Finanziato dall'Unione europea
NextGenerationEU

Ministero dell'Università e della Ricerca

Italiadomani
PIANO NAZIONALE DI RIPRESA E RESILIENZA

ICSC
Centro Nazionale di Ricerca in HPC, Big Data and Quantum Computing

ICSC
Centro Nazionale di Ricerca in HPC, Big Data and Quantum Computing

Spoke 3 - Astrophysics and Cosmos Observations

Ugo Becciani e Pasquale Lubrano

Spoke 3 General Meeting

12-14 Giugno 2023

Dipartimento di Fisica e Astronomia – Università di Catania

Progetto: Porting di codice seriale su HPC & Quantum Computing

Progetto: Porting di codice seriale su HPC & Quantum Computing

Capofila	**Sogei-Membro ICSC privato** A. Ballarin – M. Innocenti (SNI)
Membri ICSC coinvolti	**INAF**
Spoke Proponente	**Spoke 3 «Astrofisics & cosmos observation»**
Altri Spoke coinvolti	**Spoke 10 «Quantum Computing»**
Livello TRL	***TRL 7*** — **Dimostrazione di un prototipo di sistema in ambiente operativo**

Altri programmi coinvolti	**Keep Calm - Kernel Engines Enable to Prevent Cyber Attacks with Learning Machines (progetto co-finanziato da Cyber 4.0)**

Progetto: Porting di codice seriale su HPC & Quantum Computing

Descrizione generale del Progetto:
Porting di codice seriale su HPC & Quantum Computing

Scrittura di algoritmi di Machine Learning (ML), reperibili nelle loro versioni in Open Source, in un linguaggio adatto a:

- **computazione HPC,**
- **computazione quantistica.**

L'obiettivo riguarda lo sviluppo di sistemi basati su algoritmi di Machine Learning ai fini della previsione degli attacchi cibernetici (Progetto KeepCalm).

Ambienti HPC e/o basati su computazione quantistica, consentirebbero una migliore risposta in real-time agli attacchi cibernetici, incrementando la capacità reattiva, aspetto basilare in ambito cybersecurity.

Progetto: Porting di codice seriale su HPC & Quantum Computing

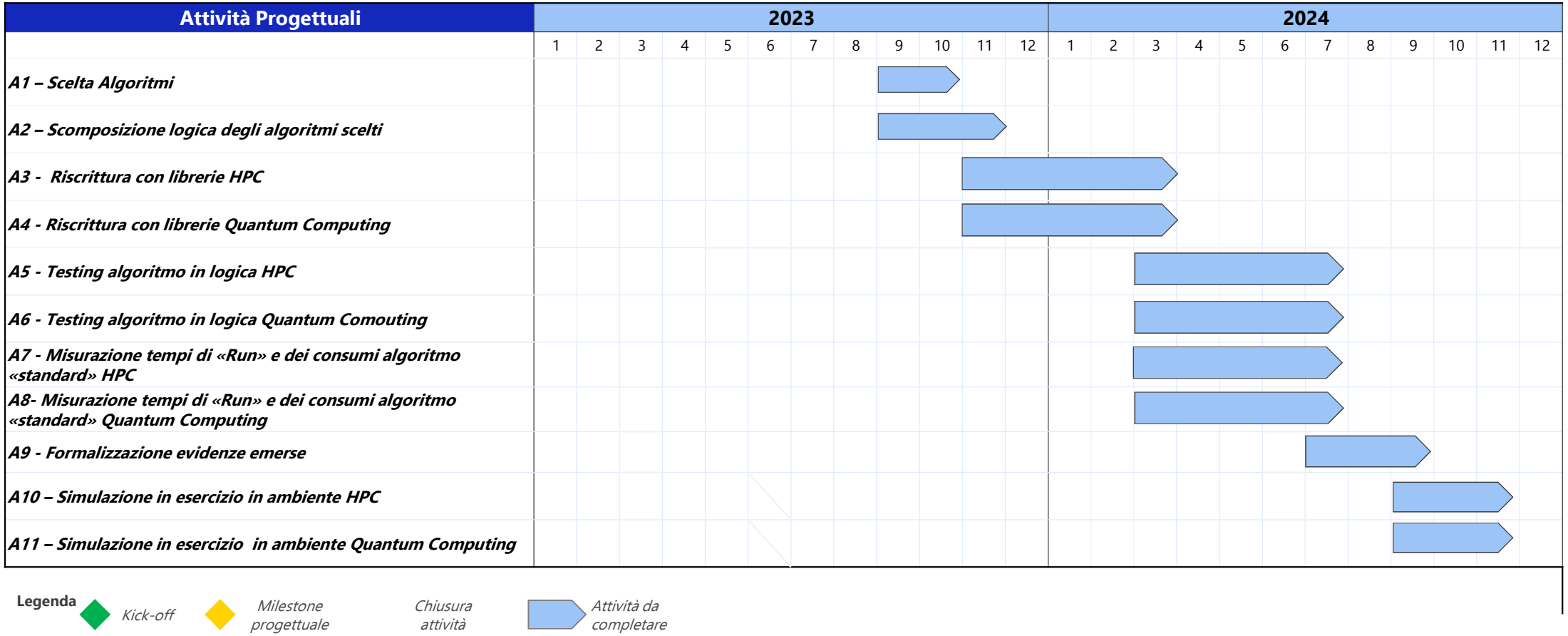
Obiettivi del Progetto:
Porting di codice seriale su HPC & Quantum Computing

- Creazione di un ambiente a supporto della previsione e identificazione preventiva di minacce cyber:
  a) tempistiche prossime al real-time,
  b) incremento del grado di resilienza contro le singole minacce.

