BANCA D'ITALIA
EUROSISTEMA

CONCORSO 5 ESPERTI - PROFILO TECNICO CON ESPERIENZA NEL CAMPO DELLA *CYBER SECURITY* O DELLA *CYBER INTELLIGENCE* APPLICATE ALLA DIFESA PREVENTIVA, PROATTIVA O REATTIVA

(Lettera B - Bando del 24 aprile 2026)

Testo n. 2

LA SICUREZZA DELLE ARCHITETTURE INFORMATICHE

QUESITO N. 1

A. Si illustrino gli *smart contract* e si specifichi quali sono i principali rischi cyber derivanti dalla loro adozione.

B. Gli agenti autonomi basati su LLM (es. architetture ReAct, AutoGPT, sistemi multi-agente come CrewAI) possono essere utilizzati in *task* complessi che richiedono pianificazione e uso di strumenti esterni. Si discutano i rischi cyber derivanti dall'uso di agenti che possono interagire con sistemi informatici tramite API.

C. In un sistema multiagente, si illustrino gli approcci che possono essere utilizzati per mitigare il rischio legato alla *supply chain* di modelli già parzialmente addestrati e di moduli *software* per il *tooling*.

QUESITO N. 2

Si consideri un'architettura *Big Data* composta da un *cluster* distribuito (ad esempio, Spark/Hadoop con *ingestion* dei dati tramite Kafka), *storage* principale su HDFS e un livello di accesso ai dati basato su *database* NoSQL. L'architettura è distribuita su più *data center* mediante replica dei dati e dei servizi tra ambienti distinti.

A. Si descrivano le principali superfici di attacco, distinguendo le vulnerabilità a livello di:
   - rete, con riferimento alla comunicazione tra nodi, ai *broker* Kafka e alla replica tra *data center*;
   - *storage*, con riferimento a HDFS, *snapshot*, *backup* e gestione dei permessi;
   - livello applicativo, con riferimento a *job scheduler*, API di accesso, interfacce di amministrazione e strumenti di esecuzione o monitoraggio dei *job*.

B. Si proponga un sistema di sicurezza *defense-in-depth* che includa:
   - meccanismi di autenticazione e autorizzazione per utenti, servizi e applicazioni;
   - cifratura dei dati *at-rest* e *in-transit*;
   - segmentazione di rete e isolamento dei nodi, includendo *firewall*, *subnet* dedicate e zone DMZ per l'*ingestion*;
   - la gestione sicura delle credenziali e delle chiavi crittografiche.

C. Si illustri un sistema di monitoraggio e *audit logging* centralizzato con l'obiettivo di rilevare tempestivamente le principali minacce di sicurezza; si discuta, inoltre, come ottenere un adeguato bilanciamento tra livello di dettaglio dei *log* e complessità di gestione.

LE VERIFICHE DI SICUREZZA E LA CYBER DEFENCE

QUESITO N. 3

A. Si discutano gli accorgimenti che un'organizzazione che si sottopone a *test* avanzati di cybersicurezza di tipo *Threat-Led Penetration Testing* (TLPT) deve adottare affinché siano opportunamente mitigati gli eventuali effetti negativi associati alla conduzione di tali *test* sui propri servizi ICT. Si descrivano, in particolare, quali regole di ingaggio sia opportuno prevedere nei confronti di un fornitore di servizi di *red team testing* (c.d. *Red Team Provider*).

