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

Una Prestampa

Giuseppe Canale, CISSP
Ricercatore Indipendente
kaolay@gmail.com, g.canale@cpf3.org
URL: cpf3.org
ORCID: 0009-0007-3263-6897

November 18, 2025

Abstract

Presentiamo il Cybersecurity Psychology Framework (CPF), un innovativo modello interdisciplinare che identifica le vulnerabilità pre-cognitive nelle posture di security organizzative attraverso l'integrazione sistematica della teoria psicoanalitica e della psicologia cognitiva. A differenza degli approcci tradizionali di consapevolezza della security che si concentrano sul processo decisionale cosciente, CPF mappa gli stati psicologici inconsci e le dinamiche di gruppo a vettori di attacco specifici, consentendo strategie di security predittive piuttosto che reattive. Il framework comprende 100 indicatori attraverso 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. 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 di security.

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

1 Introduzione

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

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

Il Cybersecurity Psychology Framework (CPF) colma questa lacuna fornendo la prima integrazione sistematica di:

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

Questo documento presenta il fondamento teorico di CPF, la progettazione architetturale e la roadmap per futuri studi di validazione.

2 Fondamento Teorico

2.1 Il Fallimento degli Interventi a Livello Cosciente

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

Evidenza Neuroscientifica:

- Gli studi fMRI mostrano che l'attivazione dell'amigdala (risposta alla minaccia) si verifica prima dell'impegno della corteccia prefrontale (analisi razionale)[13]
- Il processo decisionale coinvolge marcatori somatici che bypassano l'elaborazione cosciente[6]

Evidenza dall'Economia Comportamentale:

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

Evidenza Psicoanalitica:

- Le organizzazioni sviluppano "sistemi di difesa sociale" contro l'ansia che creano punti ciechi nella security[15]
- La proiezione delle minacce interne su "hacker" esterni impedisce il riconoscimento dei rischi insider[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)**: Ricerca di un leader/tecnologia onnipotente per la protezione
- **Attacco-Fuga (baF)**: Percezione delle minacce come nemici esterni che richiedono difesa aggressiva o evitamento
- **Accoppiamento (baP)**: Speranza di salvezza futura attraverso nuove soluzioni

Nei contesti di cybersecurity, queste si manifestano come:

- **baD**: Eccessivo affidamento su fornitori di security/soluzioni "proiettile d'argento"
- **baF**: Difesa perimetrale aggressiva ignorando le minacce insider
- **baP**: Acquisizione continua di tool senza affrontare le vulnerabilità fondamentali

2.2.2 Relazioni Oggettuali Kleiniane

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

- Insider fidati (idealizzati) vs. aggressori esterni (demonizzati)
- Sistemi legacy (familiari/buoni) vs. nuovi requisiti di security (minacciosi/cattivi)
- Proiezione delle vulnerabilità organizzative su "aggressori 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 test di realtà negli ambienti virtuali
- Confusione tra identità digitale e sé
- Fantasie onnipotenti nel cyberspazio

2.2.4 L'Ombra e la Proiezione Junghiana

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

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

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

Limitazioni del Sistema 2:

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

2.3.2 I Principi di Influenza di Cialdini nel Contesto Cyber

I sei principi di Cialdini[5] si mappano direttamente sui vettori di ingegneria sociale:

1. **Reciprocità**: Attacchi quid pro quo
2. **Impegno/Coerenza**: Escalation graduale delle richieste
3. **Prova sociale**: "Tutti cliccano questo link"
4. **Autorità**: Frodi CEO, falso supporto IT
5. **Simpatia**: Costruzione del rapporto 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:

- Compromessi tra complessità e memorizzabilità delle password
- Affaticamento da alert dalla proliferazione di tool di security
- Paralisi decisionale da troppe opzioni di security

2.4 Vulnerabilità Psicologiche Specifiche dell'IA

Man mano che i sistemi IA diventano parte integrante delle operazioni di security, emergono nuove vulnerabilità psicologiche:

2.4.1 Antropomorfizzazione

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

2.4.2 Automation Bias

- Eccessivo affidamento sugli strumenti di security automatizzati
- Ridotta vigilanza umana ("moral hazard")
- Atrofia delle competenze nei team di security

2.4.3 Effetti di Trasferimento IA-Umano

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

3 L'Architettura del Modello CPF

3.1 Principi di Progettazione

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. **Implementazione Agnostica**: Si mappa alle vulnerabilità, non a soluzioni specifiche
4. **Fondamento Scientifico**: Ogni indicatore collegato a ricerca consolidata
5. **Praticità Operativa**: Punteggio ternario per insight attuabili

