Tecnico Superiore “Tecnico superiore per lo sviluppo software, web e l'analisi dei dati - Software & Web Developer”
BIENNIO 2024-26

[Rif. Pa 2024-22900/RER - CUP E61J24000820007]

approvata con Del. di Giunta Regionale DGR 1670/2024 del 29/07/2024 -
DD 19065/2024 del 17/09/2024 finanziata da FSE+ 2. Istruzione e formazione

Prova TEORICO-PRATICA
(minimo 24 punti - massimo 40 punti)

AMBITO [Architetture e infrastrutture per i sistemi di comunicazione]

Ferrara 16/07/2026

Dossier di lavoro di [Sara Fava]

Brief di progetto	**Introduzione** La società SecureNet Cloud ha subito una serie di tentativi di intrusione. Il tuo compito è realizzare una Dashboard di Analisi Incidenti che legga un file di log in formato JSON, visualizzi le minacce in modo chiaro e utilizzi una logica di "Suggerimento AI" per fornire contromisure immediate al team di sicurezza.

	Queste le richieste, suddivise in task:
Task 1	Elaborazione Dati (Il "Motore" PHP) Dato il seguente set di dati JSON (simulato) per popolare la tua applicazione: [{"id": "EVT-001", "ip": "192.168.1.45", "tipo": "Brute Force", "pericolo": "Alto", "stato": "Rilevato", "data": "2026-03-26 08:30:12"}, {"id": "EVT-002", "ip": "10.0.0.12", "tipo": "SQL Injection", "pericolo": "Critico", "stato": "Bloccato", "data": "2026-03-26 09:15:45"}, {"id": "EVT-003", "ip": "172.16.254.1", "tipo": "Port Scanning", "pericolo": "Basso", "stato": "Monitorato", "data": "2026-03-26 09:40:00"}, {"id": "EVT-004", "ip": "185.220.101.34", "tipo": "DDoS Attack", "pericolo": "Critico", "stato": "Bloccato", "data": "2026-03-26 10:05:22"}, {"id": "EVT-005", "ip": "192.168.1.112", "tipo": "XSS Payload", "pericolo": "Medio", "stato": "Rilevato", "data": "2026-03-26 10:12:10"}, {"id": "EVT-006", "ip": "5.45.201.12", "tipo": "Malware Callback", "pericolo": "Alto", "stato": "Isolato", "data": "2026-03-26 10:25:55"}, {"id": "EVT-007", "ip": "10.0.5.88", "tipo": "Unauthorized Login", "pericolo": "Alto", "stato": "Rilevato", "data": "2026-03-26 10:45:30"}, {"id": "EVT-008", "ip": "88.150.12.4", "tipo": "Data Exfiltration", "pericolo": "Critico", "stato": "Bloccato", "data": "2026-03-26 11:00:01"}, {"id": "EVT-009", "ip": "192.168.1.200", "tipo": "Local Privilege Escalation", "pericolo": "Alto", "stato": "Rilevato", "data": "2026-03-26 11:15:18"}, {"id": "EVT-010", "ip": "172.16.0.5", "tipo": "ARP Spoofing", "pericolo": "Basso", "stato": "Monitorato", "data": "2026-03-26 11:30:44"}, {"id": "EVT-011", "ip": "45.33.22.11", "tipo": "Botnet Activity", "pericolo": "Medio", "stato": "Rilevato", "data": "2026-03-26 11:45:00"}, {"id": "EVT-012", "ip": "10.0.0.254", "tipo": "SSH Tunneling", "pericolo": "Alto", "stato": "Bloccato", "data": "2026-03-26 12:05:12"}, {"id": "EVT-013", "ip": "192.168.10.15", "tipo": "Phishing Link Click", "pericolo": "Medio", "stato": "Rilevato", "data": "2026-03-26 12:20:33"}, {"id": "EVT-014", "ip": "91.210.10.44", "tipo": "Credential Stuffing", "pericolo": "Alto", "stato": "Isolato", "data": "2026-03-26 12:40:55"}, {"id": "EVT-015", "ip": "172.16.254.10", "tipo": "Dictionary Attack", "pericolo": "Basso", "stato": "Bloccato", "data": "2026-03-26 13:00:10"}] Richiesta: Decodifica il JSON in PHP e crea una tabella che mostri gli incidenti. Logica Colore: Se il pericolo è "Critico", la riga deve lampeggiare o avere un bordo rosso marcato.

