raccolta e analisi, in maniera centralizzata, sia da singole che molteplici fonti, arricchendo le informazioni disponibili sull'XDR e migliorandone le capacità di rilevazione e risposta agli incidenti. Questa telemetria deve permettere di rilevare tempestivamente i comportamenti anomali.			
	Presenza di agent per la gestione di sistemi Mobili, come iOS e sistemi Android-based.			
	Presenza di funzionalità di quarantena di un endpoint, mantenendo attiva la gestione da remoto di tale dispositivo tramite la soluzione stessa, permettendo anche di eseguire comandi a bordo di quest'ultimo.			
	Presenza di funzionalità di rappresentazione di tutta l'architettura di sicurezza e dei dispositivi connessi al XDR all'interno dell'azienda, permettendo di identificare anomalie ed eventuali malfunzionamenti.			
	~~Presenza di funzionalità di mapping delle tecniche e tattiche di attacco, mettendole in relazione con la tassonomia ACN.~~ Capacità di mapping delle tecniche e tattiche di attacco, mettendole in relazione al MITRE ATT&CK e/o alla tassonomia personalizzabile dalla PA (ACN).			
	~~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~~. 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.			
	XDR – Quantità aggiuntive nei formati tecnologici previsti Offerta di quantità migliorative dei formati tecnologici rispetto alle quantità minime previste dal Capitolato Tecnico Speciale – Lotto 4, par. 2.1.1.3. Sarà premiata la disponibilità di ulteriori istanze/soluzioni XDR nei formati tecnologici Appliance Virtuale o Cloud/SaaS, offerte in aggiunta alle quantità minime richieste dal Capitolato Tecnico. La premialità sarà attribuita come segue: - 100% del punteggio assegnato qualora l'Operatore Economico offra 1 quantità migliorativa.			

Tabella 35 - Requisiti migliorativi XDR