- Creazione di un sistema metodologico che guidi la trascrizione di codice tipicamente seriale verso piattaforme ad alte prestazioni.

- Unificare le fasi di sviluppo che architetture HPC e quantistiche hanno in comune.

Gantt - Porting di codice seriale su HPC & Quantum Computing



Progetto: Porting di codice seriale su HPC & Quantum Computing

Le Minacce Cyber: Porting di codice seriale su HPC & Quantum Computing

Gli **effetti economici e sociali** degli attacchi cyber sono diventati sempre più rilevanti per le vittime tanto quanto la **perdita di reputazione** con la diffusione di dati sensibili.

Prendendo in considerazione il 2022, i cyber-attacchi nel mondo sono cresciuti del 38% confrontandoli con l'anno precedente (Check Point Research). Il confronto tra Nord America, America Latina ed Europa segna, rispettivamente: +52%, +29%.

I settori più colpiti sono le amministrazioni pubbliche e la sanità. Sono cresciuti anche gli attacchi a discapito di banche (8%), produttori di tecnologie hardware e software (7%) e istituzioni per la formazione e la ricerca (18%).

Inoltre, il **divario** tra il **potenziale danno** e l'**efficacia delle possibili contromisure** si è ampliato:

i rischi informatici non solo stanno crescendo in modo sostanziale, ma continuano anche a mancare di un efficace contenimento.

Generalmente, quando si è a conoscenza di un attacco, la minaccia ha già portato i suoi effetti devastanti al sistema.
Per questo è necessario

intervenire sulla capacità previsionale, il prima possibile, in modo da evitare potenziali danni.

Progetto: Porting di codice seriale su HPC & Quantum Computing

Gli Algoritmi:
Porting di codice seriale su HPC & Quantum Computing

Algoritmi di machine learning sperimentati nella previsione di attacchi cyber:

AdaBoost M1	Random Committees
Hoeffding Tree	Random Tree
Naïve Bayes	Real Ada Boost
Random Forest	Stochastic Gradient Descent

Gli algoritmi qui elencati vengono utilizzati in ensemble, ovvero simultaneamente, al fine di aumentare la capacità di intercettazione della minaccia.
Training su casi di esempio.
Modalità supervisionata.
Anomalie segnalate costituiscono gli elementi di retraining per il fine tuning.

Progetto: Porting di codice seriale su HPC & Quantum Computing

Scenari Operativi e Use Case:
Porting di codice seriale su HPC & Quantum Computing

- **Phishing**: Strategia hacker per estrarre informazioni sensibili tramite email oppure suggerendo il download di allegati pericolosi.
  - I modelli di machine learning sono proposti per l'**analisi del contenuto**, **struttura** e **metadati** delle email per identificare tentativi di phishing.
  - Classificazione delle email come legittime o sospette.

- **Distributed Denial-of-Service** (DDoS): sono attacchi che interrompono la disponibilità di un sistema informatico, impediscono agli utenti di accedere, inondandolo di traffico internet.
  - I modelli di machine learning monitorano il traffico della rete e segnalano alert in caso di attività sospette.

Progetto: Porting di codice seriale su HPC & Quantum Computing

Risultati Attesi:
Porting di codice seriale su HPC & Quantum Computing

Il **risultato principale atteso dal progetto** è la realizzazione di un sistema di rilevamento il quanto più possibile tempestivo di attacchi cyber.

L'analisi di pattern, anomalie e indicatori consentono una risposta diretta:

- **attenuando**, gli effetti degli attacchi,
- **riducendo** i danni e i tempi di non disponibilità dei sistemi informatici.

Ci si aspetta una riduzione di falsi positivi e una difesa proattiva.
Obiettivi che assicurano **patch software tempestive**, **riduzione delle vulnerabilità** e **implementazione di misure** che minimizzano i successi di attacco.

Progetto: Porting di codice seriale su HPC & Quantum Computing

Impatti Sul Business:
Porting di codice seriale su HPC & Quantum Computing

- **Alerts tempestivi** su potenziali attacchi cyber.
- **Misure proattive** che rafforzano le difese e mitigano i rischi.
- **Analisi di dataset a larga scala**, identificazione sorgenti emergenti di attacco e predizione di trend future di attacco.
- Sviluppo di robuste **strategie di sicurezza**.
- **Processing and analisi veloce dei dati** per risposte real-time per rilevare, mitigare e analizzare le minacce cyber.

Tutto ciò potrebbe ridurre al minimo il potenziale danno causato da un attacco in corso e accelerare gli sforzi di ripristino.