AREA	Servizio	ID	Requisiti	Tabellari / Discrezionali	Punteggio MAX
SIEM	SIEM	AS.1.1	Acquisizione dei log/eventi, tramite parser completi già disponibili nella soluzione di specifiche sorgenti richieste dall'Amministrazione non comprese tra quelle minime e migliorative previste in AQ	T	2
SIEM	SIEM	AS.1.2	Integrazione con specifica piattaforma di vulnerability management richiesta dall'Amministrazione	T	2
SIEM	SIEM	AS.1.3	Qualità del feed di threat intelligence. Sarà premiata: - la numerosità e la varietà di fonti, fra cui fonti OSINT, utilizzate dal feed di threat intelligence; - la capacità di arricchimento degli indicatori di compromissione (threat actors, IP addresses, etc.) - l'innovatività e la capacità dei motori di machine learning di correlare le informazioni di sicurezza provenienti da varie fonti, al fine di rendere più rapida l'analisi di tali informazioni e il processo decisionale da parte degli operatori di sicurezza.	D	5
SIEM	SIEM	AS.1.4	Cattura e analisi dei flussi di rete anche in formato Jflow	T	0,5
SIEM	SIEM	AS.1.5	Cattura e analisi dei flussi di rete anche in formato Sflow	T	0,5
SIEM	SIEM	AS.1.6	Efficacia delle analitiche messe a disposizione per la rilevazione di potenziali minacce mediante l'analisi del traffico di rete e del comportamento utente (UBA), al fine di rilevare con accuratezza gli attacchi informatici e ridurre i tempi di indagine e i tempi di risposta associati alle minacce.	D	5
SIEM	SIEM	AS.1.7	Efficacia delle funzionalità che indirizzino e semplifichino la gestione della compliance al GDPR, in termini di: -semplicità e rapidità nella produzione di reportistica adeguata a comprovare lo stato di compliance su dati storici e in real time, provenienti da un'ampia varietà di sistemi IT dell'organizzazione; -semplificazione dell'attività di monitoraggio della compliance in real time; - capacità di individuare i dati associati al GDPR più a rischio.	D	5
SIEM	SIEM	AS.1.8	Configurazione della soluzione in alta affidabilità. Saranno valutate le modalità implementative proposte per la configurazione in alta affidabilità, in termini di disponibilità della soluzione e delle sue componenti in caso di guasto.	D	2
SOAR	SOAR	AS.2.1	Varietà e numerosità delle integrazioni native con sorgenti di eventi di sicurezza (firewalls, endpoint protection, SIEM, threat intelligence, authentication, etc.) sia in fase di apertura dell'incidente informatico, sia per la raccolta di ulteriori informazioni per il triage e l'analisi degli incidenti che per la fase di remediation	D	4
SOAR	SOAR	AS.2.2	ntegrazione con una specifica piattaforma di Service Management richiesta dall'Amministrazione	T	2
SOAR	SOAR	AS.2.3	Qualità del feed di threat intelligence. Sarà premiata: - la numerosità e la varietà di fonti, fra cui fonti OSINT, utilizzate dal feed di threat intelligence; - la capacità di arricchimento degli indicatori di compromissione (threat actors, IP addresses, etc.) - l'innovatività e la capacità dei motori di machine learning di correlare le informazioni di sicurezza provenienti da varie fonti, al fine di rendere più rapida l'analisi di tali informazioni e il processo decisionale da parte degli operatori di sicurezza.	D	5
SOAR	SOAR	AS.2.4	Efficacia, innovatività e semplicità di utilizzo degli strumenti di comunicazione e collaborazione integrati che consentano la condivisione delle informazioni fra gli analisti di sicurezza, al fine di ottimizzare la fase di risposta agli incidenti informatici.	D	2
SOAR	SOAR	AS.2.5	Varietà, semplicità di utilizzo dei playbook messi a disposizione della soluzione e adattabilità al contesto specifico dell'Amministrazione, al fine di semplificare e accelerare il processo di risposta agli incidenti di sicurezza	D	4
