Procedura telematica aperta per l'affidamento di un servizio Security Operations Center in modalità "as a service" (SOCaaS) con il criterio dell'offerta economicamente più vantaggiosa sulla base del miglior rapporto qualità/prezzo - CPV 72500000-0 Servizi informatici - CUI S01279680480202600001

RELAZIONE

Responsabile Unico del Progetto

Il sottoscritto Dott. Fabrizio Fioravanti (e-mail: fabrizio.fioravanti@unifi.it), Responsabile del Settore Sistemi, tecnologie cloud e di sicurezza informatica - Area per l'Innovazione e Gestione dei Sistemi Informativi ed Informatici, in qualità di Responsabile Unico del Progetto ai sensi dell'art. 15 del D.lgs. 36/2023, nominato con D.D. Prot. 137405/2026

PREMESSO CHE

L'Università degli Studi di Firenze, in linea con gli obblighi previsti dalla Direttiva NIS 2 (Direttiva UE 2022/2555) e dal contesto normativo italiano in materia di sicurezza delle reti e dei sistemi informativi, intende rafforzare la propria capacità di prevenzione, rilevamento e risposta agli incidenti di sicurezza informatica.

La crescente complessità delle minacce cyber e l'esigenza di garantire la continuità operativa dei servizi digitali dell'Ateneo rendono necessaria l'adozione di un servizio SOC (Security Operations Center) as a Service, ovvero un servizio gestito di monitoraggio, analisi e risposta agli eventi di sicurezza operativo 24 ore su 24, 7 giorni su 7.

La presente Relazione definisce i requisiti minimi obbligatori, i criteri di valutazione e le modalità per l'affidamento del servizio SOCaaS, nell'ottica di individuare la soluzione economicamente più vantaggiosa per l'Ateneo.

DICHIARA

La necessità di acquistare, al fine di supportare le attività sopra elencate, un servizio Security

Operations Center in modalità "as a service" (SOCaaS) che garantisca:

- Progetto di onboarding per le risorse UNIFI da monitorare
- Monitoraggio continuo 24x7 degli eventi di sicurezza provenienti dalle infrastrutture IT di UNIFI;
- Correlazione e analisi degli eventi attraverso l'utilizzo di piattaforme SIEM (Security Information and Event Management) o Incident Management dell'operatore economico che potrà prelevare gli alert e/o i log dal SIEM della stazione appaltante o usare direttamente il SIEM della stazione appaltante per il monitoraggio e gestione degli incidenti;
- Rilevamento tempestivo delle minacce e degli incidenti di sicurezza (incident detection);
- Classificazione e gestione degli incidenti (incident triage e incident response);
- Notifica tempestiva ai referenti indicati da UNIFI degli eventi rilevanti;
- Eventuale attivazione di contromisure concordate tramite apposita procedura da definire e rivedere durante il periodo contrattuale atta a contrastare nell'immediato incidenti particolarmente critici;
- Supporto nell'analisi approfondita degli incidenti con suggerimenti per la remediation;
- Reportistica periodica sullo stato di sicurezza e sugli incidenti gestiti.

Il servizio dovrà integrarsi con l'infrastruttura Google SecOps indicata dalla stazione appaltante, garantendo la raccolta e l'analisi dei log provenienti dalle diverse fonti tecnologiche presenti nell'Ateneo.
A valle dell' onboarding a servizio attivo, le regole di correlazione aggiunte durante l'erogazione del servizio per minimizzare i falsi positivi, limitare gli errori di detection o intercettare nuove minacce dovranno essere inserite o replicate sull'infrastruttura SIEM della stazione appaltante nei limiti dichiarati nella proposta tecnica.
Tutte le regole di correlazione create sul SIEM della stazione appaltante rimarranno in uso alla stazione appaltante anche al termine del contratto.

Nello specifico i requisiti minimi sono:

1. Progetto di onboarding portato a termine nel limite massimo di 3 mesi con l'integrazione di almeno 100 fonti on-premise o di tutte le fonti se inferiori a 100, Google Workspace for education, piattaforma Veeam e piattaforma EDR Bitdefender in cloud

2. Piattaforma SOAR (Security Orchestration, Automation and Response) o di incident management

   Se l'operatore economico non utilizzerà la piattaforma SOAR della stazione appaltante per l'erogazione del servizio, dovrà specificare:

- Quale piattaforma SOAR o di incident management è utilizzata per erogare il servizio e con quali modalità di utilizzo (gestione diretta da parte del fornitore, accesso in lettura/scrittura per UNIFI, accesso in sola lettura per UNIFI);
- Le funzionalità di automazione e orchestrazione disponibili per la risposta agli incidenti.