Task 2	Crea una sezione della dashboard chiamata "AI Security Consultant". - Quando l'utente clicca su un incidente, il sistema deve generare un "Consiglio AI" automatico. - Esempio di logica da implementare (Switch/If): *Se il tipo è Brute Force → Suggerire: "Attivare 2FA e blocco IP dopo 3 tentativi". Se il tipo è SQL Injection → Suggerire: "Utilizzare Prepared Statements (PDO) e sanitizzare gli input".
Task 3	- Realizza una dashboard Responsive con una barra laterale di navigazione. - Inserisci un grafico (anche statico o realizzato con CSS) che mostri la percentuale di minacce bloccate rispetto a quelle solo rilevate. - Area Prompt: Aggiungi un campo di testo dove l'analista può scrivere un comando per "Chiedere all'AI" un approfondimento su un IP specifico.
Task 4	- Generazione PDF Incident Report: Il sistema deve generare un PDF professionale che riassuma l'incidente selezionato, includendo l'indirizzo IP dell'attaccante e il consiglio tecnico generato dall'AI. - Security Lock: L'accesso alla dashboard è consentito solo tramite la password: Admin_Secure_2026.
Quesito 1	Perché è più efficiente scambiare dati tra un server Cloud e una Dashboard usando il formato JSON rispetto a un semplice file di testo o XML?
Quesito 2	Nel caso dell'incidente "SQL Injection" rilevato nel log, spiega come l'utilizzo di PDO in PHP avrebbe potuto prevenire l'attacco alla radice.
Durata	5 ore Inizio ore 9,00 - Termine ore 14,00
Risorse tecnologiche a disposizione delle candidate / dei candidati	File Json – esempio chiamata Ai – credenziali FTP – Filezilla – Visual Studio

Modalità di consegna degli elaborati	Consegnare in formato ZIP l'elaborato scritto con le domante e l'applicativo. Utilizzare PHP – Javascript – Java - Html

