REQUISITI MIGLIORATIVI ACCORDO QUADRO			
AREA	**Servizio**	**ID**	**Requisiti**
SIEM	SIEM	1.1	Acquisizione dei log/eventi, tramite parser completi già disponibili nella soluzione, anche dalle seguenti tipologie di sorgenti: switch e router di ulteriori due Produttori (oltre ai due minimi richiesti) sempre tra i seguenti: Cisco, Juniper, HPE, Huawei, Alcatel-Lucent;
SIEM	SIEM	1.2	Acquisizione dei log/eventi, tramite parser completi già disponibili nella soluzione, anche dalle seguenti tipologie di sorgenti: sistema operativo Mac OS
SIEM	SIEM	1.3	Acquisizione dei log/eventi, tramite parser completi già disponibili nella soluzione, anche dalle seguenti tipologie di sorgenti: piattaforma di virtualizzazione KVM
SIEM	SIEM	1.4	Acquisizione dei log/eventi, tramite parser completi già disponibili nella soluzione, anche dalle seguenti tipologie di sorgenti: piattaforma di virtualizzazione Hyper-V
SIEM	SIEM	1.5	Filtraggio dei log/eventi ricevuti o prelevati dalle sorgenti per evitare che vengano elaborati e memorizzati
SIEM	SIEM	1.6	Possibilità di interrogare la base dati della soluzione tramite API
SIEM	SIEM	1.7	Possibilità di integrare piattaforme di threat intelligence tramite standard STIX/TAXII
SOAR	SOAR	2.1	Automazione di azioni basate su scripts
SOAR	SOAR	2.2	Possibilità di interrogare la base dati della soluzione tramite API
SOAR	SOAR	2.3	Integrabilità con piattaforme e sorgenti di eventi sicurezza tramite API e/o SDK
SEG	SEG	3.1	Cifratura automatica dei messaggi in uscita per i quali risultano verificate delle politiche di identificazione configurabili (policy based encryption)
SEG	SEG	3.2	Identificazione di immagini potenzialmente dannose (almeno contenuti pornografici)
SEG	SEG	3.3	Creazione di regole di spam personalizzate
SEG	SEG	3.4	Identificazione di testo nascosto all'interno di immagini presenti nelle email
SEG	SEG	3.5	Possibilità di interfacciarsi con piattaforme di threat intelligence (almeno MISP)
SEG	SEG	3.6	Possibilità interrogare la base-dati della soluzione tramite API.
SEG	SEG	3.7	Funzionalità di Data Loss Prevention nell'ispezione delle mail in uscita attraverso l'identificazione di parole chiave o pattern di dati.
SEG	SEG	3.8	Rimozione del contenuto attivo dell'email (ad esempio la rimozione di MACRO)
SEG	SEG	3.9	Funzionalità di sandboxing integrata o su cloud del Produttore
SEG	SEG	3.10	Funzionalità di Cousin Domain Detection
SWG	SWG	4.1	Funzionalità di SSL/TLS Inspection a livello hardware su chipset dedicato
SWG	SWG	4.2	Supporto del protocollo WCCP per l'implementazione in modalità trasparente
SWG	SWG	4.3	Funzionalità di file reputation
SWG	SWG	4.4	Identificazione di testo nascosto all'interno di immagini presenti nel traffico web
SWG	SWG	4.5	Funzionalità di DLP nell'ispezione del traffico verso server (HTTP POST): - identificazione di parole chiave o pattern di dati - possibilità di effettuare fingerprinting di file/cartelle
SWG	SWG	4.6	Possibilità interrogare la base-dati della soluzione tramite API.
SWG	SWG	4.7	Possibilità di configurare delle eccezioni relativamente al traffico da non intercettare in modalità SSL inspection
SWG	SWG	4.8	Supporto del protocollo ICAP per l'integrazione con Server ICAP esterni
DB_Security	DB Security	5.1	Possibilità di effettuare un controllo dei privilegi di accesso ai dati per singolo record e per singolo campo di record.