3. Operatività 24x7

   Il servizio SOC dovrà essere operativo 24 ore su 24, 7 giorni su 7, garantendo la presenza continuativa di security analyst qualificati per il monitoraggio, l'analisi e la risposta agli incidenti di sicurezza.

4. Rispondenza alla norma ISO 27001

   Si richiede inoltre la dichiarazione di conformità al GDPR ed alle misure previste al momento della gara dal recepimento italiano della NIS2.

   Il numero minimo di security analyst (figure specializzate nel monitoraggio, individuazione e mitigazione di incidenti cyber) dedicati al servizio SOC non dovrà essere inferiore a 5.

   La piattaforma SIEM/SOAR utilizzata dall'operatore economico per erogare il servizio dovrà avere i dati collocati in datacenter che rientrino fra quelli permessi dal GDPR.

5. SLA e performance operative

   Si richiedono i seguenti livello di servizio minimi attesi in relazione alla individuazione, classificazione, triage e notifica:

   - TTD (Time to Detect): presa in carico dell'incidente entro 2 ore
   - TTT (Time to Triage): classificazione (critico, alto, medio, basso) dell'incidente entro 4 ore
   - TTN (Time to Notify): notifica dell'incidente entro 8 ore per incidenti critici, 16 ore per incidenti medio/alti e 24 ore per incidenti classificati come bassa priorità nel caso in cui tali incidenti siano stati indicati come da segnalare.

6. Servizi analoghi

Si richiede come requisito economico di fatturato che l'esecuzione, nei dieci anni precedenti la data di indizione della procedura, di servizi analoghi al servizio Security Operations Center in modalità "as a service" (SOCaaS) abbia avuto un importo complessivo almeno pari a € 600.000,00 oltre IVA;

L'importo a base d'asta è pari a euro 600.000,00 oltre IVA.
La durata dell'appalto è di 4 anni decorrenti dalla data di sottoscrizione del contratto, con possibilità di rinnovo per ulteriori 4 anni
Per i primi dodici mesi, il contratto si intende conferito a titolo di prova, per consentire una valutazione ampia e complessiva del rapporto, in relazione a quanto indicato in offerta dal contraente.

L'importo degli oneri per la sicurezza da interferenze è pari a € 0,00 poiché considerate le caratteristiche del servizio, non si rilevano interferenze per le quali intraprendere misure di prevenzione e protezione finalizzate a eliminare o ridurre eventuali rischi, nello specifico il servizio consiste essenzialmente nell'offrire un servizio di analisi dei dati di log finalizzato a fornire allerte circa potenziali problemi di sicurezza informatica
Si considera il servizio in oggetto di natura prevalentemente intellettuale poiché non sono previste attività manuali di nessun genere, né interventi su apparati della Stazione Appaltante o body rental di nessun tipo. Non rientrando quindi nel novero delle attività manutentive standard ma di attività comunque consulenziali, non sono stati stimati i costi della manodopera.
La copertura finanziaria della spesa graverà sui fondi dell'Area per l'Innovazione e gestione dei sistemi informativi ed informatici.
La copertura finanziaria prevista per il contributo di gara previsto dalla legge in favore dell'Autorità Nazionale Anticorruzione, da parte della Stazione Appaltante, pari ad € 410,00 è assicurata dai fondi dell'Area per l'Innovazione e gestione dei sistemi informativi ed informatici.

L'affidamento avverrà mediante procedura aperta e con applicazione del criterio dell'offerta economicamente più vantaggiosa individuata sulla base del miglior rapporto qualità prezzo, ai sensi dell'art. 108 D.Lgs 36/2023.
Le caratteristiche tecniche minime, devono essere necessariamente possedute, a pena di esclusione dalla gara.
Le caratteristiche tecniche migliorative sono valutate, se offerte, in sede di attribuzione del

punteggio tecnico, secondo i criteri definiti nel Disciplinare di gara.

