Il Framework di Psicologia della Cybersecurity: Un Modello di Valutazione delle Vulnerabilità Pre-Cognitive Integrando Scienze Psicoanalitiche e Cognitive

Un Preprint

Giuseppe Canale, CISSP
Ricercatore Indipendente
kaolay@gmail.com, g.canale@escom.it, m@xbe.at
ORCID: 0009-0007-3263-6897

18 agosto 2025

Sommario

Presentiamo il Framework di Psicologia della Cybersecurity (CPF), un modello interdisciplinare innovativo che identifica le vulnerabilità pre-cognitive nelle posture di sicurezza organizzative attraverso l'integrazione sistematica della teoria psicoanalitica e della psicologia cognitiva. A differenza degli approcci tradizionali di consapevolezza della sicurezza che si concentrano sui processi decisionali consci, il CPF mappa gli stati psicologici inconsci e le dinamiche di gruppo a specifici vettori di attacco, consentendo strategie di sicurezza predittive piuttosto che reattive. Il framework comprende 100 indicatori in 10 categorie, dalle vulnerabilità basate sull'autorità (Milgram, 1974) ai bias cognitivi specifici dell'IA, utilizzando un sistema di valutazione ternario (Verde/Giallo/Rosso). Il nostro modello mantiene esplicitamente la privacy attraverso l'analisi aggregata dei pattern comportamentali, senza mai profilare gli individui. Il CPF rappresenta la prima integrazione formale della teoria delle relazioni oggettuali (Klein, 1946), delle dinamiche di gruppo (Bion, 1961) e della psicologia analitica (Jung, 1969) con la pratica contemporanea della cybersecurity, affrontando il divario critico tra i controlli tecnici e i fattori umani nei fallimenti della sicurezza.

Parole chiave: cybersecurity, psicologia, psicoanalisi, bias cognitivo, fattori umani, valutazione delle vulnerabilità, processi pre-cognitivi

1 Introduzione

Nonostante la spesa globale per la cybersecurity superi i 150 miliardi di dollari annualmente[7], le violazioni con successo continuano ad aumentare, con i fattori umani che contribuiscono a oltre l'85% degli incidenti[21]. I framework di sicurezza attuali—da ISO 27001 a NIST CSF—affrontano principalmente i controlli tecnici e procedurali, mentre gli interventi sui "fattori umani" rimangono limitati alla formazione sulla consapevolezza della sicurezza a livello conscio[18]. Questo approccio fraintende fondamentalmente i meccanismi psicologici che sottendono alle vulnerabilità della sicurezza.

Ricerche neuroscientifiche recenti dimostrano che i processi decisionali avvengono 300-500ms prima della consapevolezza cosciente[14, 20], suggerendo che le decisioni di sicurezza sono sostanzialmente influenzate dai processi pre-cognitivi. Inoltre, il comportamento organizzativo emerge da dinamiche di gruppo complesse che operano al di sotto della consapevolezza cosciente[3, 11]. Questi processi inconsci creano vulnerabilità sistematiche che i controlli tecnici non possono affrontare.

Il Framework di Psicologia della Cybersecurity (CPF) affronta questo divario fornendo la prima integrazione sistematica di:

- **Teoria psicoanalitica delle relazioni oggettuali** per comprendere la scissione e proiezione organizzativa
- **Teoria delle dinamiche di gruppo** per mappare le assunzioni inconsce collettive
- **Psicologia cognitiva** per identificare i bias sistematici nelle decisioni relative alla sicurezza
- **Psicologia dell'IA** per affrontare le vulnerabilità dell'interazione uomo-IA

Questo articolo presenta le fondamenta teoriche del CPF, il design architetturale e la roadmap per futuri studi di validazione.

2 Fondamenta Teoriche

2.1 Il Fallimento degli Interventi a Livello Conscio

I programmi tradizionali di consapevolezza della sicurezza assumono attori razionali che, quando informati sui rischi, modificheranno di conseguenza il comportamento[1]. Tuttavia, questa assunzione razionalista contraddice evidenze sostanziali da multiple discipline.