3.2 Struttura del Framework

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

Table 1: Categorie Primarie CPF e Fondamenti Teorici

Codice	Categoria	Riferimento Primario
[1.x]	Vulnerabilità Basate sull'Autorità	Milgram (1974)
[2.x]	Vulnerabilità Temporali	Kahneman & Tversky (1979)
[3.x]	Vulnerabilità da Influenza Sociale	Cialdini (2007)
[4.x]	Vulnerabilità Affettive	Klein (1946), Bowlby (1969)
[5.x]	Vulnerabilità da Sovraccarico Cognitivo	Miller (1956)
[6.x]	Vulnerabilità delle Dinamiche di Gruppo	Bion (1961)
[7.x]	Vulnerabilità da Risposta allo Stress	Selye (1956)
[8.x]	Vulnerabilità dei Processi Inconsci	Jung (1969)
[9.x]	Vulnerabilità da 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 senza domande all'autorità apparente

1.2 Diffusione della responsabilità nelle strutture gerarchiche

1.3 Suscettibilità all'impersonificazione di figure di autorità

1.4 Bypass della security per convenienza del superiore

1.5 Conformità basata sulla paura senza verifica

1.6 Gradiente di autorità che inibisce la segnalazione di security

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 in crisi

3.2.2 Dettaglio Categoria: Vulnerabilità Temporali [2.x]

2.1 Bypass della security indotto dall'urgenza

2.2 Degradazione cognitiva per pressione temporale

2.3 Accettazione del rischio guidata dalle scadenze

2.4 Present bias negli investimenti di security

2.5 Sconto iperbolico delle minacce future

2.6 Pattern di esaurimento temporale

2.7 Finestre di vulnerabilità basate sull'ora del giorno

2.8 Lacune di security nei weekend/festività

2.9 Finestre di sfruttamento al cambio turno

2.10 Pressione di coerenza temporale

3.2.3 Dettaglio Categoria: Vulnerabilità da 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 basato sulla simpatia

3.5 Decisioni guidate dalla scarsità

3.6 Sfruttamento del principio di unità

3.7 Conformità alla 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 della fiducia ai sistemi

4.4 Attaccamento ai sistemi legacy

4.5 Occultamento della security basato sulla vergogna

4.6 Iperconformità guidata dal senso di colpa

4.7 Errori innescati dall'ansia

4.8 Negligenza correlata alla depressione

4.9 Incuria indotta dall'euforia

4.10 Effetti di contagio emotivo

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

5.1 Desensibilizzazione da affaticamento degli alert

5.2 Errori da affaticamento decisionale

5.3 Paralisi da sovraccarico informativo

5.4 Degradazione da multitasking

5.5 Vulnerabilità da 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 della security da groupthink

6.2 Fenomeni di spostamento rischioso

6.3 Diffusione della responsabilità

6.4 Social loafing nei compiti di security

6.5 Effetto spettatore nella risposta agli incidenti

6.6 Assunzioni di gruppo di dipendenza

6.7 Posture di security attacco-fuga

6.8 Fantasie di speranza nell'accoppiamento

6.9 Scissione organizzativa

6.10 Meccanismi di difesa collettivi

3.2.7 Dettaglio Categoria: Vulnerabilità da 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 Iperconformità da risposta di compiacimento

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 aggressori

8.2 Identificazione inconscia con le minacce

8.3 Pattern di compulsione alla ripetizione

8.4 Transfert verso figure di autorità

8.5 Punti ciechi da controtransfert

8.6 Interferenza dei meccanismi di difesa

8.7 Confusione dell'equazione simbolica

8.8 Trigger di attivazione archetipica

8.9 Pattern dell'inconscio collettivo

8.10 Logica onirica negli spazi digitali

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

9.1 Antropomorfizzazione dei sistemi IA

9.2 Override del bias di automazione

9.3 Paradosso dell'avversione agli algoritmi

9.4 Trasferimento di autorità all'IA

9.5 Effetti della valle perturbante

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 non ritorno

10.4 Allineamento del formaggio svizzero

10.5 Cecità al cigno nero

10.6 Negazione del rinoceronte grigio

10.7 Catastrofe della complessità

10.8 Imprevedibilità emergente

10.9 Fallimenti di accoppiamento del sistema

10.10 Gap di security da 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 proposti di raccolta dati daranno priorità alle tecniche di preservazione della 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 ritardato nel tempo: minimo 72 ore
- Analisi basata sui ruoli piuttosto che individuale
- Traccia di audit per tutti gli accessi ai dati