Il RUP attesta che il servizio in oggetto non è presente all'interno delle convenzioni CONSIP vigenti.

Ai sensi dell'articolo 108, comma 4 del Codice, verranno valorizzati gli elementi qualitativi dell'offerta e individuati criteri tali da garantire un confronto concorrenziale effettivo sui profili tecnici. A tal fine si stabilisce un tetto massimo per il punteggio economico entro il limite del 25% per cento del punteggio complessivo.

La valutazione dell'offerta tecnica e dell'offerta economica è effettuata in base ai seguenti punteggi:

	Punteggio
Offerta economica	25
Offerta tecnica	75
Totale	**100**

CRITERI DI VALUTAZIONE DELL'OFFERTA TECNICA

Il punteggio dell'offerta tecnica è attribuito sulla base dei criteri di valutazione elencati nella sottostante tabella con la relativa ripartizione dei punteggi.

Nella colonna identificata con la lettera D vengono indicati i "Punteggi discrezionali", vale a dire i punteggi il cui coefficiente è attribuito in ragione dell'esercizio della discrezionalità spettante alla commissione giudicatrice.

Nella colonna identificata dalla lettera T vengono indicati i "Punteggi tabellari", vale a dire i punteggi fissi e predefiniti che saranno attribuiti o non attribuiti in ragione dell'offerta o mancata offerta di quanto specificamente richiesto.

Tabella dei criteri discrezionali (D) e tabellari (T) di valutazione dell'offerta tecnica

N°	CRITERI DI VALUTAZIONE	PUNTI MAX		SUB-CRITERI DI VALUTAZIONE	PUNTI D MAX	PUNTI T MAX
			1.1	Completezza delle fonti dati gestite dall'operatore economico sulla base di quelle presenti nell'infrastruttura UNIFI	3	0

1	PROGETTO DI ONBOARDING	15	1.2	*Architettura del sistema di monitoraggio con descrizione di come la piattaforma SIEM/SOAR di UNIFI sarà integrata durante il progetto*	4	0
			1.3	*Architettura del BindPlane e suo deploy all'interno del progetto di onboarding e modalità di configurazione delle fonti che dovranno trasferire i log alla piattaforma SIEM*	4	0
			1.4	Modalità di implementazione delle regole di correlazione su Google Sec Ops e piano di implementazione delle regole per la riduzione dei falsi positivi	4	0

Criteri motivazionali n. 1:

1.1 Il punteggio sarà attribuito sulla base delle fonti dichiarate come integrabili e che ricadano nella seguente lista di potenziali fonti da integrare

1. Sistemi di Identity & Access Management (IAM) come Active directory, LDAP, sistemi IAM come CAS e Syncope.
2. EDR: Endpoint con console in cloud BitDefender (workstation, server), anche limitatamente ai soli incidenti
3. Apparati di rete (firewall in particolare Fortinet e Cisco, switch in particolare Cisco, router e log server a servizio di essi come syslog server e Fortianalyzer)
4. Servizi cloud (Microsoft 365, Google Workspace)
5. Sistemi application server come Tomcat e stack LAMP
6. Sistemi di virtualizzazione (VMWARE)
7. Database (Oracle, Postgresql e MariaDB/Mysql)
8. Veeam Data Platform (Backup & Replication, VeeamOne, Recon Scanner e Orchestrator)
9. Server Linux anche se non gestiti da EDR
10. Server Windows anche se non gestiti da EDR

1.2 Valutazione della solidità architetturale della soluzione proposta e dell'integrazione della piattaforma SIEM/SOAR di UNIFI all'interno del progetto

1.3 Architettura bindplane ed acquisizione delle fonti di log

a. Valutazione della solidità architetturale e della versatilità della soluzione proposta, valutando sulla base del progetto presentato la semplicità di futura integrazione di nuove fonti e la fattibilità nei tempi indicati dell'onboarding delle fonti minime richieste
b. Valutazione del gantt del progetto di onboarding includendo i tempi massimi di onboarding per il raggiungimento della piena operatività del servizio con un limite massimo di 3 mesi con l'integrazione di 100 fonti on-premise, Google Workspace for education, piattaforma Veeam e piattaforma EDR Bitdefender in cloud
c. Piano di test e verifica della corretta ricezione e correlazione dei log

