All. 1

SCHEDA PROGETTO

Responsabile del progetto e dell'esecuzione del contratto:
Prof. Alessandro Armando (Professore ordinario – Settore Scientifico Disciplinare - IINF-05/A – Sistemi di elaborazione delle informazioni)

Obiettivo del progetto:
Il progetto ARTIC (Spoke 4 del progetto PNRR SERICS) mira ad affrontare le sfide operative e di ricerca legate all'utilizzo di Cyber Range come banco di prova per la sperimentazione di attacchi di cybersecurity e il supporto alle attività formative del personale preposto alla gestione delle infrastrutture ICT. Nel contesto dell'aumento della frequenza e della gravità degli incidenti informatici che colpiscono infrastrutture pubbliche e private, emerge la necessità di rafforzare le capacità di risposta attraverso adeguati percorsi di formazione. In particolare, è fondamentale disporre di materiali didattici aggiornati e coerenti con le più recenti normative e buone pratiche internazionali, in grado di supportare efficacemente l'acquisizione e la valutazione delle competenze nella gestione degli incidenti informatici.

Oggetto della prestazione:
Attività di consulenza: "Sviluppo di Materiale Didattico a supporto di Attività di Formazione e Valutazione delle Competenze sulla Gestione degli Incidenti Informatici" a vantaggio delle attività dello Spoke 4, del Programma di Ricerca "SEcurity and RIghts in the CyberSpace", acronimo "SERICS", contraddistinto dal codice identificativo PE00000014 - finanziato nell'ambito del Piano Nazionale di Ripresa e Resilienza, Missione 4, "Istruzione e Ricerca" - Componente 2, "Dalla ricerca all'impresa" - Linea di investimento Investimento 1.3 "Creazione di Partenariati Estesi alle università, centri di ricerca, alle aziende per il finanziamento di progetti di ricerca di base", finanziato dall'Unione europea – NextGenerationEU, CUP - D33C22001300002.

Descrizione dettagliata della prestazione:
L'incarico ha per oggetto la progettazione e la realizzazione di materiale didattico a supporto di iniziative formative nell'ambito della gestione degli incidenti informatici. In particolare, il prestatore dovrà:
● sviluppare contenuti formativi (quali presentazioni, esercitazioni pratiche, casi di studio, simulazioni, test ed esercizi di valutazione, ecc.) volti a illustrare le principali fasi del processo di gestione degli incidenti: identificazione, analisi, contenimento, risposta, recupero e reporting;
● contribuire alla definizione di strumenti e metodologie per la valutazione delle competenze acquisite dai partecipanti;
● garantire l'aderenza dei materiali agli standard nazionali e internazionali in materia di sicurezza informatica e incident response.
Il materiale prodotto dovrà essere strutturato in modo da risultare idoneo sia per l'erogazione in presenza che in modalità online, e potrà essere utilizzato in contesti formativi rivolti a studenti, professionisti o personale tecnico operante nel settore della cybersecurity.
Il materiale didattico che dovrà essere prodotto dal prestatore deve essere composto da:
1. Specifica dei prerequisiti (competenze in ingresso), min 1500 - max 3000 caratteri
2. Specifica degli obiettivi formativi (learning outcome), min 1500 - max 3000 caratteri
3. Syllabus dettagliato (**basato su quello indicato a seguire,** eventualmente raffinato)
4. Slides (min 800, max 1200) in formato pptx (ma ben visualizzabili anche in GDrive) corredata da script per video lezione incluso ciascuna slide nella sezione "speaker notes"
5. Un'esercitazione pratica, un caso di studio o una simulazione per ciascuna sezione del syllabus
6. 8 esercizi svolti per ciascuna sezione del syllabus
7. 1 test di autovalutazione per ciascuna sezione del syllabus Il materiale di cui ai punti 1, 2 e 3 dovranno essere consegnati entro 15 giorni dall'inizio delle attività. Una prima versione del materiale di cui al punto 4 e 4 degli esercizi di cui al punto 5 dovranno essere consegnati entro 45 giorni dall'inizio dell'attività.