SEG	SEG	AS.3.1	Integrazione con soluzioni di sicurezza richieste dalla PA (soluzioni Anti APT, NGFW, SIEM, etc)	T	2
SEG	SEG	AS.3.2	Configurazione della soluzione in alta affidabilità. Saranno valutate le modalità implementative	D	2
SWG	SWG	AS.4.1	Integrazione con soluzioni di sicurezza richieste dalla PA (soluzioni Anti APT, NGFW, SIEM, etc)	D	2
SWG	SWG	AS.4.2	Configurazione della soluzione in alta affidabilità. Saranno valutate le modalità implementative proposte per la configurazione in alta affidabilità, in termini di disponibilità della soluzione e delle sue componenti in caso di guasto.	T	2
DB_Security	DB Security	AS.5.1	Varietà dei DB relazionali supportati (oltre ai minimi previsti in AQ)	D	2
DB_Security	DB Security	AS.5.2	Integrazione con uno specifico sistema HSM richiesto dall'Amministrazione per la generazione e lo storage delle chiavi di crittografia	T	2
DB_Security	DB Security	AS.5.3	Integrazione con una specifica piattaforma di SIEM richiesta dall'Amministrazione	T	2
DB_Security	DB Security	AS.5.4	Varietà dei DB non relazionali supportati	D	2
DB_Security	DB Security	AS.5.5	Efficacia delle funzionalità di transparent encryption su dati non strutturati. Sarà valutata la varietà e numerosità di tipologie di dati non strutturati per la quale viene resa disponibile la funzionalità richiesta	D	2
DB_Security	DB Security	AS.5.6	Modalità per la realizzazione della configurazione in alta affidabilità. Saranno valutate le modalità implementative proposte per la realizzazione della configurazione in alta affidabilità (architettura proposta, HA nativa della soluzione offerta, HA realizzata tramite ambiente di virtualizzazione, ecc.)	D	2
DB_Security	DB Security	AS.5.7	Varietà di ambienti cloud supportati e scalabilità in termini di numero di istanze gestibili	D	2
DLP	DLP	AS.6.1	Possibilità di implementare policy che consentano di prevenire l'invio di dati verso IP appartenenti ad area geografiche considerate rischiose.	T	1
DLP	DLP	AS.6.2	Supporto al *file fingerprinting*	T	1
DLP	DLP	AS.6.3	Integrazione con una piattaforma di MDM specificata dall'Amministrazione	T	2
DLP	DLP	AS.6.4	Capacità della funzionalità DLP Risk Assessment di identificare con accuratezza il livello di rischio associato alla perdita di dati, associato in particolare agli specifici contesti di business dell'Amministrazione	D	2

DLP	DLP	AS.6.5	Capacità della funzionalità di Drip DLP di individuare anche modeste fuoriuscite di quantità di dati che perdurano per archi di tempo brevi o lunghi	D	2
DLP	DLP	AS.6.6	Compatibilità della soluzione CASB con specifiche applicazioni cloud richieste dall'Amministrazione	T	2
DLP	DLP	AS.6.7	Capacità della soluzione CASB di garantire la visibilità e la categorizzazione di applicazioni cloud anche non note (shadow IT) in funzione del loro livello di rischio sulla base di specifici requisiti (ad. es. normativi).	D	2
DLP	DLP	AS.6.8	Capacità della soluzione di supportare, semplificandola, l'attività di classificazione dei dati da parte degli operatori, presente e futura.	D	1
DLP	DLP	AS.6.9	Efficacia delle analitiche messe a disposizione per la rilevazione tempestiva di potenziali minacce che potrebbero implicare la perdita di dati mediante l'analisi del comportamento utente (UBA).	D	5
DLP	DLP	AS.6.10	Funzionalità di Application awareness, ovvero funzionalità che consenta di riconoscere le applicazioni e associare policy specifiche in modo da gestire in maniera selettiva e sicura quali dati possono essere trattati e verso quali periferiche o destinazioni esterne	T	1