B. Nell'ambito di un TLPT, il *Red Team* ha pianificato la seguente catena di attacco:

1. Si inviano delle *e-mail* alle *mailbox* aziendali di specifici obiettivi identificati, avendo preventivamente recuperato informazioni che consentono di costruire un pretesto ritenuto convincente. Le *e-mail* non contengono allegati ma inducono a cliccare su un *link* presente al loro interno.
2. A seguito dell'apertura del *link*, si avvia automaticamente il *download* di un archivio con estensione .ZIP che viene scaricato sulla postazione della vittima.
3. La vittima è indotta a estrarre il contenuto del *file* .ZIP e cliccare su un *file* estratto con estensione .LNK, la cui icona e il cui nome lo fanno sembrare un normale documento PDF.
4. All'apertura del .LNK viene eseguito del codice che apre un documento PDF presente nell'archivio e che avvia un'applicazione portatile legittima, nascosta anch'essa nell'archivio.
5. Il processo avviato carica una DLL, nascosta, di tipo malevolo, estratta dal *file* .ZIP.
6. L'impianto, in esecuzione, tenta la comunicazione in HTTPS verso uno o più *server* esterni.

Si illustrino i componenti principali dell'infrastruttura d'attacco necessari per eseguire quanto descritto; inoltre, si specifichino per ciascuno dei punti elencati le tattiche e le tecniche di attacco utilizzate, anche facendo riferimento a *framework* internazionali.

C. Si illustrino, con l'ausilio di esempi pratici, le tecniche di *cyber deception* che possono essere utilizzate per contrastare i tentativi locali di *discovery* e *privilege escalation* condotti su un *server* con sistema operativo Linux.

QUESITO N. 4

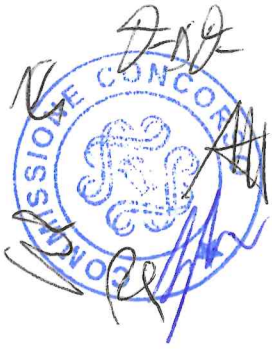
A. Si descriva la catena di custodia e il suo ruolo nell'ambito delle attività di *digital forensics*; inoltre, si illustrino metodi e strumenti per l'acquisizione delle evidenze digitali da una postazione di lavoro compromessa.

B. Si consideri l'analisi di un campione malevolo rinvenuto su una postazione di lavoro compromessa. Si illustrino le principali tecniche di analisi statica e dinamica del *malware*, evidenziando le finalità dei due approcci e le cautele operative da adottare. Si descrivano i possibili vantaggi e i rischi che l'utilizzo di *large language model* di frontiera può introdurre in tale ambito.

C. Durante l'analisi preliminare del campione malevolo sono stati rilevati i seguenti elementi:

- `file: update_service.exe;`
- `hash SHA-256: 8f3a9c4e2b7d1f90a6c2e48b7712a0f35e6c9b4a3d8f1120c7e65a9b0d123456;`
- `mutex: Global\WinUpdSvc_2024;`
- `chiave di registro: HKCU\Software\Microsoft\Windows\CurrentVersion\Run\WinUpdateService;`
- `dominio contattato: cdn-update-check[.]com;`
- `indirizzo IP remoto: 198.51.XXX.27;`
- `processo figlio osservato: powershell.exe -ExecutionPolicy Bypass -WindowStyle Hidden.`

Si individuino gli elementi classificabili come indicatori di compromissione; inoltre, si indichino quali tra essi risultano più facilmente modificabili dall'attore della minaccia e quali sono più significativi per il rilevamento dell'attività malevola.



LA CYBER THREAT INTELLIGENCE E L'INFORMATION SHARING

QUESITO N. 5

A. Si illustrino le finalità, la struttura e le caratteristiche della *Cyber Kill Chain* descrivendone ciascuna delle fasi. Si confronti inoltre la *Cyber Kill Chain* con altri modelli concettuali di rappresentazione delle fasi di un attacco cyber, descrivendo i pro e i contro nell'utilizzo di ciascun modello.

