Gli studenti devono rispondere a 1 dei 2 casi presentati. Di seguito sono riportate le indicazioni relative alla lunghezza del saggio e ai
requisiti di formattazione. Gli studenti possono utilizzare qualsiasi risorsa fornita in classe o trovata online. Le risorse online devono essere basate su prove provenienti da fonti sottoposte a revisione paritaria.

Insieme all'esame dovrà essere consegnata anche una presentazione di 10 minuti sul processo di ricerca delle informazioni rilevanti per il saggio. La presentazione non è un riassunto del saggio, ma una riflessione su come sono state trovate le informazioni rilevanti e su come si è deciso di utilizzarle. La presentazione può essere realizzata in qualsiasi formato (ad esempio PowerPoint), ma deve essere consegnata come file video (.mp4).

Caso 1: Progettazione di uno strumento di visualizzazione incentrato sull'uomo per la consapevolezza della situazione informatica

I centri operativi di sicurezza (SOC) sono responsabili del monitoraggio, dell'analisi e della risposta alle minacce alla sicurezza informatica in tempo reale. Tuttavia, gli analisti SOC si trovano spesso a dover gestire quantità enormi di dati, con conseguente sovraccarico cognitivo, affaticamento decisionale e ritardi nella risposta alle minacce critiche. La complessità dei dashboard di sicurezza informatica, gli allarmi eccessivi e la scarsa gerarchia delle informazioni possono rendere difficile per gli analisti identificare in modo efficiente le minacce reali. Queste sfide sono aggravate da fattori umani e psicologici.

Il vostro compito è quello di sviluppare una base empirica per un futuro strumento di visualizzazione incentrato sull'uomo che migliori il riconoscimento delle minacce informatiche da parte degli analisti SOC. Lo strumento incorporerebbe i principi dell'ergonomia cognitiva e delle scienze comportamentali per migliorare la consapevolezza situazionale. Considerate il fattore umano e gli elementi psicologici e discutete come le interfacce interattive possono supportare il processo decisionale.

Endsley, M. R., & Jones, D. G. (2024). Progettazione orientata alla consapevolezza della situazione: revisione e direzioni future. *International Journal of Human–Computer Interaction*, *40*(7), 1487-1504.

Caso 2:

Compito d'esame: Migliorare la comunicazione nella risposta agli incidenti di sicurezza informatica

Una multinazionale ha recentemente subito un attacco mirato di ingegneria sociale che ha sfruttato la debole comunicazione tra il suo team di sicurezza informatica, l'alta dirigenza e i dipendenti in generale. Sebbene il team di sicurezza IT abbia rilevato l'attacco in anticipo, i suoi avvertimenti non sono stati trasmessi in modo efficace ai responsabili delle decisioni, con il risultato di una risposta lenta e frammentaria. L'errata interpretazione dei dettagli tecnici, la mancanza di strutture di reporting chiare e i silos organizzativi hanno ritardato gli sforzi di mitigazione, aumentando l'impatto complessivo dell'attacco. Questo incidente evidenzia la sfida più ampia della comunicazione intersettoriale nella sicurezza informatica, dove esperti tecnici, dirigenti e personale non tecnico devono lavorare insieme per gestire e prevenire le minacce. Tuttavia, le differenze in termini di competenze, percezione del rischio e stili di comunicazione spesso portano a interruzioni che indeboliscono la posizione di sicurezza di un'organizzazione.

Il tuo compito è analizzare i rischi legati al fattore umano che contribuiscono ai fallimenti nella sicurezza informatica e proporre strategie per mitigarli. Proponi soluzioni basate su dati concreti che garantiscano una risposta adeguata in materia di sicurezza informatica a tutti i livelli di un'organizzazione. La tua risposta dovrebbe tenere conto delle ricerche sui fattori umani nella sicurezza, nella comunicazione di crisi e nelle scienze comportamentali a sostegno delle tue raccomandazioni per migliorare la resilienza della sicurezza informatica.