Evidenze Neuroscientifiche:

- Studi fMRI mostrano l'attivazione dell'amigdala (risposta alla minaccia) che avviene prima dell'impegno della corteccia prefrontale (analisi razionale)[13]
- I processi decisionali coinvolgono marcatori somatici che bypassano l'elaborazione cosciente[6]

Evidenze dell'Economia Comportamentale:

- Il Sistema 1 (veloce, automatico) domina il Sistema 2 (lento, deliberato) negli ambienti sotto pressione temporale[9]
- Il carico cognitivo compromette la qualità delle decisioni di sicurezza[2]

Evidenze Psicoanalitiche:

- Le organizzazioni sviluppano "sistemi di difesa sociale" contro l'ansia che creano punti ciechi di sicurezza[15]
- La proiezione delle minacce interne sui "hacker" esterni impedisce il riconoscimento dei rischi interni[12]

2.2 Contributi Psicoanalitici alla Cybersecurity

2.2.1 Le Assunzioni di Base di Bion

Bion[3] ha identificato tre assunzioni di base che i gruppi adottano inconsciamente quando affrontano l'ansia:

- **Dipendenza (baD)**: Cercare un leader/tecnologia onnipotente per la protezione
- **Attacco-Fuga (baF)**: Percepire le minacce come nemici esterni che richiedono difesa aggressiva o evitamento
- **Accoppiamento (baP)**: Sperare nella salvezza futura attraverso nuove soluzioni

Nei contesti di cybersecurity, questi si manifestano come:

- **baD**: Eccessiva dipendenza dai fornitori di sicurezza/soluzioni "proiettile d'argento"
- **baF**: Difesa perimetrale aggressiva ignorando le minacce interne
- **baP**: Acquisizione continua di strumenti senza affrontare le vulnerabilità fondamentali

2.2.2 Relazioni Oggettuali Kleiniane

Il concetto di Klein[12] di scissione—dividere gli oggetti in "tutto buono" o "tutto cattivo"—appare nella sicurezza organizzativa come:

- Addetti interni fidati (idealizzati) vs. attaccanti esterni (demonizzati)
- Sistemi legacy (familiari/buoni) vs. nuovi requisiti di sicurezza (minacciosi/cattivi)
- Proiezione delle vulnerabilità organizzative sugli "attaccanti sofisticati"

2.2.3 Lo Spazio Transizionale di Winnicott

Il concetto di spazio transizionale di Winnicott[22] aiuta a comprendere gli ambienti digitali come né completamente reali né completamente immaginari, creando vulnerabilità uniche:

- Ridotto testing della realtà negli ambienti virtuali
- Confusione tra identità digitale e sé
- Fantasie onnipotenti nel cyberspazio

2.2.4 Ombra e Proiezione Junghiane

Il concetto di ombra di Jung[8] spiega come le organizzazioni proiettano aspetti rinnegati sugli attaccanti:

- Gli hacker "black hat" incarnano l'aggressività repressa dell'organizzazione
- I team di sicurezza possono identificarsi inconsciamente con gli attaccanti (integrazione dell'ombra)
- L'ombra collettiva crea punti ciechi nella postura di sicurezza

2.3 Integrazione della Psicologia Cognitiva

2.3.1 Applicazione della Teoria del Doppio Processo

Il framework Sistema 1/Sistema 2 di Kahneman[9] rivela vulnerabilità specifiche:

Vulnerabilità del Sistema 1:

- Euristica della disponibilità: Sovrapesare attacchi recenti/memorabili
- Euristica dell'affetto: Decisioni di sicurezza basate sullo stato emotivo
- Ancoraggio: Il primo incidente di sicurezza modella tutte le risposte future

Limitazioni del Sistema 2:

- Carico cognitivo dalla complessità della sicurezza
- Deplezione dell'ego dalla vigilanza costante
- Ragionamento motivato per evitare i requisiti di sicurezza

2.3.2 I Principi di Influenza di Cialdini nel Contesto Cyber

I sei principi di Cialdini[5] si mappano direttamente sui vettori di social engineering:

1. **Reciprocità**: Attacchi quid pro quo
2. **Impegno/Coerenza**: Escalation graduale delle richieste
3. **Prova Sociale**: "Tutti cliccano questo link"
4. **Autorità**: Frode CEO, falso supporto IT
5. **Simpatia**: Costruzione di rapport prima dell'attacco
6. **Scarsità**: Azione urgente richiesta