B. Si rappresentino le fasi di un attacco *ransomware* schematizzandole attraverso un modello concettuale di riferimento. Si descrivano inoltre le caratteristiche di ciascuna fase dell'attacco e si illustrino: *i)* le finalità di questa tipologia di attacchi; *ii)* le modalità possibili per ottenere l'accesso iniziale alle infrastrutture informatiche delle organizzazioni vittime; *iii)* le tecniche comunemente adottate dai gruppi *ransomware* per compromettere la disponibilità e/o la riservatezza dei dati e dei servizi informatici; *iv)* le modalità di estorsione tipicamente utilizzate dai gruppi *ransomware; v)* le infrastrutture generalmente utilizzate dai gruppi *ransomware* per condurre gli attacchi e gestire l'attività estorsiva.

C. Durante l'analisi di un attacco cyber che ha colpito un'organizzazione, sono state identificate le seguenti informazioni:

   i. il *threat actor* ha sfruttato alcune vulnerabilità *n-day* presenti in sistemi esposti su internet;
   ii. il *threat actor* ha utilizzato script *Powershell* per enumerare gli utenti di dominio;
   iii. il *threat actor* ha creato nuovi account utente con privilegi di amministratore;
   iv. il *threat actor* ha esfiltrato alcuni dati dell'organizzazione utilizzando cartelle di rete condivise (*SMB shares*);
   v. il *threat actor* ha cifrato i sistemi di virtualizzazione e *backup* compromettendone la disponibilità e causando l'interruzione dell'operatività aziendale.

   Si identifichino tattiche e tecniche adottate dal *threat actor* facendo riferimento al *framework* MITRE-ATT&CK, esplicitando eventuali ipotesi aggiuntive.

QUESITO N. 6

A. Si illustrino i principali modelli per l'*information sharing* sulla minaccia cyber, delineando inoltre standard e strumenti tecnologici abilitanti a eseguire lo scambio informativo in modo strutturato, sicuro e automatizzato. Si comparino schematicamente i modelli descritti raffrontandone le caratteristiche ed evidenziandone le differenze.

B. Il CERT di un'organizzazione riceve, tramite strumenti automatizzati, le informazioni riportate di seguito:

Campagna InvoiceUpdate-2026

Event ID [redacted]

UUID bc284e6e-e855-471b-9bee-[redacted]

Creator org Contoso Ltd.

Date	Category	Type	Value	Tags	Comment	IDS
2026-06-25	Network activity	Domain	acme-energy-support.com	tlp:green	Dominio di phishing	X
2026-06-25	Network activity	Domain	sync-telemetry-cloud.net	tlp:red	Command & Control	X
2026-06-25	Payload delivery	Filename	Invoice_Update_June2026.pdf	tlp:green	PDF malevolo	X
2026-06-25	Payload delivery	sha256	6f5d98f93d56aab8f1d0a8f96eb0d23f30db7a4e4d91e88bc36a447f3ea61d4a	tlp:red	Hash file malevolo	X
2026-06-25	Attribution	threat-actor	Road Runner	tlp:red	Threat actor	

- Si produca una breve informativa di *operational cyber threat intelligence* che descriva l'evento "*Campagna InvoiceUpdate-2026*".
- Si esplicitino: *i*) le valutazioni che il CERT dell'organizzazione deve effettuare per condividere a controparti esterne le informazioni tecniche e l'informativa precedentemente prodotta sull'evento; *ii*) gli strumenti da adottare per gestire l'*information sharing* sull'evento.

C. Si illustrino gli elementi che il CERT di un'organizzazione pubblica operante nel settore finanziario deve valutare per intraprendere attività di *information sharing* con altre controparti nazionali e internazionali, stipulando accordi bilaterali per lo scambio informativo e/o partecipando a iniziative multilaterali. Si presentino inoltre i contenuti principali di un accordo bilaterale per lo scambio informativo sulle minacce cyber con una controparte nazionale.

<u>Prova in lingua inglese</u>

To promote sustainable tourism, fifteen South Tyrol Rangers will be employed in the Dolomites this summer to educate tourists about respecting the environment and reducing their impact on local ecosystems. Do you think initiatives like this are an effective way to address the challenges of mass tourism? Discuss.