DLP	DLP	AS.6.11	Numerosità delle versioni di sistemi operativi e infrastrutture desktop virtuali supportate e completezza della funzionalità offerte, anche con particolare riguardo al supporto di sistemi legacy	D	2
DLP	DLP	AS.6.12	varietà e numerosità degli ulteriori protocolli supportati dalla soluzione DLP volti sia a prevenire efficacemente la fuoriuscita di dati sensibili, personali sia ad incrementare il grado di integrità, riservatezza dei dati, preservando al tempo stesso l'operatività degli utenti	D	2
PAM	PAM	AS.7.1	Supporto di ulteriori specifici sistemi operativi richiesti dall'Amministrazione	T	1
PAM	PAM	AS.7.2	Efficacia delle funzionalità messe a disposizione della soluzione per la gestione dei privilegi di amministratore su macchine Windows e/o UNIX e/o altri sistemi operativi richiesti dall'Amministrazione. Sarà valutata: - il grado di dettaglio delle policy per i privilegi di amministratore e la relativa semplicità d'implementazione; - la capacità della soluzione di garantire un'elevata produttività degli utenti mantenendo al contempo i sistemi sicuri; - la capacità di effettuare un controllo applicativo su un'ampia varietà di applicazioni; - l'integrazione con strumenti di analisi delle minacce informatiche, in modo da identificare, segnalare e bloccare attività privilegiate anomale, anche in funzione del loro grado di criticità	D	5
PAM	PAM	AS.7.3	Efficacia della specifica soluzione per la gestione degli accessi applicativi.Saranno valutate: la proposizione di modalità implementative della soluzione differenti in relazione alla loro adattabilità al contesto specifico dell'Amministrazione (ad es. agent, agentless) e al fine di evitare l'utilizzo di password embedded nel codice; - la varietà numerosità di ambienti applicativi supportati	D	5
PAM	PAM	AS.7.4	Supporto di dispositivi di rete e di dispositivi e sistemi di sicurezza specifici richiesti dall'Amministrazione	T	2
PAM	PAM	AS.7.5	Integrazione con una specifica piattaforma di vulnerability management richiesta dall'Amministrazione	T	2
PAM	PAM	AS.7.6	Integrazione con una specifica soluzione di MFA richiesta dall'Amministrazione	T	2
PAM	PAM	AS.7.7	Possibilità di limitare l'accesso sulla base della localizzazione dell'utente	T	1
PAM	PAM	AS.7.8	Efficacia della specifica soluzione per la protezione di Domain Controller in ambiente Windows. Saranno valutate: - la numerosità delle tecniche di attacco riconosciute; - la varietà delle azioni di mitigazione degli attacchi messe a disposizione dalla soluzione anche al fine di accelerare la fase di remediation da parte degli operatori di sicurezza	D	2
PAM	PAM	AS.7.9	Configurazione della soluzione in alta affidabilità. Saranno valutate le modalità implementative proposte per la configurazione in alta affidabilità, in termini di disponibilità della soluzione e delle sue componenti in caso di guasto.	D	2
PAM	PAM	AS.7.10	Modalità di implementazione dei workflow per la gestione del processo autorizzativo degli accessi per gli account privilegiati. Saranno premiate soluzioni che consentano di implementare meccanismi di controllo degli accessi a più livelli.	D	1
WAF	WAF	AS.8.1	Qualità e Innovatività del sistema di apprendimento automatico basato su Machine Learning del comportamento applicativo, in grado di rilevare le azioni che si discostano dal comportamento applicativo appreso, riducendo i falsi positivi.	D	5
WAF	WAF	AS.8.2	Integrazione con soluzioni di sicurezza richieste dalla PA (soluzioni Anti APT, NGFW, SIEM, etc)	T	3