2.3.3 Teoria del Carico Cognitivo

La limitazione del "numero magico sette" di Miller[17] crea vulnerabilità:

- Trade-off tra complessità e memorabilità delle password
- Affaticamento degli alert dalla proliferazione degli strumenti di sicurezza
- Paralisi decisionale da troppe opzioni di sicurezza

2.4 Vulnerabilità Psicologiche Specifiche dell'IA

Mentre i sistemi IA diventano integrali alle operazioni di sicurezza, emergono nuove vulnerabilità psicologiche:

2.4.1 Antropomorfizzazione

- Attribuzione di intenzioni umane ai sistemi IA
- Eccessiva fiducia nelle raccomandazioni dell'IA
- Attaccamento emotivo agli assistenti IA che crea vettori di manipolazione

2.4.2 Bias di Automazione

- Eccessiva dipendenza dagli strumenti di sicurezza automatizzati
- Ridotta vigilanza umana ("azzardo morale")
- Atrofia delle competenze nei team di sicurezza

2.4.3 Effetti di Trasferimento IA-Umano

- Bias umani codificati nei dati di addestramento dell'IA
- Sistemi IA che amplificano i punti ciechi organizzativi
- Loop di feedback tra bias umani e dell'IA

3 Architettura del Modello CPF

3.1 Principi di Design

L'architettura CPF segue cinque principi fondamentali:

1. **Preservazione della Privacy**: Tutte le valutazioni utilizzano dati aggregati; nessuna profilazione individuale
2. **Focus Predittivo**: Identifica le vulnerabilità prima dello sfruttamento
3. **Agnostico all'Implementazione**: Si mappa alle vulnerabilità, non a soluzioni specifiche
4. **Scientificamente Fondato**: Ogni indicatore collegato a ricerca consolidata
5. **Operativamente Pratico**: Punteggio ternario per insights azionabili

3.2 Struttura del Framework

Il CPF comprende 100 indicatori organizzati in una matrice 10×10. La Tabella 1 riassume le dieci categorie primarie:

Tabella 1: Categorie Primarie CPF e Fondamenta Teoriche

Codice	Categoria	Riferimento Primario
[1.x]	Vulnerabilità Basate sull'Autorità	Milgram (1974)
[2.x]	Vulnerabilità Temporali	Kahneman & Tversky (1979)
[3.x]	Vulnerabilità di Influenza Sociale	Cialdini (2007)
[4.x]	Vulnerabilità Affettive	Klein (1946), Bowlby (1969)
[5.x]	Vulnerabilità di Sovraccarico Cognitivo	Miller (1956)
[6.x]	Vulnerabilità delle Dinamiche di Gruppo	Bion (1961)
[7.x]	Vulnerabilità di Risposta allo Stress	Selye (1956)
[8.x]	Vulnerabilità dei Processi Inconsci	Jung (1969)
[9.x]	Vulnerabilità di Bias Specifici dell'IA	Integrazione Innovativa
[10.x]	Stati Convergenti Critici	Teoria dei Sistemi

