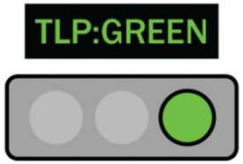
INTRODUZIONE A

NIST CYBERSECURITY FRAMEWORK 2.0



#whoami

Andrea Piras – CERT Manager

- 20 anni di esperienza in ICT e Cybersecurity
- Lavoro in ambito Cyber Threat Intelligence, Incident Response e Digital Forensics
- Esperienza in grandi aziende e settori critici: ESA, Leonardo, Accenture, PA, energia, banking
- Supporto strategico al top management e attività di pre-sales
- Focal Point nel trasformare esigenze business in soluzioni di sicurezza operative

MSc CyberSecurity

EC-Council Incident Handler

CIFI Forensic Analyst

Cybercrime Investigator

Virtual Hacking Pentester

CompTIA Secutiry+

TLP:GREEN

A cosa serve il NIST CSF

- **Valutare e migliorare la postura di cybersecurity**: Fornisce un linguaggio comune e una struttura per identificare le lacune nella sicurezza informatica.
- **Comunicare internamente ed esternamente**: Aiuta a uniformare il linguaggio tra IT, sicurezza, top management e stakeholder esterni (es. clienti, regolatori).
- **Allinearsi alle best practice**: Integra controlli e principi già riconosciuti (come ISO/IEC 27001, COBIT, NIST 800-53).
- **Pianificare investimenti in sicurezza**: Aiuta a prioritizzare le azioni in base al rischio.

Processo CSF

TLP:GREEN

Funzioni e Categorie

Function	Category	Category Identifier
Govern (GV)	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Cybersecurity Supply Chain Risk Management	GV.SC
	Roles, Responsibilities, and Authorities	GV.RR
	Policies, Processes, and Procedures	GV.PO
	Oversight	GV.OV
Identify (ID)	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Improvement	ID.IM
Protect (PR)	Identity Management, Authentication, and Access Control	PR.AA
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Platform Security	PR.PS
	Technology Infrastructure Resilience	PR.IR
Detect (DE)	Continuous Monitoring	DE.CM
	Adverse Event Analysis	DE.AE
Respond (RS)	Incident Management	RS.MA
	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
Recover (RC)	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO

TLP:GREEN

Definizione del contesto e degli obiettivi

- **Attività**:
  - Identifica il contesto di business, i beni critici, i regolamenti applicabili (es. NIS2, DORA).
  - Coinvolgi gli stakeholder chiave (IT, CISO, risk manager, compliance, direzione).
- **Output**:
  - Ambito di applicazione del framework (es. solo IT, oppure tutta l'azienda).
  - Obiettivi aziendali di sicurezza (es. continuità operativa, protezione dati).

Processo CSF

TLP:GREEN

Valutazione iniziale (Current Profile)

- **Attività**:
    - Mappa le attività esistenti rispetto alle **6 Function del CSF v2.0:** Govern, Identify, Protect, Detect, Respond, Recover
    - Usa i **Category e Subcategory** come checklist per valutare dove sei (AS-IS).
- **Output**:
    - "Profilo attuale" (Current Profile): fotografia della postura di sicurezza attuale.

Ogni categoria CSF viene valutata con un **punteggio di implementazione da 0 a 3** in base alla maturità dei controlli e dei processi dell'organizzazione:

- **0 = Non implementato**: nessuna implementazione o capacità significativa in questo settore.
- **1 = Ad hoc / Parzialmente implementato**: esistono alcune pratiche informali o reattive, ma sono incomplete o non applicate in modo coerente.
- **2 = Definito / Informato sul rischio**: sono in atto e documentati controlli o processi per l'area, anche se potrebbero non essere pienamente efficaci o applicati in modo uniforme in tutta l'organizzazione.
- **3 = Gestito / Adattivo**: i controlli sono pienamente implementati, regolarmente rivisti e integrati in un processo di miglioramento continuo (che riflette un alto livello di maturità)

Processo CSF

TLP:GREEN

Definizione degli obiettivi (Target Profile)

- **Attività**:
  - Definisci il livello desiderato di **maturità** per ciascuna funzione.
  - Considera rischi, priorità di business, risorse disponibili.
- **Output**:
  - "Profilo target" (Target Profile): obiettivi che si vuole raggiungere per ogni category / subcategory.

NOTA: anche il Target Profile può avere un **punteggio di implementazione da 0 a 3** che serve a identificare immediatamente il GAP che c'è con quello corrente nella fase successiva.

Processo CSF

TLP:GREEN

Analisi del gap e priorità

- **Attività:**
  - Confronta Current vs Target Profile per identificare le lacune.
  - Assegna una priorità basata su impatto e rischio.
- **Output:**
  - **Piano di miglioramento (Action Plan**), prioritizzando per impatto ed effort.

NOTA: le due fasi «Target Profile» e «Gap Analysis» alle volte vengono fuse insieme

Processo CSF

TLP:GREEN

Esecuzione e gestione continua

- **Attività:**
  - Implementa i controlli tecnici, procedurali e organizzativi.
  - Misura i risultati con KPI/KRI.
  - Aggiorna regolarmente i profili Current (e se occorre anche quelli Target).
  - Comunica i risultati a direzione e stakeholder (es. audit, board).

- **Output:**
  - Dashboard della sicurezza, metriche di avanzamento, incident report.
  - Documentazione di governance, comunicazione al top management.

Processo CSF

TLP:GREEN

Esempi di KPI / KRI per il Monitoraggio

Esempi di KPI rilevanti

Govern

- % dipendenti che hanno completato la formazione obbligatoria

Identify

- % asset mappati e classificati in CMDB
- % di fornitori valutati con criteri di rischio cyber

Protect

- % di workstation/server con patch critiche installate entro 15 giorni
- % autenticazioni protette con MFA

Detect

- % eventi critici rilevati dal SIEM analizzati entro 24h

Respond

- Tempo medio di risposta a incidenti di sicurezza (MTTR)

Recover

- Tempo medio di recovery da backup testato (RTO effettivo)
- % esercitazioni di disaster recovery completate

Esempi di KRI rilevanti

- Numero di vulnerabilità critiche non ancora patchate dopo 30gg
- Numero di account privilegiati attivi e non tracciati
- Numero di fornitori terzi ad alto rischio senza piani di mitigazione
- Frequenza di violazioni policy segnalate dal SOC
- % di asset con antivirus disabilitato o non aggiornato

TLP:GREEN

Sessione Demo

Inizia lo use case

TLP:GREEN