Descrizione del Progetto

Ogni studente deve realizzare una presentazione tecnica individuale o una relazione scritta su un tema riguardante gli standard, la compliance e la responsabilità professionale nell'ambito della sicurezza informatica. Questo progetto è strettamente collegato al modulo "Standard, legislazione e responsabilità digitale" affrontato in classe e intende esplorare l'intersezione tra aspetti tecnici, normativi ed etici.

Obiettivi

- Approfondire il rapporto tra standard tecnici e requisiti normativi
- Comprendere il concetto di responsabilità professionale nella sicurezza IT
- Analizzare framework e best practices riconosciuti internazionalmente
- Sviluppare una visione critica dell'evoluzione normativa in ambito digitale

Tematiche Proposte

1. Framework di Gestione della Sicurezza a Confronto

- Analisi comparativa di ISO 27001, NIST CSF e CIS Controls
- Implementazione pratica: dalla teoria alla conformità effettiva
- Gap analysis e risk assessment metodologie
- Certificazione e audit: processi e valore aggiunto
- Integrazione con altri standard (business continuity, privacy)

2. Security Operations Center (SOC): Implementazione Standard-Compliant

- Architettura di un SOC conforme a standard internazionali
- Log management e monitoraggio secondo best practices
- Incident response procedures e documentazione
- Metriche di sicurezza e reporting strutturato
- Integrazione del SOC con il security program aziendale

3. Responsible Disclosure e Programmi di Bug Bounty

- Evoluzione storica e principi della responsible disclosure
- Framework etici e legali per security researchers
- Struttura e gestione di un programma di bug bounty
- Standardizzazione dei processi di vulnerability management
- Casi studio di collaborazione ricercatori-aziende

4. Identità Digitale e Sistemi di Autenticazione Avanzati

- Evoluzione dei sistemi di autenticazione e standard emergenti
- FIDO2/WebAuthn: funzionamento tecnico e implementazione
- Single Sign-On e federazione delle identità: architetture sicure
- Gestione delle credenziali in contesti enterprise
- Self-Sovereign Identity: principi e tecnologie

5. PKI e Infrastrutture di Fiducia Digitale

- Architettura e gestione di una PKI enterprise-grade
- Standard per certificati digitali e loro evoluzione
- Certificate Authority: requisiti operativi e tecnici
- eIDAS e normative sulla firma digitale
- Trust models tradizionali vs. decentralizzati

6. Compliance GDPR in Sistemi Complessi

- Privacy by Design: implementazione tecnica nei sistemi IT
- Data Protection Impact Assessment: metodologia e documentazione
- Gestione tecnica dei diritti degli interessati
- Data breach: detection, containment e notification
- Casi studio di implementazione in settori regolamentati

7. Sicurezza del Codice e Secure Software Development Lifecycle

- Standard e framework per lo sviluppo sicuro (OWASP SAMM, BSIMM)
- DevSecOps: integrazione della sicurezza nel ciclo di sviluppo
- Automated security testing: strumenti e metodologie
- Gestione sicura delle dipendenze e supply chain
- Secure coding standards e code review

Formato dell'Elaborato

Opzione 1: Presentazione Tecnica (Preferita)

- **Numero slide**: Massimo 12 slide
- **Durata**: 10-12 minuti di presentazione + 5 minuti per domande tecniche
- **Formato**: PowerPoint o Google Slides

Struttura Consigliata per la Presentazione

1. Overview e contesto normativo/standard
2. Framework teorico di riferimento
3. Analisi dei requisiti tecnici e di compliance
4. Mapping tra controlli tecnici e requisiti normativi
5. Gap analysis e criticità comuni
6. Approccio implementativo e soluzioni
7. Documentazione e evidence collection
8. Audit e verification process
9. Caso studio o implementazione reale
10. Considerazioni etiche e professionali
11. Evoluzione futura degli standard
12. Riferimenti tecnici e normativi

Opzione 2: Relazione Tecnica

- **Lunghezza**: 7-10 pagine (esclusi copertina, indice, appendici e bibliografia)
- **Formato**: Documento Word o PDF, font Times New Roman 12pt, interlinea 1,5
- **Struttura**: Abstract tecnico, introduzione, metodologia, analisi dettagliata, implementazione, conclusioni e bibliografia

Requisiti Tecnici

- Approfondimento del framework normativo/standard scelto con dettagli implementativi
- Inclusione di almeno un diagramma di architettura o workflow
- Documentazione di strumenti o metodologie per la verifica della compliance

Criteri di Valutazione

Criterio	Peso	Descrizione
Comprensione degli Standard	30%	Accurata interpretazione dei framework di sicurezza, corretta applicazione dei requisiti normativi, comprensione delle relazioni tra controlli e compliance
Implementazione Tecnica	30%	Dettaglio delle soluzioni tecniche proposte, analisi della loro efficacia, mappatura concreta tra requisiti e controlli implementativi
Analisi delle Problematiche	20%	Identificazione di gap e sfide nell'implementazione, analisi critica dei limiti degli standard, proposte innovative per migliorare la conformità
Qualità dell'Elaborato	20%	Per presentazioni: organizzazione logica, efficacia comunicativa, gestione delle domande tecniche Per relazioni: struttura metodologica, precisione terminologica, documentazione adeguata

Suggerimenti per lo Sviluppo

1. Focalizzatevi su uno standard specifico o sul confronto mirato tra due framework complementari
2. Elaborate un caso di studio realistico che dimostri l'applicazione pratica dei requisiti
3. Create una matrice di mappatura tra requisiti normativi e controlli tecnici implementabili
4. Analizzate criticamente l'efficacia dei controlli proposti in relazione alle minacce attuali
5. Laddove possibile, fate riferimento a situazioni locali o nazionali per rendere il tema più concreto

Nota Importante

Gli elaborati saranno valutati in base alla loro qualità tecnica e all'analisi dell'impatto sociale dell'infrastruttura di rete scelta. **Una presentazione o relazione particolarmente curata e approfondita potrà essere considerata per una valutazione aggiuntiva in Sistemi e Reti**. La presentazione viene generalmente valutata con maggior peso rispetto alla relazione scritta, per via dell'acquisizione di competenze comunicative. Elementi che verranno considerati per la valutazione aggiuntiva:

- Approfondimento tecnico appropriato dell'infrastruttura di rete
- Capacità di collegare aspetti tecnici e implicazioni sociali
- Originalità dell'analisi e delle soluzioni proposte
- Per le presentazioni: efficacia comunicativa e gestione delle domande

Contatti

Per chiarimenti sul progetto e supporto tecnico: g.rovesti@gferraris.it