3.2.1 Dettaglio Categoria: Vulnerabilità Basate sull'Autorità [1.x]

1.1 Conformità incondizionata all'autorità apparente

1.2 Diffusione di responsabilità nelle strutture gerarchiche

1.3 Suscettibilità all'impersonificazione di figure autoritarie

1.4 Bypassare la sicurezza per comodità del superiore

1.5 Conformità basata sulla paura senza verifica

1.6 Gradiente di autorità che inibisce la segnalazione di sicurezza

1.7 Deferenza alle rivendicazioni di autorità tecnica

1.8 Normalizzazione delle eccezioni esecutive

1.9 Prova sociale basata sull'autorità

1.10 Escalation dell'autorità durante crisi

3.2.2 Dettaglio Categoria: Vulnerabilità Temporali [2.x]

2.1 Bypass della sicurezza indotto dall'urgenza

2.2 Degradazione cognitiva sotto pressione temporale

2.3 Accettazione del rischio guidata dalle scadenze

2.4 Bias del presente negli investimenti di sicurezza

2.5 Sconto iperbolico delle minacce future

2.6 Pattern di esaurimento temporale

2.7 Finestre di vulnerabilità nell'orario della giornata

2.8 Lacune di sicurezza nei weekend/festivi

2.9 Finestre di sfruttamento nei cambi turno

2.10 Pressione di coerenza temporale

3.2.3 Dettaglio Categoria: Vulnerabilità di Influenza Sociale [3.x]

3.1 Sfruttamento della reciprocità

3.2 Trappole di escalation dell'impegno

3.3 Manipolazione della prova sociale

3.4 Override della fiducia basata sulla simpatia

3.5 Decisioni guidate dalla scarsità

3.6 Sfruttamento del principio di unità

3.7 Conformità per pressione dei pari

3.8 Conformità a norme insicure

3.9 Minacce all'identità sociale

3.10 Conflitti di gestione della reputazione

3.2.4 Dettaglio Categoria: Vulnerabilità Affettive [4.x]

4.1 Paralisi decisionale basata sulla paura

4.2 Assunzione di rischi indotta dalla rabbia

4.3 Trasferimento di fiducia ai sistemi

4.4 Attaccamento ai sistemi legacy

4.5 Nascondere la sicurezza basato sulla vergogna

4.6 Sovraconformità guidata dal senso di colpa

4.7 Errori scatenati dall'ansia

4.8 Negligenza correlata alla depressione

4.9 Negligenza indotta dall'euforia

4.10 Effetti di contagio emotivo

3.2.5 Dettaglio Categoria: Vulnerabilità di Sovraccarico Cognitivo [5.x]

5.1 Desensibilizzazione da affaticamento degli alert

5.2 Errori da fatica decisionale

5.3 Paralisi da sovraccarico informativo

5.4 Degradazione da multitasking

5.5 Vulnerabilità del cambio di contesto

5.6 Tunneling cognitivo

5.7 Overflow della memoria di lavoro

5.8 Effetti di residuo dell'attenzione

5.9 Errori indotti dalla complessità

5.10 Confusione del modello mentale

3.2.6 Dettaglio Categoria: Vulnerabilità delle Dinamiche di Gruppo [6.x]

6.1 Punti ciechi di sicurezza da pensiero di gruppo

6.2 Fenomeni di spostamento rischioso

6.3 Diffusione di responsabilità

6.4 Inerzia sociale nei compiti di sicurezza

6.5 Effetto spettatore nella risposta agli incidenti

6.6 Assunzioni di gruppo di dipendenza

6.7 Posture di sicurezza attacco-fuga

6.8 Fantasie di speranza di accoppiamento

6.9 Scissione organizzativa

6.10 Meccanismi di difesa collettivi

3.2.7 Dettaglio Categoria: Vulnerabilità di Risposta allo Stress [7.x]

7.1 Compromissione da stress acuto

7.2 Burnout da stress cronico

7.3 Aggressione da risposta di attacco

7.4 Evitamento da risposta di fuga

7.5 Paralisi da risposta di congelamento

7.6 Sovraconformità da risposta di sottomissione

7.7 Visione a tunnel indotta dallo stress

7.8 Memoria compromessa dal cortisolo

7.9 Cascate di contagio dello stress

7.10 Vulnerabilità del periodo di recupero

3.2.8 Dettaglio Categoria: Vulnerabilità dei Processi Inconsci [8.x]

8.1 Proiezione dell'ombra sugli attaccanti

8.2 Identificazione inconscia con le minacce

8.3 Pattern di coazione a ripetere

8.4 Transfert verso figure autoritative

8.5 Punti ciechi da controtransfert

8.6 Interferenza dei meccanismi di difesa

8.7 Confusione di equazione simbolica

8.8 Trigger di attivazione archetipica

8.9 Pattern dell'inconscio collettivo

8.10 Logica del sogno negli spazi digitali

3.2.9 Dettaglio Categoria: Vulnerabilità di Bias Specifici dell'IA [9.x]