Syllabus Incident Response

INTRODUZIONE

- Differenza tra evento e incidente con focus sugli obiettivi principali dell'Incident Response
- Panoramica sulle fasi dell'Incident Response (Preparation, Detection and Analysis, Containment/Eradication/Recovery, Post-Incident Activity)
- NIST SP 800-61 Rev. 2: struttura e contenuti principali
- NIST SP 800-86: approccio forense nell'IR
- NIS 2: identificazione degli incidenti ed impatti sui servizi erogati
- Confronto con altri standard/framework (ISO/IEC 27035, SANS, MITRE ATT&CK)
- Linee guida ISO/IEC per l'integrazione fra IR e le pratiche di analisi forense: integrazione di ISO/IEC 27035 con ISO/IEC 27037, ISO/IEC 27041, ISO/IEC 27042 e ISO/IEC 27043

PREPARAZIONE

- Ruoli e responsabilità (CIRT/CSIRT, SOC, IT, management)
- Policy e procedure per l'incident response
- Costruzione del team di risposta agli incidenti
- Inventory, logging, correlation e monitoraggio proattivo
- Training e simulazioni (tabletop exercises, Red/Blue team)
- Comunicazioni interne ed esterne (inclusi aspetti legali e pubbliche relazioni)

INDIVIDUAZIONE ED ANALISI

- Tecniche e fonti di rilevamento (IDS, SIEM, EDR, log analytics)
- Analisi degli indicatori di compromissione (IoC)
- Prioritizzazione e classificazione degli incidenti
- Uso del MITRE ATT&CK per la mappatura delle tattiche/tecniche

CONTENIMENTO, ERADICAZIONE E RIPRISTINO

- Strategie di contenimento a breve/lungo termine
- Integrazione delle tecniche forensi (da NIST 800-86): acquisizione dati volatili, immagini disco, memoria
- Analisi delle cause e strumenti/modalità di eradicazione
- Pianificazione del ripristino (tempi, sistemi prioritari, sicurezza post-ripristino, monitoraggio)
- Comunicazioni con le parti interessate (enti regolatori, autorità, clienti, fornitori)

ATTIVITÀ POST-INCIDENTE

- Lessons Learned: raccolta e analisi informazioni post-mortem
- Reportistica tecnica e gestionale
- Aggiornamento di policy e controlli
- Misurazione dell'efficacia della risposta (KPI, metriche)
- Miglioramento nell'automazione nella risposta agli incidenti (policy, procedure e tecniche)

Competenze richieste al prestatore:

- Possesso di almeno uno dei seguenti titoli di studio: Diploma di Laurea quinquennale in Ingegneria delle Telecomunicazioni, Ingegneria Elettronica, Ingegneria Informatica, Ingegneria dell'Automazione, Informatica, Sicurezza Informatica, Matematica, Fisica, Ingegneria Gestionale, conseguito ai sensi della normativa previgente al D.M. 3 Novembre 1999, n. 509, ovvero Laurea Specialistica in una delle seguenti classi: 30/S, 32/S, 35/S, 29/S, 23/S, 45/S, 20/S, 34/S, ovvero Laurea Magistrale in una delle seguenti classi: LM-27, LM-29, LM-32, LM-25, LM-18, LM-66, LM-40, LM-17, LM-31;
- Esperienza, anche in ambito accademico, in istituzioni o enti, pubblici o privati, anche a supporto di studi e ricerche nel settore di riferimento di almeno 2 anni;
- Competenze e conoscenze documentabili attraverso il curriculum ed acquisite tramite corsi, attività di ricerca o esperienze lavorative, in particolare, nei seguenti ambiti:
  - Esperienza delle best practice e standard internazionali per la gestione della risposta agli incidenti informatici;
  - Esperienza di progettazione e attuazione di piani per la gestione degli incidenti informatici;

Durata del progetto: La prestazione deve essere conclusa **entro 3 mesi**
Compenso: Compenso lordo per l'intero periodo contrattuale: euro 48.000,00 + IVA (se dovuta) e comprensivo di oneri previdenziali ed assistenziali a carico del prestatore, se dovuti; Modalità di pagamento/frazionamento: euro 15.000,00 dopo 1 mese, previa verifica dello stato di avanzamento, e la seconda pari a euro 33.000,00, a saldo al termine del contratto.
Natura Fiscale della prestazione: Prestazione unica ad esecuzione pressoché istantanea: • lavoro autonomo – redditi diversi (art. 67, comma 1, lett. I, D.P.R. 917/86 TUIR); • lavoro autonomo – redditi di lavoro autonomo- professionisti abituali (art. 53, comma 1, D.P.R. 917/86 TUIR);

Il Responsabile del progetto e dell'esecuzione del contratto

(prof. Alessandro Armando)

(Documento firmato digitalmente)

ALESSANDRO
ARMANDO
UNIVERSITÀ
DEGLI
STUDI DI
GENOVA
23.07.2025
11:17:12
UTC