Programma di dettaglio della tesi
(da presentare al completamento del 20% delle attività di tesi)

(*compilato dallo studente entro due mesi dalla comunicazione dell'assegnazione della tesi da parte della Commissione Tesi a seguito dell'incontro con il docente relatore e del relativo avvio delle attività*)

Da inviare utilizzando il seguente form:
https://forms.office.com/Pages/ResponsePage.aspx?id=22cHw9o91E2KTQl9IsuZ03nJw8jHdCpNpV5x3k_J3dRUOFBDOFRXVDNOWEVZNUIxWVNLWFI0MjJQVS4u

Nome Cognome studente
Luigi Russo

Docente relatore
Giuseppe D'Aniello, Sabrina Senatore

Insegnamento di riferimento
Situation Awareness

Titolo argomento di tesi
Costruzione e specializzazione di un Knowledge Graph per la Cyber Situation Awareness

Descrizione dell'attività

1. ***Descrizione del problema che si vuole affrontare (circa 5 righe)***
   Nella cybersecurity, l'analisi e la risposta a vulnerabilità e minacce sono essenziali per strategie di difesa efficaci, ma i metodi tradizionali spesso non reggono l'aumento dei dati e della complessità. La Situation Awareness consente una visione globale degli eventi in corso, cruciale per comprendere il profilo di sicurezza di un'organizzazione. Un approccio basato su knowledge graph per modellare mediante relazioni le minacce e vulnerabilità di sistemi, attraverso domande in linguaggio naturale, può aiutare gli utenti a identificare situazioni critiche, risolverle e rispondere efficacemente agli incidenti di sicurezza.

2. ***Analisi dello stato dell'arte, scientifico e/o tecnologico (circa mezza pagina)***
   - *Se la tesi ha carattere prevalentemente progettuale – applicativo, identificare lo stato dell'arte tecnologico.*
   - *Se la tesi ha invece carattere prevalentemente metodologico, fare riferimento a lavori scientifici o metodologie a cui la tesi è collegata.*
   - *I riferimenti devono essere riportati nella forma [1] [2] ecc e devono essere inclusi nella sezione "Bibliografia"*

   I grafi di conoscenza per la cybersecurity offrono approcci olistici per elaborare enormi volumi di dati complessi sulla sicurezza informatica provenienti da fonti diverse. Questi strumenti possono supportare gli analisti di sicurezza nell'ottenere informazioni dettagliate sulle minacce informatiche, migliorare la consapevolezza della situazione (cyber-situation awareness), ottenere nuove conoscenze, e comprendere le correlazioni tra i dati aggregati. Inoltre,

permettono di visualizzare reti, flussi di dati e percorsi di attacco, agevolando la comprensione e la prevenzione delle minacce. Attraverso l'aggregazione e l'integrazione di dati eterogenei e la loro rappresentazione strutturata è possibile aumentare il livello di situation awareness consentendo il monitoraggio delle minacce in tempo reale e l'anticipazione di possibili scenari di rischio. In [1] si esaminano i modelli di dati basati su grafi più rilevanti utilizzati in questo ambito. Ci sono molte caratteristiche relative alla sicurezza informatica e ai processi di rete che devono essere memorizzate, e la semantica delle conoscenze catturate varia notevolmente a seconda del modello di dati del grafo utilizzato.

L'analisi immediata dei rapporti di cybersecurity è una sfida fondamentale per gli esperti di sicurezza, poiché ogni giorno viene generata una quantità incommensurabile di informazioni informatiche, che richiede strumenti di estrazione automatica delle informazioni per facilitare l'interrogazione e il recupero dei dati. In [2] viene presentato Open-CyKG: un framework Open Cyber Threat Intelligence (CTI) Knowledge Graph (KG) costruito utilizzando un modello neurale di Open Information Extraction (OIE) basato sull'attenzione per estrarre informazioni preziose sulle minacce informatiche da rapporti non strutturati di Advanced Persistent Threat (APT). In particolare, per prima cosa vengono identificate le entità rilevanti sviluppando un Named Entity Recognizer (NER) neurale per la cybersecurity che aiuta a etichettare le triple generate dal modello OIE. In seguito, i dati strutturati estratti vengono canonicalizzati per costruire il KG utilizzando tecniche di fusione con word embeddings. Di conseguenza, i professionisti della sicurezza possono eseguire query per recuperare informazioni preziose dal framework Open-CyKG.