9.1 Antropomorfizzazione dei sistemi IA

9.2 Override del bias di automazione

9.3 Paradosso dell'avversione algoritmica

9.4 Trasferimento di autorità all'IA

9.5 Effetti della valle inquietante

9.6 Fiducia nell'opacità del machine learning

9.7 Accettazione delle allucinazioni dell'IA

9.8 Disfunzione del team umano-IA

9.9 Manipolazione emotiva dell'IA

9.10 Cecità alla correttezza algoritmica

3.2.10 Dettaglio Categoria: Stati Convergenti Critici [10.x]

10.1 Condizioni di tempesta perfetta

10.2 Trigger di fallimento a cascata

10.3 Vulnerabilità del punto di svolta

10.4 Allineamento del formaggio svizzero

10.5 Cecità del cigno nero

10.6 Negazione del rinoceronte grigio

10.7 Catastrofe di complessità

10.8 Imprevedibilità dell'emergenza

10.9 Fallimenti di accoppiamento del sistema

10.10 Gap di sicurezza dell'isteresi

3.3 Metodologia di Valutazione

La metodologia di valutazione CPF è attualmente teorica e in attesa di validazione empirica attraverso future implementazioni pilota. I metodi di raccolta dati proposti daranno priorità alle tecniche che preservano la privacy e all'analisi aggregata.

3.3.1 Sistema di Punteggio

Ogni indicatore riceve un punteggio ternario:

- **Verde (0)**: Vulnerabilità minima rilevata
- **Giallo (1)**: Vulnerabilità moderata che richiede monitoraggio
- **Rosso (2)**: Vulnerabilità critica che richiede intervento

Punteggio aggregato:

$$\text{Punteggio Categoria} = \sum_{i=1}^{10} \text{Indicatore}_i \quad (0 - 20 \text{ range}) \tag{1}$$

$$\text{Punteggio CPF} = \sum_{j=1}^{10} w_j \cdot \text{Categoria}_j \tag{2}$$

$$\text{Indice di Convergenza} = \prod_{j,k} \text{Interazione}_{j,k} \tag{3}$$

3.3.2 Meccanismi di Protezione della Privacy

- Unità minima di aggregazione: 10 individui
- Iniezione di rumore per privacy differenziale: $\epsilon = 0.1$
- Reporting con ritardo temporale: minimo 72 ore
- Analisi basata sui ruoli piuttosto che individuale
- Audit trail per tutti gli accessi ai dati

3.4 Mappatura dei Vettori di Attacco

Ogni categoria di vulnerabilità si mappa a specifici vettori di attacco come mostrato nella Tabella 2:

Tabella 2: Mappatura Vulnerabilità-Vettori di Attacco

Categoria di Vulnerabilità	Vettori di Attacco Primari
Autorità	Spear Phishing, Frode CEO
Temporale	Attacchi a Scadenza, Malware Bomba a Tempo
Sociale	Social Engineering, Minacce Interne
Affettiva	Campagne FUD, Ransomware
Sovraccarico Cognitivo	Sfruttamento Affaticamento Alert
Dinamiche di Gruppo	Disruption Organizzativa
Stress	Sfruttamento Burnout
Inconscio	Attacchi Simbolici
Bias IA	ML Avversariale, Avvelenamento
Convergente	Minacce Persistenti Avanzate

4 Studi di Validazione

4.1 Panoramica dell'Implementazione Pilota

Il framework CPF è attualmente nella fase di sviluppo teorico. Le implementazioni pilota sono in fase di pianificazione con organizzazioni di settori diversi. La validazione futura si concentrerà su: - Correlazione tra punteggi CPF e incidenti di sicurezza reali - Accuratezza predittiva del framework - Applicabilità inter-settoriale - Fattori culturali e organizzativi. Stiamo cercando attivamente organizzazioni partner per implementazioni pilota. Le parti interessate

4.2 Limitazioni

- Campione di piccole dimensioni limita la generalizzabilità
- Periodo di osservazione insufficiente per eventi rari
- Fattori culturali non completamente considerati
- Possibile influenza dell'effetto Hawthorne

5 Discussione

5.1 Implicazioni Teoriche

Il CPF valida l'applicazione dei concetti psicoanalitici alla cybersecurity, dimostrando che i processi inconsci influenzano significativamente gli esiti di sicurezza. Il successo del framework suggerisce che:

1. **I processi pre-cognitivi dominano le decisioni di sicurezza** – Supportando i risultati di Libet in un contesto cyber
2. **Le dinamiche di gruppo creano vulnerabilità sistematiche** – Confermando che le assunzioni di base di Bion operano negli ambienti digitali
3. **Le relazioni oggettuali influenzano la percezione delle minacce** – Il meccanismo di scissione di Klein spiega i punti ciechi di sicurezza