1.4 Modalità di implementazione delle regole di correlazione su Google Sec Ops e piano di implementazione delle regole per la riduzione dei falsi positivi

- Implementazione delle regole di correlazione su GoogleSecOps e loro modalità di manutenzione ed integrazione durante l'intero periodo del servizio
- Modalità di tuning delle regole di correlazione per l'intera durata del servizio per la minimizzazione dei falsi positivi

2	Struttura e capacità del SOC	18	2.1	*Certificazioni del SOC*	0	4
			2.2	Maturità del SOC	0	3
			2.3	Numero di clienti attivi nel SOC	0	3
			2.4	Numero di pubbliche amministrazioni clienti del SOC	0	3
			2.5	Numero di Atenei italiani clienti del SOC	0	4
			2.6	Tempo massimo di onboarding	0	1

Criterio adottato n 2: Questa macro-area valuta la solidità organizzativa e l'esperienza del fornitore nella gestione di servizi SOC con particolare riferimento all'erogazione di tali servizi nel contesto della pubblica amministrazione Italiana.

2.1 Punteggio attribuito per ogni certificazione posseduta tra le seguenti:

- ISO/IEC 27017 (Sicurezza del cloud computing) per il servizio SOC;
- ISO/IEC 27018 (Protezione dei dati personali nel cloud) per il servizio SOC;
- ISO 22301 (Business Continuity Management System) per il servizio SOC;
- ISO 20000 (Service Management System) per il servizio SOC;
- almeno 1 Professional Security Operations Engineer (PSOE);

Modalità di attribuzione: +1 punto per ogni certificazione posseduta, fino a un massimo di 4 punti.

2.2 Punteggio basato sugli anni di attività operativa del SOC:

- < 3 anni: 0 punti
- 3-5 anni: 1 punto
- 6-10 anni: 2 punti
- > 10 anni: 3 punti

2.3 Punteggio in base al numero totale di organizzazioni servite:

- 2 - 50 clienti: 0 punti
- 51-150 clienti: 1 punto
- 151-300 clienti: 2 punti
- > 300 clienti: 3 punti

2.4 Punteggio in base al numero di PA italiane servite dal servizio SOC:

- 0-2 PA: 0 punti
- 3-5 PA: 1 punto
- 5-10 PA: 2 punti
- > 10 PA: 3 punti

2.5 Punteggio bonus se il fornitore serve già almeno un Ateneo italiano:

- 0 Atenei: 0 punti
- per ogni 1 Ateneo: 1 punto (max 4 punti)

2.6 Punteggio in base ai tempi dichiarati per il raggiungimento della piena operatività:

- <=2 mesi: 1 punto

La piena operatività deve includere la configurazione completa di sistemi di rilevamento, correlazione e reportistica, verificabile tramite checklist e log di attivazione.

3	Copertura e integrazione tecnica	22	3.1	Integrazione con sistemi UNIFI	0	4
			3.2	Numero di regole di correlazione o playbook al mese su SIEM/SOAR dopo l'onboarding implementate sul sistema UNIFI	0	4
			3.3	Framework e metodologie di riferimento	0	6
			3.4	Incident Response Team	0	6
			3.5	Conservazione dei dati degli incidenti	0	2

Criterio adottato n. 3: Questa macro-area valuta la capacità del fornitore di integrarsi con l'infrastruttura esistente di UNIFI e la completezza della copertura tecnologica oltre alla validazione della presenza di una struttura in grado di rispondere agli incidenti.

3.1 Punteggio attribuito in base alla capacità dichiarata di integrazione con le seguenti categorie di sistemi:

- Nessuna fonte integrativa rispetto a quelle minime previste : 0 punti
- 50 fonti oltre a quelle minime previste : 1 punto
- 100 fonti oltre a quelle minime previste: 2 punti
- Fonti illimitate: 4 punti

3.2 Punteggio attribuito in base al numero di regole di correlazione o playbook SIEM/SOAR dopo l'onboarding incluse nell'offerta:

- nessuna: 0 punti
- fino a 10: 1 punto
- fino a 20: 2 punti
- nessun limite 4: punti