3. ***Finalità della tesi, contributo dello studente e descrizione dell'attività progettuale di tesi (circa una pagina)***
   - *Descrivere dettagliatamente il progetto che si intende svolgere nell'ambito della tesi.*
     - *Descrivere gli obiettivi, le metodologie/tecnologie adottate (che cosa lo studente farà durante la sua attività di tesi e come lo farà)*
     - *Dettagliare (se presente) il carattere di innovatività introdotto nel progetto rispetto allo stato dell'arte*
     - *Descrivere le fasi in cui si articolerà lo sviluppo del progetto di tesi*

L'obiettivo principale di questa attività di tesi è la modellazione e progettazione di un Knowledge Graph per la Cyber Situation Awareness in modo da catturare le minacce e garantire una maggiore sicurezza.
In un contesto come quello della cybersecurity, in cui ci sono enormi quantità di informazioni complesse e veloci, consentirebbe all'utente (es. analista della sicurezza) di raggiungere e mantenere un livello di Situation Awareness (SA) che gli permetta di identificare, comprendere e anticipare le minacce in evoluzione.
A tale scopo saranno utilizzate ontologie presenti in letteratura o create ad hoc, realizzate mediante modelli di estrazione delle informazioni (OIE) per individuare relazioni ed entità e definire le triple secondo il modello RDF.

L'attività di tesi si articola nelle seguenti fasi:

- **Analisi preliminare del dominio e dello stato dell'arte -** La prima fase riguarda un'analisi preliminare del dominio di interesse e l'analisi del relativo stato dell'arte.

Verranno esplorate e comprese le metodologie e tecnologie esistenti per l'estrazione delle informazioni, con particolare attenzione all'utilizzo di dataset relativi alla CyberSA. Verranno individuate le best practices e le soluzioni più accreditate nell'applicazione di tali tecnologie.

- **Studio dei dati e modellazione della Goal-Driven Task Analysis (GDTA) -** La seconda fase consiste nello studio dei dati e la raccolta di dataset rappresentativi del dominio di interesse. Inoltre, sulla base del dataset scelto e del contesto di analisi (tipologia di attacco o minaccia nel dominio di interesse della Cybersecurity) verrà modellata la Goal Driven Task Analysis (GDTA, metodologia della Situation Awareness) per identificare gli obiettivi, i task e le decisioni che possono consentire di incrementare il livello comprensione della situazione.
- **Costruzione del Knowledge Graph** Nella terza fase verrà sviluppato un Knowledge Graph (KG) partendo da un modello semantico-ontologico. Questo modello integrerà la conoscenza di dominio specifica e farà uso di ontologie esistenti in letteratura, anche se parziali o ad alto livello, per descrivere il contesto applicativo.
- **Interrogazione del Knowledge Graph -** La quarta fase si concentrerà sull'utilizzo di linguaggi di interrogazione come SPARQL e Cypher per consentire un accesso efficiente alle informazioni nel Knowledge Graph.
- **Traduzione delle query in linguaggio naturale -**Verranno poi implementati meccanismi che permettano di tradurre in linguaggio naturale le query strutturate, ad esempio sfruttando tecniche avanzate di Natural Language Processing (NLP) e di Large Language Models.
- **Testing e valutazione del sistema** - Ci sarà una fase di test per valutare le prestazioni del sistema in condizioni realistiche, apportando miglioramenti e ottimizzazioni basate sui risultati dei test.