Svolgimento della prova

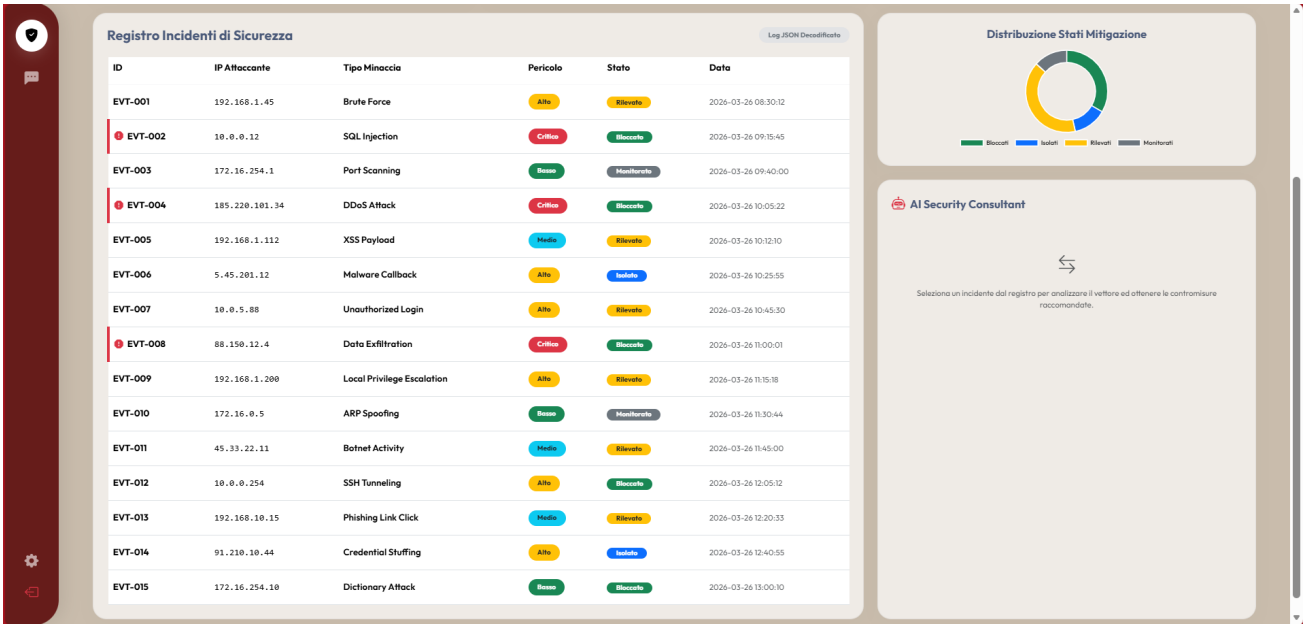
Task 1

Elaborazione Dati (Il "Motore" PHP)
Dato il seguente set di dati JSON (simulato) per popolare la tua applicazione:


```
[
  {"id": "EVT-001", "ip": "192.168.1.45", "tipo": "Brute Force", "pericolo": "Alto", "stato": "Rilevato", "data": "2026-03-26 08:30:12"},
  {"id": "EVT-002", "ip": "10.0.0.12", "tipo": "SQL Injection", "pericolo": "Critico", "stato": "Bloccato", "data": "2026-03-26 09:15:45"},
  {"id": "EVT-003", "ip": "172.16.254.1", "tipo": "Port Scanning", "pericolo": "Basso", "stato": "Monitorato", "data": "2026-03-26 09:40:00"},
  {"id": "EVT-004", "ip": "185.220.101.34", "tipo": "DDoS Attack", "pericolo": "Critico", "stato": "Bloccato", "data": "2026-03-26 10:05:22"},
  {"id": "EVT-005", "ip": "192.168.1.112", "tipo": "XSS Payload", "pericolo": "Medio", "stato": "Rilevato", "data": "2026-03-26 10:12:10"},
  {"id": "EVT-006", "ip": "5.45.201.12", "tipo": "Malware Callback", "pericolo": "Alto", "stato": "Isolato", "data": "2026-03-26 10:25:55"},
  {"id": "EVT-007", "ip": "10.0.5.88", "tipo": "Unauthorized Login", "pericolo": "Alto", "stato": "Rilevato", "data": "2026-03-26 10:45:30"},
  {"id": "EVT-008", "ip": "88.150.12.4", "tipo": "Data Exfiltration", "pericolo": "Critico", "stato": "Bloccato", "data": "2026-03-26 11:00:01"},
  {"id": "EVT-009", "ip": "192.168.1.200", "tipo": "Local Privilege Escalation", "pericolo": "Alto", "stato": "Rilevato", "data": "2026-03-26 11:15:18"},
  {"id": "EVT-010", "ip": "172.16.0.5", "tipo": "ARP Spoofing", "pericolo": "Basso", "stato": "Monitorato", "data": "2026-03-26 11:30:44"},
  {"id": "EVT-011", "ip": "45.33.22.11", "tipo": "Botnet Activity", "pericolo": "Medio", "stato": "Rilevato", "data": "2026-03-26 11:45:00"},
  {"id": "EVT-012", "ip": "10.0.0.254", "tipo": "SSH Tunneling", "pericolo": "Alto", "stato": "Bloccato", "data": "2026-03-26 12:05:12"},
  {"id": "EVT-013", "ip": "192.168.10.15", "tipo": "Phishing Link Click", "pericolo": "Medio", "stato": "Rilevato", "data": "2026-03-26 12:20:33"},
  {"id": "EVT-014", "ip": "91.210.10.44", "tipo": "Credential Stuffing", "pericolo": "Alto", "stato": "Isolato", "data": "2026-03-26 12:40:55"},
  {"id": "EVT-015", "ip": "172.16.254.10", "tipo": "Dictionary Attack", "pericolo": "Basso", "stato": "Bloccato", "data": "2026-03-26 13:00:10"}
]
```


Richiesta: Decodifica il JSON in PHP e crea una tabella che mostri gli incidenti.
Logica Colore: Se il pericolo è "Critico", la riga deve lampeggiare o avere un bordo rosso marcato.

Inserire screenshot della Tabella: Un'immagine della dashboard che mostri gli incidenti caricati, evidenziando la logica colore (bordo rosso o effetto lampeggiante) per gli eventi CRITICI