3.3 Punteggio per l'adozione di framework e/o norme riconosciuti a livello internazionale nella classificazione degli incidenti:

- MITRE ATT&CK: 2 punti
- NIST Cybersecurity Framework: 2 punti

- CIS Critical Security Controls 8.1 o superiore: 2 punti

3.4 Punteggio attribuito in base al numero di giornate uomo dell'Incident Response Team dell'operatore economico per anno di servizio incluse nell'offerta economica:

- nessuna: 0 punti
- fino a 3: 1 punto
- da 4 a 6: 2 punti
- da 7 a 9: 3 punti
- 10 a 14: 5 punti
- 15 o superiore: 6 punti

3.5 Punteggio attribuito in base alla conservazione dei dati degli incidenti rilevati comprensivi di timeline ed operazioni effettuate dai singoli operatori del SOC

- almeno 6 mesi: 0 punti
- almeno 9 mesi: 1 punto
- almeno 12 mesi: 2 punti

4	Qualità della reportistica e collaborazione		4.1	Frequenza e completezza della reportistica	0	6
			4.2	Gestione e tracciabilità degli incidenti	0	3
			4.3	Servizi di formazione e awareness	0	5
			4.4	Esercitazioni periodiche di simulazione incidenti	0	4

Criterio adottato n. 4: Questa macro-area valuta la capacità del fornitore di comunicare efficacemente con UNIFI e di supportare l'Ateneo nel miglioramento continuo della postura di sicurezza

4.1 Punteggio attribuito in base alla frequenza dei report periodici sullo stato di sicurezza:

- Nessuna reportistica o reportistica superiore a 3 mesi: 0 punti
- Report trimestrale: 1 punto
- Report mensile: 2 punti
- Report settimanale: 4 punti
- Disponibilità di dashboard in tempo reale: +1 punto aggiuntivo
- Reportistica avanzata con analisi di remediation: + 1 punto aggiuntivo

Punteggio massimo: 6 punti (report settimanale + dashboard in tempo reale + reportistica avanzata). 4.2 Punteggio attribuito in base alla disponibilità di sistemi di ticketing integrati e tracciabilità completa: ● Sistema di ticketing dedicato: 1 punto ● Per ogni incidente disponibilità della timeline di azione, delle azioni e valutazioni effettuate e degli esiti della segnalazione alla stazione appaltante: 2 punti 4.3 Punteggio attribuito per l'inclusione di attività formative nell'offerta del servizio: ● Formazione iniziale per il personale UNIFI: 1 punto ● Per ogni sessione annuale di aggiornamento e awareness: 1 punto (max 4 punti) 4.4 Punteggio attribuito per la disponibilità di esercitazioni incluse nell'offerta (tabletop exercise, red team/blue team): ● Nessuna esercitazione prevista: 0 punti ● Per ogni esercitazione all'anno: 1 punto (max 4 punti)						
5	Conformità e sicurezza dei dati		5.1	Data residency e sovranità dei dati	0	2
Criterio adottato n. 5: Questa macro-area valuta la conformità del fornitore alle normative vigenti e la sicurezza nella gestione dei dati sensibili di UNIFI. 5.1 Punteggio attribuito in base alla localizzazione dei datacenter e dei dati della piattaforma di incident management dell'operatore economico utilizzata per il servizio: ● Datacenter localizzati nell'Unione Europea: 1 punto ● Datacenter localizzati in Italia: 2 punti						

Il concorrente è escluso dalla gara nel caso in cui consegua un punteggio inferiore alla soglia minima di sbarramento pari a 35 per il punteggio tecnico complessivo (75 punti)

OFFERTA ECONOMICA

L'offerta economica dovrà indicare il ribasso percentuale offerto sui seguenti importi:

1. Onboarding - base d'asta: € 40.000 - 2 punti
2. canone annuale del servizio base d'asta € 70.000/ anno - 23 punti

Per tutto quanto sopra esposto il sottoscritto trasmette la presente relazione e il quadro economico per effettuare la gara d'appalto al Settore Gare e appalti per quanto di loro competenza e per l'espletamento della procedura.

Responsabile Unico del Progetto

Firmato digitalmente da FABRIZIO FIORAVANTI
Data: 30/06/2026 14:22:14 CEST

Allegati:

1. Quadro economico