4. Descrizione del protocollo sperimentale o del setup sperimentale (circa mezza pagina)

- *Sperimentazione che si intende effettuare (per tesi di tipo prevalentemente metodologico) o descrizione dettagliata del setup sperimentale (per tesi di tipo prevalentemente applicativo)*
- *Indici prestazionali che saranno utilizzati per misurare la bontà del lavoro svolto e riferimento ai valori di tali indici (se già disponibili) di sistemi esistenti o di metodi allo stato dell'arte*

Per valutare le prestazioni del sistema proposto, sarà definito un ambiente sperimentale che simula scenari realistici nel contesto della Cyber Situation Awareness (Cyber SA). A tal fine, verranno utilizzati i dataset rappresentativi modellati e rappresentati attraverso un Knowledge Graph (KG) che fungerà da base per tutte le fasi successive.
Nella fase preliminare, il sistema Open-CyKG [2] individuato inizialmente per estrarre le NE è stato scartato a causa di incompatibilità con il dataset scelto. Di conseguenza il grafo di conoscenza sarà modellato manualmente utilizzando ed estendendolo con le ontologie standard del dominio.

Le query del sistema saranno progettate per rispecchiare esigenze operative degli analisti della sicurezza, includendo domande relative alla comprensione delle minacce emergenti, alla correlazione degli eventi e all'identificazione di misure di risposta adeguate.
Questo setting permetterà di verificare il funzionamento del sistema in condizioni che riflettono l'uso reale, analizzando le sue capacità di elaborare informazioni, effettuare retrieval mirati e generare risposte contestualizzate.

Il setup sperimentale comprenderà:

- Una fase di elaborazione e pre-processing dei dati iniziali per estrarre entità e relazioni, costruendo un grafo di conoscenza utilizzando approcci semantici.
- Creazione di una struttura coerente e navigabile utilizzando Neo4j.
- Generazione di query SPARQL e Cypher per consentire agli utenti di esplorare il Knowledge Graph e recuperare informazioni pertinenti.
- Utilizzo di un set di domande in linguaggio naturale che verranno poi tradotte in query strutturate.
- Valutazione del sistema attraverso:
    - Graph Knowledge Embedding (GKE): mediante l'uso di tecniche di ML come GKE, saranno estratte le rappresentazioni vettoriali delle entità presenti nel grafo ontologico costruito in precedenza, in modo da consentire un confronto più organico tra le strutture a grafo e impiegare metriche di stato dell'arte come Hits@N e Mean Reciprocal Rank (MRR) per valutare le prestazioni.
    - Analisi qualitativa, volta a individuare errori o informazioni mancanti. In particolare, le risposte del sistema saranno confrontate con quelle di un sistema basato su Retrieval-Augmented Generation (RAG).

5. ***Dettaglio dei dataset che saranno utilizzati per la sperimentazione (con riferimento al tipo di dataset, se reale o sintentico, al numero campioni, ecc) (circa 5 righe)***

   In tale sezione devono essere chiarite le motivazioni alla base della scelta di quel dataset evidenziando il fatto che il dataset sia rappresentativo di un'istanza reale del problema affrontato. Laddove non è possibile utilizzare un'istanza reale del problema, è necessario chiarire e motivare accuratamente le ragioni alla base di tale circostanza.

   Per la sperimentazione verranno utilizzato il dataset D3FEND [3] e il dataset ATT&CK [4] di MITRE, che modellano e rappresentano contromisure tecniche offensive relative alla cybersecurity. Si tratta di dataset reali che integrano informazioni provenienti da brevetti, documentazione tecnica e letteratura scientifica, analizzando oltre 500 brevetti selezionati tra il 2001 e il 2018. La scelta di questi dataset è motivata dalla loro capacità di fornire una rappresentazione semantica dettagliata delle tecniche di difesa informatica, incluse le loro relazioni con tattiche offensive.

   D3FEND e ATT&CK sono stati scelti poiché rappresentano un'istanza reale del dominio di interesse, offrendo un'ampia copertura e specificità nel contesto della Cyber Situation Awareness, con il potenziale di supportare sistemi avanzati di interrogazione.

6. ***Descrizione del dimostratore che sarà realizzato nell'ambito della tesi***

   - *Laddove non sia prevista la realizzazione di alcun dimostratore, specificare il motivo per cui non è possibile realizzare un dimostratore da mostrare live (anche nella forma di un video) durante la seduta di laurea*

   Sarà prodotto un video esplicativo che illustra il funzionamento del sistema. In particolare, verranno mostrate le risposte del sistema con e senza contesto.