ID	IP Attaccante	Tipo Minaccia	Pericolo	Stato	Data
EVT-001	192.168.1.45	Brute Force	Alto	Rilevato	2026-03-26 08:30:12
EVT-002	10.0.0.12	SQL Injection	Critico	Bloccato	2026-03-26 09:15:45
EVT-003	172.16.254.1	Port Scanning	Basso	Monitorato	2026-03-26 09:40:00
EVT-004	185.220.101.34	DDoS Attack	Critico	Bloccato	2026-03-26 10:05:22
EVT-005	192.168.1.112	XSS Payload	Medio	Rilevato	2026-03-26 10:12:10
EVT-006	5.45.201.12	Malware Callback	Alto	Isolato	2026-03-26 10:25:55
EVT-007	10.0.5.88	Unauthorized Login	Alto	Rilevato	2026-03-26 10:45:30
EVT-008	88.150.12.4	Data Exfiltration	Critico	Bloccato	2026-03-26 11:00:01
EVT-009	192.168.1.200	Local Privilege Escalation	Alto	Rilevato	2026-03-26 11:15:18
EVT-010	172.16.0.5	ARP Spoofing	Basso	Monitorato	2026-03-26 11:30:44
EVT-011	45.33.22.11	Botnet Activity	Medio	Rilevato	2026-03-26 11:45:00
EVT-012	10.0.0.254	SSH Tunneling	Alto	Bloccato	2026-03-26 12:05:12
EVT-013	192.168.10.15	Phishing Link Click	Medio	Rilevato	2026-03-26 12:20:33
EVT-014	91.210.10.44	Credential Stuffing	Alto	Isolato	2026-03-26 12:40:55
EVT-015	172.16.254.10	Dictionary Attack	Basso	Bloccato	2026-03-26 13:00:10

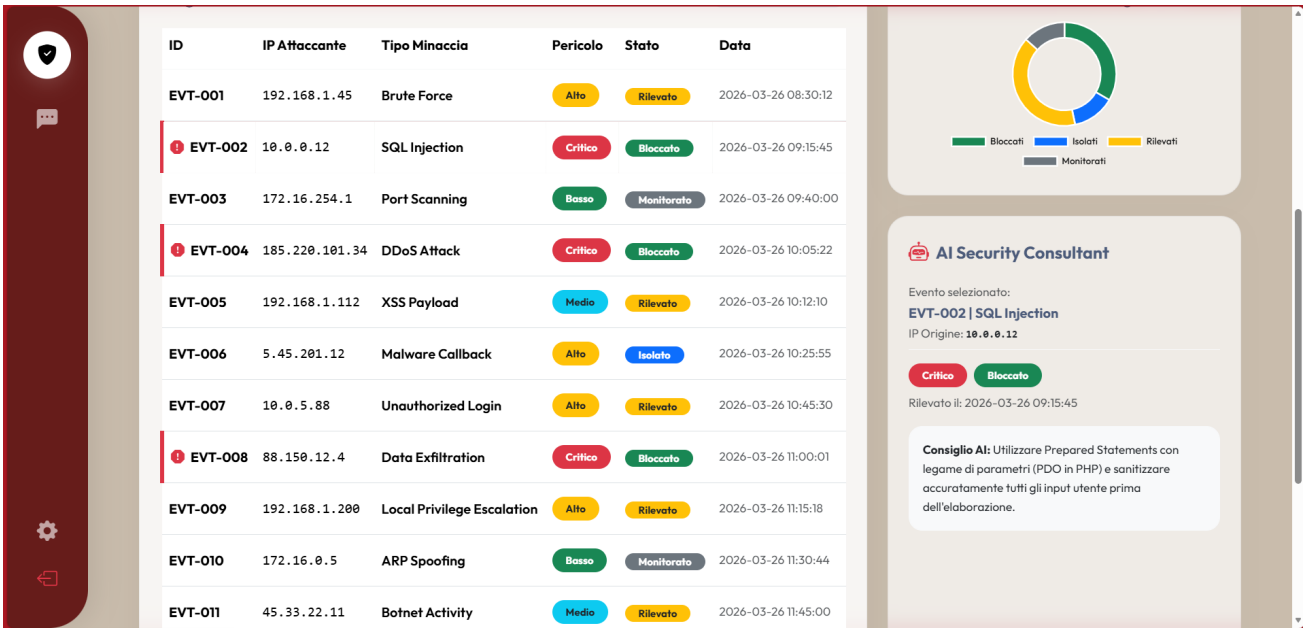
Task 2

Crea una sezione della dashboard chiamata "AI Security Consultant".

- Quando l'utente clicca su un incidente, il sistema deve generare un "Consiglio AI" automatico.
- Esempio di logica da implementare (Switch/If): *Se il tipo è Brute Force → Suggerire: "Attivare 2FA e blocco IP dopo 3 tentativi".

Se il tipo è SQL Injection → Suggerire: "Utilizzare Prepared Statements (PDO) e sanitizzare gli input".