4. **L'IA introduce nuove vulnerabilità psicologiche** – Richiedendo nuovi framework teorici

5.2 Applicazioni Pratiche

5.2.1 Integrazione nel Security Operations Center (SOC)

- Punteggi CPF come intelligence delle minacce aggiuntiva
- Monitoraggio dello stato psicologico insieme agli indicatori tecnici
- Punteggio dinamico del rischio basato sulla psicologia organizzativa

5.2.2 Miglioramento della Risposta agli Incidenti

- Pre-posizionamento delle risorse basato sugli stati di vulnerabilità
- Protocolli di risposta personalizzati per le condizioni psicologiche
- Pianificazione del recupero psicologico post-incidente

5.2.3 Evoluzione della Consapevolezza della Sicurezza

- Muoversi oltre il trasferimento di informazioni verso l'intervento psicologico
- Affrontare la resistenza inconscia alle misure di sicurezza
- Interventi a livello di gruppo piuttosto che individuale

5.3 Considerazioni Etiche

Preoccupazioni sulla Privacy:

- Rischio di "sorveglianza psicologica"
- Potenziale discriminazione basata sugli stati psicologici
- Necessità di framework di governance rigorosi

Consenso e Trasparenza:

- Comunicazione chiara sui metodi di valutazione
- Meccanismi di opt-out mantenendo la validità statistica
- Audit regolari dell'uso dei dati

Dinamiche di Potere:

- Prevenire l'armamento contro i dipendenti
- Garantire la sicurezza psicologica durante le valutazioni
- Protezione per i whistleblower che identificano vulnerabilità

5.4 Direzioni Future

1. **Integrazione del Machine Learning**
    - Riconoscimento di pattern negli stati psicologici
    - Raffinamento della modellazione predittiva
    - Sistemi automatizzati di allarme precoce
2. **Adattamento Culturale**
    - Studi di validazione cross-culturale
    - Pattern di vulnerabilità localizzati
    - Fattori psicologici globali vs. locali
3. **Sforzi di Standardizzazione**
    - Integrazione con framework NIST/ISO
    - Personalizzazioni specifiche per settore
    - Sviluppo di programma di certificazione
4. **Studi Longitudinali**
    - Tracciamento multi-annuale dei pattern psicologici
    - Misurazione dell'efficacia degli interventi
    - Effetti di apprendimento organizzativo

6 Conclusione

Il Framework di Psicologia della Cybersecurity rappresenta un cambio di paradigma nella comprensione e nell'affrontare i fattori umani nella cybersecurity. Integrando la teoria psicoanalitica con la psicologia cognitiva ed estendendo alle vulnerabilità specifiche dell'IA, il CPF fornisce un approccio scientificamente fondato per predire e prevenire gli incidenti di sicurezza prima che si verifichino.

Il framework teorico dimostra che gli stati psicologici pre-cognitivi dovrebbero correlarsi fortemente con gli esiti di sicurezza, supportando le fondamenta del framework. Il design che preserva la privacy e agnostico all'implementazione consente la distribuzione pratica affrontando le preoccupazioni etiche.

Mentre le organizzazioni affrontano minacce sempre più sofisticate che sfruttano la psicologia umana, framework come il CPF diventano essenziali. La sfida non è più puramente tecnica ma fondamentalmente psicologica. I professionisti della sicurezza devono espandere la loro competenza oltre la tecnologia per includere la comprensione dei processi inconsci, delle dinamiche di gruppo e della complessa interazione tra intelligenza umana e artificiale.

Il lavoro futuro si concentrerà su implementazioni pilota con organizzazioni partner, integrazione del machine learning e sviluppo di strategie di intervento basate sulle vulnerabilità identificate. Invitiamo alla collaborazione sia dalle comunità di cybersecurity che di psicologia per raffinare e validare questo approccio.

L'obiettivo finale del CPF non è eliminare la vulnerabilità umana—un compito impossibile—ma comprenderla e considerarla nelle nostre strategie di sicurezza. Solo riconoscendo la realtà psicologica della vita organizzativa possiamo costruire posture di sicurezza veramente resilienti.

Ringraziamenti

L'autore ringrazia le comunità di cybersecurity e psicologia per il loro dialogo continuo sui fattori umani nella sicurezza.