DB_Security	DB Security	5.2	Possibilità di interrogare la base dati della soluzione tramite API
DLP	DLP	6.1	Crittografia dei file basata sulle policy aziendali per la protezione dei dati sensibili archiviati in supporti rimovibili
DLP	DLP	6.2	Rilevazione testo per immagini OCR: possibilità di analizzare il contenuto informativo all'interno di file immagine, quali scansioni di documenti, bloccandone l'eventuale trasmissione (come allegato email, upload web, etc.), sia per email, canali web che per endpoint
DLP	DLP	6.3	Possibilità di interrogare la base dati della soluzione tramite API
PAM	PAM	7.1	Discovery automatico degli account privilegiati
PAM	PAM	7.2	Supporto all'autenticazione di terze parti (ad es. fornitori, consulenti) che accedono da remoto
PAM	PAM	7.3	Supporto dispositivi IoS e Android
PAM	PAM	7.4	Possibilità di utilizzare una password in real-time senza che l'utente conosca mai la password utilizzata
PAM	PAM	7.5	Supporto della connessione ai sistemi target tramite protocollo IPv6
PAM	PAM	7.6	Possibilità di interrogare la base dati della soluzione tramite API
PAM	PAM	7.7	Encryption delle password anche mediante ulteriori protocolli (ad es. RSA)
PAM	PAM	7.8	Possibilità di definire dei workflow per la gestione del processo autorizzativo degli accessi per gli account privilegiati.
PAM	PAM	7.9	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.
WAF	WAF	8.1	Dashboard di monitoraggio in tempo reale con funzionalità drill-down almeno per: Attacchi, Sessioni, dati Geografici di accesso.
WAF	WAF	8.2	Virtual Patching
WAF	WAF	8.3	Ispezione del traffico FTP e FTPS
WAF	WAF	8.4	Funzionalità di Data Loss Prevention
WAF	WAF	8.5	Possibilità di interrogare la base dati della soluzione tramite API
WAF	WAF	8.6	Funzionalità di sandboxing su cloud del Produttore
Trasversali	Organizzazione ed erogazione	9.1	Qualità dei Centri di Competenza nel settore della Sicurezza ICT, in termini di: - varietà e specificità delle competenze del personale impiegato, acquisite sia in ambito nazionale che internazionale; - tipologie, modalità e frequenza degli aggiornamenti formativi; - numerosità e continuità delle collaborazioni con università, enti di ricerca, start up, produttori di tecnologia; - presenza di laboratori presso i quali analizzare o testare le soluzioni tecnologiche da inserire nel proprio portfolio di offerta.
Trasversali	Organizzazione ed erogazione	9.2	Capacità di ottimizzare le attività di aggiornamento (9.2) … anche ai fini di dimostrare il soddisfacimento dei livelli di servizio offerti dal Concorrente descritti nel Capitolato Tecnico in base ai seguenti elementi: - modalità operative e strumenti adottati per una diagnosi proattiva e/o tempestiva di eventuali anomalie software e hardware, che potrebbero compromettere e/o che compromettono la sicurezza dei sistemi dell'Amministrazione; - modalità di rilascio e deployment degli aggiornamenti software, al fine di assicurare la continuità operativa dei sistemi dell'Amministrazione e al contempo la loro sicurezza.
Manutenzione	Organizzazione ed erogazione	9.3	Capacità di ottimizzare … l'erogazione dei servizi di manutenzione (9.3) … anche ai fini di dimostrare il soddisfacimento dei livelli di servizio offerti dal Concorrente descritti nel Capitolato Tecnico in base ai seguenti elementi: - modello organizzativo e strumenti adottati dalle strutture di supporto qualificato e per la logistica, per le attività di ripristino/riparazione dei prodotti software e hardware oggetto della fornitura(es. strutture di coordinamento, di assistenza tecnica hardware e software, magazzini di parti di ricambio, etc.); - modalità e tempistiche di approvvigionamento e gestione delle parti di ricambio.
Hardening_Client	Organizzazione ed erogazione	9.4	Capacità di ottimizzare … hardening su client (9.4) anche ai fini di dimostrare il soddisfacimento dei livelli di servizio offerti dal Concorrente descritti nel Capitolato Tecnico in base ai seguenti elementi: Modalità operative e strumenti adottati per il servizio di hardening su client al fine di semplificare le fasi di progettazione e/o distribuzione degli adeguamenti software sugli elementi di un cluster omogeneo e su più cluster in parallelo, anche ottimizzando i tempi di rilascio dei deliverable.