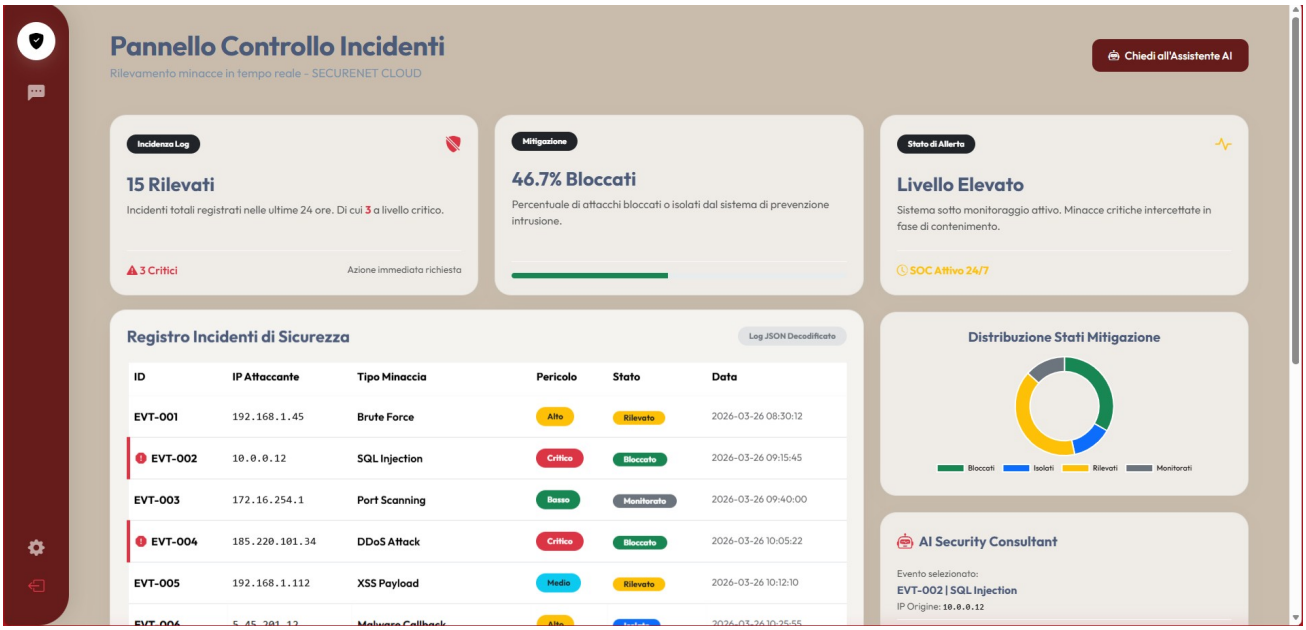
Inserire un'immagine che mostri cosa succede quando si clicca su un incidente e come appare il box "AI Security Consultant" con il consiglio generato



Task 3

- Realizza una dashboard Responsive con una barra laterale di navigazione.
- Inserisci un grafico (anche statico o realizzato con CSS) che mostri la percentuale di minacce bloccate rispetto a quelle solo rilevate.
- Area Prompt: Aggiungi un campo di testo dove l'analista può scrivere un comando per "Chiedere all'AI" un approfondimento su un IP specifico.

Inserire screenshot della Dashboard Completa: Una vista d'insieme che mostri la barra laterale di navigazione e il layout adattivo



Task 4

- Generazione PDF Incident Report: Il sistema deve generare un PDF professionale che riassuma l'incidente selezionato, includendo l'indirizzo IP dell'attaccante e il consiglio tecnico generato dall'AI. - Security Lock: L'accesso alla dashboard è consentito solo tramite la password: Admin_Secure_2026.

Inserire un'immagine o una scansione del report PDF professionale prodotto dal sistema, contenente l'ID incidente, l'IP dell'attaccante e il consiglio dell'AI.

Inserire anche il frammento di codice (es. gestione sessione o controllo POST) che verifica la password

```
if ($_SERVER['REQUEST_METHOD'] === 'POST' && isset($_POST['password'])) {
  if ($_POST['password'] === DASHBOARD_PASSWORD) {
    $_SESSION['logged_in'] = true;
    header("Location: index.php");
    exit;
  } else {
    $login_error = 'Password non corretta. Riprova.';
  }
}
```

Quesito 1

JSON è molto leggero e più facile da usare. E' più efficiente quando si fa una dashboard perché pesa meno, ha un tempo di elaborazione veloce e struttura ideale per i linguaggi web moderni

Quesito 2

Candidata/o [Nome e Cognome a stampatello]

…….

Firma

…….