Integrazione di Large Language Models per il supporto decisionale nella Security Assurance

Corso di Laurea Triennale in Sicurezza dei Sistemi e delle Reti Informatiche

Relatore: Prof. Marco Anisetti

Tiziano Radicchi (12172A)

16 Luglio 2025

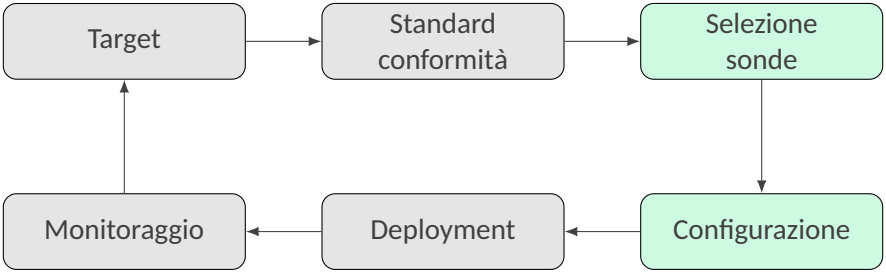
UNIVERSITÀ DEGLI STUDI DI MILANO

Agenda

1 Introduzione

- Introduzione
- Soluzione proposta
- Misurazioni
- Conclusioni

PaaS per fornire **governance** sulla sicurezza ICT attraverso **valutazione** continua della **conformità** e supporto a **standard** (CIS Benchmarks, PCI DSS, . . .).



Problema

Interazione manuale per selezione e configurazione sonde da eseguire.

- Conoscenza approfondita del catalogo sonde, soggetto a:
  - aggiunta
  - modifica
- Relazione tra standard e sonde

Produttività ridotta

Soggetto ad errori

Soluzione

1 Introduzione

Automatizzazione selezione e configurazione sonde tramite **Large Language Model** (LLM) e utilizzando **modelli** di **dimensioni ridotte**

Supporto decisionale alla selezione

Flessibilità ad aggiornamenti normativi

Costo e privacy

Soluzione

Automatizzazione selezione e configurazione sonde tramite **Large Language Model** (LLM) e utilizzando **modelli** di **dimensioni ridotte**

Supporto decisionale alla selezione

Flessibilità ad aggiornamenti normativi

Costo e privacy

Una delle prime soluzioni LLM-based per Security Assurance

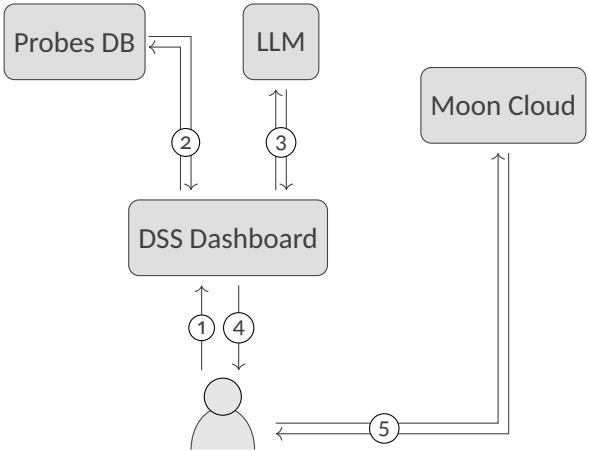
Attività svolte

2 Soluzione proposta

1. Progettazione **Decision Support System (DSS)**
2. Creazione di una **metodologia** per supportare l'uso di LLM
3. Valutazione **performance** del sistema attraverso Proof-of-Concept

Architettura

2 Soluzione proposta



Metodologia

2 Soluzione proposta

Classificazione query

Selezione base, verifica controlli/questionario

Dataset e valutazione

Nomenclatura e metriche

Set informazioni

Elenco e formato

Tassonomia prompt

Graduale arricchimento con dettagli

Prompts

3 Selezioni + configurazione

Supporto a standard

Documentazione sonde

Esempio selezione

3 Misurazioni

```
Host1:  10.3.14.2, Apache Web
server on port 8080;
Host2:  10.3.14.1, PfSense with
admin panel on port 80 and SSH
connection.
```

Verify that the Apache installation is secure.

(Qwen/Qwen2.5-Coder-14B-Instruct, t=0.3, top_p=0.3)

$\Longrightarrow$

Host1 - Apache - apache-cis

Host1 - Apache - web-vuln-scan

Host1 - Apache - observatory

Esempio selezione

3 Misurazioni

```
(...AgID control list ...)  +
Host1:  10.3.14.2, Apache Web
server on port 8080;
Host2:  10.3.14.1, PfSense with
admin panel on port 80 and SSH
connection.

I want to implement the 1.1.1 control.
```

(Qwen/Qwen2.5-Coder-14B-Instruct, t=0.3, top_p=0.3)

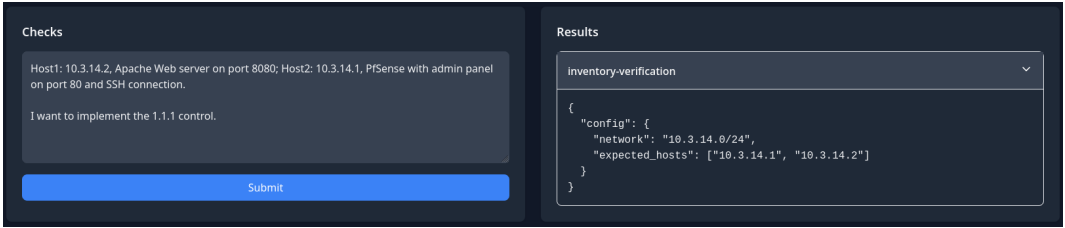
$\Longrightarrow$

"Implementare un inventario delle risorse attive correlato a quello ABSC 1.4"

inventory-verification

Esempio configurazione

3 Misurazioni



Valutazione performance

3 Misurazioni

1. **Walkthrough** dimostrativo $\implies$ risposte simili a selezione ideale (fornita da esperto)

2. Approccio **LLM-as-a-Judge**
   - **Validato**: preferenza coerente per selezione ideale
   - **Utilizzato**:
     - Dimostra legame prompt $\longleftrightarrow$ qualità output
     - $\implies$ migliori performance anche in modelli più piccoli

Conclusioni

4 Conclusioni

- Definizione di una metodologia di **Security Assurance** basata su **LLM**
- Realizzazione di un'**architettura** per selezione e configurazione di sonde
- Sviluppo di un PoC funzionante e valutazione **performance**

Sviluppi futuri

4 Conclusioni

Valutazione modelli e tecniche di decoding

Generazione dataset, esecuzione benchmarks

Fine-tuning

Embedding conoscenza cybersecurity-related

Integrazione con Moon Cloud

Deployment automatico

Integrazione di Large Language Models per il supporto decisionale nella Security Assurance

Grazie!