WAF	WAF	AS.8.3	Configurazione della soluzione in alta affidabilità. Saranno valutate le modalità implementative proposte per la configurazione in alta affidabilità, in termini di disponibilità della soluzione e delle sue componenti in caso di guasto.	D	2
WAF	WAF	AS.8.4	Efficacia delle funzionalità aggiuntive di bilanciamento del carico a livello 7 (modello IS	D	5
WAF	WAF	AS.8.5	Supporto standard PCI DSS	T	2
WAF	WAF	AS.8.6	Modalità di implementazione, varietà e numerosità delle policy/eccezioni alle policy associabili ad applicazioni in essere presso la PA al fine di semplificare la gestione in sicurezza degli applicativi	D	3
Servizi	Organizzazione ed erogazione	AS.9.5	Architettura e modalità di implementazione del collegamento (qualora questo non sia messo a disposizione dalla PA) per l'accesso remoto ai sistemi dell'Amministrazione a supporto delle attività di manutenzione, al fine di garantire l'integrità, la riservatezza e la sicurezza dei dati.	D	2
Servizi	Organizzazione ed erogazione	AS.9.6	Modelli organizzativi, modalità operative e strumenti adottati per l'erogazione dei servizi aggiuntivi ai fini di dimostrare il soddisfacimento dei livelli di servizio offerti dal Concorrente e ottimizzare i tempi di rilascio dei deliverable attesi	D	7
Ulteriori Servizi	Organizzazione ed erogazione	AS.9.1	Ulteriori competenze ed esperienze specifiche del personale addetto ai servizi (ad eccezione del supporto specialistico)	T/D	6

Ulteriori Servizi	Organizzazione ed erogazione	AS.9.2	Certificazioni Vendor Neutrali Aggiuntive del personale addetto ai servizi (ad eccezione del supporto specialistico)	T/D	
Ulteriori Servizi	Organizzazione ed erogazione	AS.9.3	Certificazioni di tipo sales o technical del personale addetto ai servizi sulle tecnologie presenti nel contesto di riferimento della PA o sulle tecnologie proposte in seconda fase (ad eccezione del supporto specialistico)	T/D	
Ulteriori Servizi	Organizzazione ed erogazione	AS.9.4	Misure premiali volte a promuovere l'assunzione di giovani e donne, la parità di genere e le ulteriori misure di conciliazione vita lavoro, indicate in conformità a quanto previsto dall'art. 47, comma 5, Decreto Legge 31 maggio 2021 n. 77.	T/D	
Supporto_Specialistico	Supporto Specialistico	AS.10.1	Security Principal - Certificazioni Vendor Neutrali Aggiuntive: Certificazioni di tipo sales o technical sulle tecnologie presenti nel contesto di riferimento della PA o sulle tecnologie proposte in seconda fase.	T	1
Supporto_Specialistico	Supporto Specialistico	AS.10.2	Senior Security Architect - Certificazioni Vendor Neutrali Aggiuntive: Certificazioni di tipo sales o technical sulle tecnologie presenti nel contesto di riferimento della PA o sulle tecnologie proposte in seconda fase.	T	1
Supporto_Specialistico	Supporto Specialistico	AS.10.3	Senior Security Tester - Certificazioni Vendor Neutrali Aggiuntive: Certificazioni di tipo sales o technical sulle tecnologie presenti nel contesto di riferimento della PA o sulle tecnologie proposte in seconda fase.	T	0,75
Supporto_Specialistico	Supporto Specialistico	AS.10.4	Senior Security Analyst - Certificazioni Vendor Neutrali Aggiuntive: Certificazioni di tipo sales o technical sulle tecnologie presenti nel contesto di riferimento della PA o sulle tecnologie proposte in seconda fase.	T	0,75
Supporto_Specialistico	Supporto Specialistico	AS.10.5	Junior Security Analyst - Certificazioni Vendor Neutrali Aggiuntive: Certificazioni di tipo sales o technical sulle tecnologie presenti nel contesto di riferimento della PA o sulle tecnologie proposte in seconda fase.	T	0,5
SLA	SLA	AS.11.1	Miglioramento dei livelli di servizio richiesti (rispetto ai valori migliorativi previsti in AQ)	D	5