PROGRAMMA

5 Esperti – profilo tecnico con esperienza nel campo della cyber security o della cyber intelligence applicate alla difesa preventiva, proattiva o reattiva

Lett. **B** dell'art.1 del bando

- **EVENTUALE TEST PRESELETTIVO -** quesiti logico-matematici, logico-deduttivi e di comprensione del testo
- **PROVA SCRITTA** - svolgimento di due quesiti tecnici su due differenti ambiti tematici, scelti tra i sei quesiti proposti dalla Commissione (verranno proposti due quesiti per ogni ambito tematico), e di un elaborato in lingua inglese

Ambiti tematici:

- **Sicurezza delle architetture informatiche**
  - Gestione delle identità digitali e controllo degli accessi
  - Sicurezza delle reti, dei dati, delle applicazioni e dei sistemi distribuiti
  - Gestione del rischio informatico: valutazione delle minacce e individuazione dei presidi
  - Normativa e framework di cyber security nazionali e internazionali
  - Sicurezza della supply chain: strategie, normative e approcci per la mitigazione del rischio
  - Crittografia post-quantum e quantum-safe
  - Artificial Intelligence e Blockchain: potenzialità e rischi per la cybersicurezza

- **Verifiche di sicurezza e cyber defence**
  - Verifiche di sicurezza, esercitazioni tabletop, attività di red team testing
  - Gestione delle vulnerabilità del software
  - Gestione e monitoraggio degli incidenti di sicurezza
  - Digital forensics: raccolta e gestione delle evidenze digitali
  - Tecniche e procedure per l'analisi del malware
  - Strategie e tecniche per la cyber deception
  - Ciclo di vita degli indicatori di compromissione e threat hunting

- **Cyber threat intelligence e information sharing**
  - Tipologie di attacchi e attori della minaccia cyber (tattiche, tecniche e procedure)
  - Metodologie e framework per l'analisi strutturata della minaccia cyber (MITRE ATT&CK, Kill Chain, Diamond Model)
  - Ciclo di intelligence e livelli della cyber threat intelligence
  - Principi e metodi per l'attribuzione di un attacco cyber
  - Open source intelligence e surface/deep/dark web monitoring
  - Modelli, metodi e protocolli per lo scambio informativo
  - Flussi informativi e modelli organizzativi per la difesa preventiva, proattiva e reattiva (ISAC, CERT, CSIRT, SOC)

- **PROVA ORALE -** un colloquio riguardante gli ambiti tematici previsti per la prova scritta e una conversazione in lingua inglese. L'argomento della tesi di laurea e le esperienze professionali maturate potranno formare oggetto del colloquio.