Proposta di sommario
Nota: Deve contenere i titoli dei capitoli e delle sezioni. Questi capitoli sono obbligatori, ma è possibile integrare con capitoli aggiuntivi.

1. Introduzione
    - Definizione del problema
    - Rilevanza della problematica nel contesto dell'ingegneria informatica

2. Stato dell'arte
    - Analisi di dettaglio dello stato dell'arte
    - I Knowledge Graph e la semantica
    - Individuazione di possibili avanzamenti rispetto allo stato dell'arte

3. Contributo originale alla soluzione del problema
    - Definizione della metodologia proposta
    - Progettazione del sistema proposto
    - Innovazioni di carattere applicativo
    - Strumenti, tecnologie e modelli utilizzati per la realizzazione

4. Validazione sperimentale e aspetti applicativi
    - Descrizione delle metriche di valutazione dei risultati
    - Definizione del protocollo sperimentale o di verifica
    - Descrizione dei dati e/o del caso di studi utilizzato per la sperimentazione
    - Presentazione e analisi dei risultati
    - Valutazione della significatività dei risultati ottenuti e dei miglioramenti apportabili

Bibliografia
[1] Sikos, L.F. Cybersecurity knowledge graphs. *Knowl Inf Syst* **65**, 3511–3531 (2023).
[2] Sarhan, Injy, and Marco Spruit. "Open-cykg: An open cyber threat intelligence knowledge graph." *Knowledge-Based Systems* 233 (2021): 107524.
[3] Kaloroumakis, Peter E., and Michael J. Smith. "Toward a knowledge graph of cybersecurity countermeasures." *The MITRE Corporation* 11 (2021): 2021.
[4] MITRE. "Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK)." MITRE Corporation. URL: https://attack.mitre.org/.

Contributi di natura progettuale ed implementativa che il tesista dovrà fornire (circa 10 righe)
Il tesista sarà responsabile di diversi aspetti progettuali e implementativi nell'ambito della tesi. Tra i contributi principali, si evidenzia:

- La progettazione e costruzione di un grafo di conoscenza rappresentativo del dominio CyberSA, basato su dataset specifici e tecnologie semantiche.
- L'utilizzo di query strutturate in SPARQL o Cypher per l'estrazione delle informazioni rilevanti.

- L’adattamento di un Large Language Model (LLM) per la fase di generazione di risposte basate su contesto, assicurando coerenza e rilevanza delle informazioni generate.
- Lo sviluppo di un ambiente di test per simulare scenari realistici di CyberSA e per valutare le performance complessive del sistema in condizioni operative.
- L’iterazione sul progetto per migliorare le prestazioni del sistema, attraverso test, approcci ML esistenti in letteratura e ottimizzazioni specifiche.

Tecnologie e materiali da impiegare durante l’attività di tesi

- *Dettagliare se il tesista avrà accesso a specifici strumenti (es: strumenti di misurazione, piattaforme robotiche, server messi a disposizione dal gruppo di ricerca, ad esempio equipaggiati con GPU)*

Durante l’attività di tesi, il tesista avrà accesso a diverse tecnologie per il completamento del progetto. Tra i principali:

- librerie python per il processamento e la gestione dei dati;
- strumenti specifici per la modellazione e l’elaborazione di grafi di conoscenza;
- LLM pre-addestrati per la gestione delle query e la generazione delle risposte;
- dataset specifici relativi al dominio della cybersecurity, utilizzati per creare la base di conoscenza.

Eventuali esami ancora da sostenere alla data di consegna del presente documento

- Indicare per ciascun esame la data (mese/anno) in cui si prevede di sostenerlo

XXX

Data (mese/anno) in cui l’attività di tesi è iniziata con un impegno sostanzialmente a tempo pieno
Dicembre 2024

Data (mese/anno) in cui presumibilmente sarà discussa la tesi di laurea
Marzo/aprile 2025

(Solo per le Tesi svolte in ERASMUS)
Sede
XXX

Periodo di svolgimento
XXX

Tutor
XXX

Note