Pollini, A., Callari, T. C., Tedeschi, A., Ruscio, D., Save, L., Chiarugi, F. e Guerri, D. (2022). Sfruttare i fattori umani nella sicurezza informatica: un approccio metodologico integrato. *Cognition, Technology & Work*, *24*(2), 371-390.

Formattazione del saggio

Il saggio può contenere **3000 ± 10% parole** nel corpo principale (abstract e riferimenti non contano) in carattere Times New Roman 12. Il saggio deve essere digitato e scritto a doppia spaziatura su carta di formato standard (A4) con margini di 1" (standard in Word Document) su tutti i lati. Includere un'intestazione di pagina
intestazione (nota anche come "intestazione corrente") nella parte superiore di ogni pagina. L'intestazione corrente è un
versione abbreviata del titolo del tuo elaborato e non può superare i 50 caratteri, spazi e punteggiatura inclusi. Il mancato rispetto di questo requisito può comportare un voto inferiore. Il conteggio delle parole non
le immagini prive di testo. Le tabelle saranno conteggiate nel conteggio finale delle parole. Se nelle tabelle sono utilizzate immagini, queste saranno conteggiate come 500 parole. Il saggio dovrà avere una pagina del titolo con il titolo e il conteggio delle parole, un abstract, un corpo principale e dei riferimenti. Questo saggio è un testo accademico.

Per ulteriori informazioni, consultare https://taltech.ee/en/formatting-guidelines

Per questo saggio, deve essere utilizzato lo stile APA 7th (vedere: https://apastyle.apa.org/style-grammar-guidelines/references/examples)

Altre risorse per l'APA 7th (io personalmente uso questa):
https://owl.purdue.edu/owl/research_and_citation/apa_style/apa_style_introduction.htm l

Valutazione

Vedere https://taltech.ee/en/grading-system per la politica di valutazione di Taltech

§ 14. Valutazione del rendimento accademico
(1) I metodi e i criteri di valutazione definiti nel programma devono essere comunicati agli studenti prima dell'inizio degli studi e non devono essere modificati durante il semestre. I metodi di valutazione definiscono le modalità di attestazione dell'acquisizione di conoscenze e competenze (ad esempio, esame orale o scritto, valutazione di idoneità/non idoneità, saggio, relazione, lavoro di gruppo, questionario). Se per la valutazione dei risultati dell'apprendimento vengono utilizzati diversi metodi, la loro peso relativo nella determinazione del voto finale deve essere specificato nel programma. Un criterio di valutazione deve specificare il livello e l'ambito di conoscenza attesi che possono essere dimostrati dai metodi di valutazione.

(3) **In caso di valutazione graduata, il raggiungimento dei risultati di apprendimento è valutato in base alla seguente scala**:
A (5) – "eccellente" – raggiungimento eccezionale e particolarmente approfondito dei risultati di apprendimento, insieme a creatività e competenza consumata nell'applicazione delle abilità e delle conoscenze;
B (4) – "ottimo" – ottimo raggiungimento dei risultati di apprendimento, insieme alla capacità di applicare le competenze e le conoscenze in modo mirato e creativo. Alcuni dettagli delle conoscenze e delle competenze possono presentare errori che non sono né sostanziali né gravi;
C (3) – "buono" – buon raggiungimento dei risultati di apprendimento, insieme alla capacità di applicare le competenze e le conoscenze in modo pertinente. Una certa imprecisione e incertezza sono evidenti nella profondità e nei dettagli delle conoscenze e delle competenze;
D (2) – "soddisfacente" – raggiungimento sufficiente dei risultati di apprendimento, insieme all'applicazione delle conoscenze e delle competenze in modo tipico; in situazioni atipiche sono evidenti sia l'incertezza che la mancanza di conoscenze e competenze.
E (1) – "scarso" – raggiungimento minimo accettabile dei risultati di apprendimento più importanti, insieme a un'applicazione limitata delle conoscenze e delle competenze in situazioni tipiche; in situazioni atipiche situazioni in cui sono evidenti sia una notevole incertezza sia una mancanza di conoscenze e competenze;
F (0) – "insufficienza" – risultati in termini di conoscenze e competenze al di sotto dello standard minimo.