Supporto_Specialistico	Supporto Specialistico	10.1	Security Principal Percentuale di risorse offerte, nell'ambito di ciascun contratto esecutivo, in possesso della certificazione ISACA CISM (Certified Information Security Manager): almeno il 50% (arrotondato all'unità superiore), coefficiente=1 - inferiore al 50% coefficiente=0

TIM - Uso Interno - Tutti i diritti riservati.

Supporto_Specialistico	Supporto Specialistico	10.2	Senior Security Architect Percentuale di risorse offerte, nell'ambito di ciascun contratto esecutivo, in possesso della certificazione (ISC)^2 CISSP (Certified Information System Security Professional): almeno il 50% (arrotondato all'unità superiore), coefficiente =1 - inferiore al 50% coefficiente=0
Supporto_Specialistico	Supporto Specialistico	10.3	Senior Security Tester Percentuale di risorse offerte, nell'ambito di ciascun contratto esecutivo, in possesso di almeno una delle seguenti certificazioni: EC-Council CEH (Certified Etical Hacker) e/o GIAC Penetration Tester e/o Offensive Security Certified Professional e/o CompTIA Pentest+: almeno il 50% (arrotondato all'unità superiore), coefficiente =1 - inferiore al 50% coefficiente=0
Supporto_Specialistico	Supporto Specialistico	10.4	Senior Security Analyst Percentuale di risorse offerte, nell'ambito di ciascun contratto esecutivo, in possesso di almeno una delle seguenti certificazioni: EC-Council CSA (Certified SOC Analyst) e/o CompTIA CySA+ (Cyber Security Analyst) e/o GIAC Certified Intrusion Analyst: almeno il 50% (arrotondato all'unità superiore), coefficiente =1 - inferiore al 50% coefficiente=0
Supporto_Specialistico	Supporto Specialistico	10.5	Junior Security Analyst: Percentuale di risorse offerte, nell'ambito di ciascun contratto esecutivo, in possesso di almeno una delle seguenti certificazioni: EC-Council CSA (Certified SOC Analyst) e/o CompTIA CySA+ (Cyber Security Analyst) e/o GIAC Certified Intrusion Analyst, e/o ISACA CSX-F (Cyber Security Fundamentals) e/o CompTIA Security+: almeno il 50% (arrotondato all'unità superiore), coefficiente =1 - inferiore al 50% coefficiente=0
Trasversali	SLA	11.1	Tempo di emissione del “Piano Operativo”: 15 giorni lavorativi caratteristica offerta, coefficiente=1 - caratteristica non offerta, coefficiente=0
Trasversali	SLA	11.2	Tempo di consegna, installazione, configurazione e verifica: 50 giorni solari caratteristica offerta, coefficiente=1 - caratteristica non offerta, coefficiente=0
Manutenzione-LP	SLA	11.3	Tempestività del tempo di intervento - Valore minimo richiedibile in AS Profilo LP: 6 ore caratteristica offerta, coefficiente=1 - caratteristica non offerta, coefficiente=0
Manutenzione-HP	SLA	11.4	Tempestività del tempo di intervento - Valore minimo richiedibile in AS Profilo HP: 3 ore caratteristica offerta, coefficiente=1 - caratteristica non offerta, coefficiente=0
Manutenzione-LP	SLA	11.5	Tempestività del tempo di Ripristino - Valore minimo richiedibile in AS Profilo LP - Severity Code 1: 12 ore caratteristica offerta, coefficiente=1 - caratteristica non offerta, coefficiente=0
Manutenzione-LP	SLA	11.6	Tempestività del tempo di Ripristino - Valore minimo richiedibile in AS Profilo LP - Severity Code 2: 16 ore caratteristica offerta, coefficiente=1 - caratteristica non offerta, coefficiente=1
Manutenzione-HP	SLA	11.7	Tempestività del tempo di Ripristino - Valore minimo richiedibile in AS Profilo HP - Severity Code 1: 4 ore caratteristica offerta, coefficiente=1 - caratteristica non offerta, coefficiente=2
Manutenzione-HP	SLA	11.8	Tempestività del tempo di Ripristino - Valore minimo richiedibile in AS Profilo HP - Severity Code 2: 8 ore caratteristica offerta, coefficiente=1 - caratteristica non offerta, coefficiente=3

.TIM - Uso Interno - Tutti i diritti riservati.