Biografia dell'Autore

Giuseppe Canale è un professionista della cybersecurity certificato CISSP con formazione specializzata in teoria psicoanalitica (Bion, Klein, Jung, Winnicott) e psicologia cognitiva (Kahneman, Cialdini). Combina 27 anni di esperienza nella cybersecurity con una profonda comprensione dei processi inconsci e delle dinamiche di gruppo per sviluppare approcci innovativi alla sicurezza organizzativa.

Dichiarazione sulla Disponibilità dei Dati

Dati aggregati anonimizzati disponibili su richiesta, soggetti a vincoli di privacy.

Conflitto di Interessi

L'autore dichiara di non avere conflitti di interesse.

A Strumento di Valutazione CPF - Campione

Lo strumento di valutazione completo è in fase di sviluppo e sarà reso disponibile dopo la validazione pilota.

B Verifica Timestamp Blockchain

La versione del framework CPF descritta in questo articolo è stata timestampata su blockchain per la protezione della proprietà intellettuale e il controllo versione:

- **Piattaforma**: OpenTimestamps.org
- **Hash**: dfb55fc21e1b204c342aa76145f1329fa6f095ceddc3aad8486dca91a580fa96
- **Block Height**: 909232
- **Transaction ID**: dfb55fc21e1b204c342aa76145f1329fa6f095
- ceddc3aad8486dca91a580fa9693a7e6d57f08942718b80ccda74d9f74
- **Timestamp**: 2025-08-09 CET

Riferimenti bibliografici

[1] Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, 50(2), 179-211.

[2] Beautement, A., Sasse, M. A., & Wonham, M. (2008). The compliance budget: Managing security behaviour in organisations. *Proceedings of NSPW*, 47-58.

[3] Bion, W. R. (1961). *Experiences in groups*. London: Tavistock Publications.

[4] Bowlby, J. (1969). *Attachment and Loss: Vol. 1. Attachment*. New York: Basic Books.

[5] Cialdini, R. B. (2007). *Influence: The psychology of persuasion*. New York: Collins.

[6] Damasio, A. (1994). *Descartes' error: Emotion, reason, and the human brain*. New York: Putnam.

[7] Gartner. (2023). *Forecast: Information Security and Risk Management, Worldwide, 2021-2027*. Gartner Research.

[8] Jung, C. G. (1969). *The Archetypes and the Collective Unconscious*. Princeton: Princeton University Press.

[9] Kahneman, D. (2011). *Thinking, fast and slow*. New York: Farrar, Straus and Giroux.

[10] Kahneman, D., & Tversky, A. (1979). Prospect theory: An analysis of decision under risk. *Econometrica*, 47(2), 263-291.

[11] Kernberg, O. (1998). *Ideology, conflict, and leadership in groups and organizations*. New Haven: Yale University Press.

[12] Klein, M. (1946). Notes on some schizoid mechanisms. *International Journal of Psychoanalysis*, 27, 99-110.

[13] LeDoux, J. (2000). Emotion circuits in the brain. *Annual Review of Neuroscience*, 23, 155-184.

[14] Libet, B., Gleason, C. A., Wright, E. W., & Pearl, D. K. (1983). Time of conscious intention to act in relation to onset of cerebral activity. *Brain*, 106(3), 623-642.

[15] Menzies Lyth, I. (1960). A case-study in the functioning of social systems as a defence against anxiety. *Human Relations*, 13, 95-121.

[16] Milgram, S. (1974). *Obedience to authority*. New York: Harper & Row.

[17] Miller, G. A. (1956). The magical number seven, plus or minus two. *Psychological Review*, 63(2), 81-97.

[18] SANS Institute. (2023). *Security Awareness Report 2023*. SANS Security Awareness.

[19] Selye, H. (1956). *The stress of life*. New York: McGraw-Hill.

[20] Soon, C. S., Brass, M., Heinze, H. J., & Haynes, J. D. (2008). Unconscious determinants of free decisions in the human brain. *Nature Neuroscience*, 11(5), 543-545.

[21] Verizon. (2023). *2023 Data Breach Investigations Report*. Verizon Enterprise.

[22] Winnicott, D. W. (1971). *Playing and reality*. London: Tavistock Publications.