3.4 Mappatura dei Vettori di Attacco

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

Table 2: Mappatura da Vulnerabilità a Vettore di Attacco

Categoria Vulnerabilità	Vettori di Attacco Primari
Autorità	Spear Phishing, Frode CEO
Temporali	Attacchi a Scadenza, Malware Time-bomb
Sociale	Ingegneria Sociale, Minacce Insider
Affettive	Campagne FUD, Ransomware
Sovraccarico Cognitivo	Sfruttamento Affaticamento Alert
Dinamiche Gruppo	Interruzione Organizzativa
Stress	Sfruttamento Burnout
Inconsci	Attacchi Simbolici
Bias IA	ML Adversarial, Poisoning
Convergenti	Advanced Persistent Threats

4 Studi di Validazione

4.1 Panoramica Implementazione Pilota

Il framework CPF è attualmente nella fase di sviluppo teorico. Le implementazioni pilota sono in fase di pianificazione con organizzazioni di diversi settori. La validazione futura si concentrerà su: - Correlazione tra punteggi CPF e incidenti di security effettivi - Accuratezza predittiva del framework - Applicabilità intersettoriale - Fattori culturali e organizzativi. Stiamo attivamente cercando organizzazioni partner per implementazioni pilota. Le parti interessate possono contattare l'autore per opportunità di collaborazione.

4.2 Limitazioni

- Dimensione campione ridotta 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

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

1. **I processi pre-cognitivi dominano le decisioni di security** – 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 della security

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

5.2 Applicazioni Pratiche

5.2.1 Integrazione Security Operations Center (SOC)

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

5.2.2 Miglioramento della Risposta agli Incidenti

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

5.2.3 Evoluzione della Consapevolezza della Security

- Andare oltre il trasferimento di informazioni all'intervento psicologico
- Affrontare la resistenza inconscia alle misure di security
- Interventi a livello di gruppo piuttosto che individuali

5.3 Considerazioni Etiche

Preoccupazioni sulla Privacy:

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

Consenso e Trasparenza:

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

Dinamiche di Potere:

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

5.4 Direzioni Future

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

6 Conclusione

Il Cybersecurity Psychology Framework rappresenta un cambiamento di paradigma nella comprensione e nell'affrontare i fattori umani nella cybersecurity. Integrando la teoria psicoanalitica con la psicologia cognitiva ed estendendosi alle vulnerabilità specifiche dell'IA, CPF fornisce un approccio scientificamente fondato per prevedere e prevenire gli incidenti di security prima che si verifichino.

Il framework teorico dimostra che gli stati psicologici pre-cognitivi dovrebbero correlare fortemente con gli esiti di security, supportando le fondamenta del framework. Il design che preserva la privacy e indipendente dall'implementazione consente il deployment pratico affrontando le preoccupazioni etiche.

Man mano che le organizzazioni affrontano minacce sempre più sofisticate che sfruttano la psicologia umana, framework come CPF diventano essenziali. La sfida non è più puramente tecnica ma fondamentalmente psicologica. I professionisti della security devono espandere la loro expertise 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 la collaborazione sia dalle comunità di cybersecurity che di psicologia per raffinare e validare questo approccio.

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

Nota sulla Composizione Assistita dall'IA

Questo manoscritto presenta il framework teorico originale e i contributi intellettuali dell'autore. Nel processo di composizione e formattazione, l'autore ha utilizzato un large language model (LLM) come strumento ausiliario per compiti specifici:

- **Refactoring Stilistico:** Riformulazione delle frasi per migliorare chiarezza e fluidità in inglese.
- **Assistenza alla Formattazione:** Aiuto nell'applicazione coerente della sintassi LaTeX per liste puntate, tabelle e riferimenti incrociati.

È fondamentale sottolineare che:

- L'idea centrale, la tassonomia CPF, la selezione e definizione di tutti gli indicatori, l'integrazione teorica e l'analisi complessiva sono esclusivamente il prodotto dell'expertise e dello sforzo intellettuale dell'autore.
- L'LLM non ha generato idee, concetti o conclusioni nuove. Il suo ruolo è stato limitato all'assistenza nella riformulazione e formattazione sotto la stretta direzione e revisione continua dell'autore.
- L'autore è interamente responsabile dell'accuratezza, validità e integrità del contenuto pubblicato.

Ringraziamenti

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

Biografia Autore

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

Dichiarazione sulla Disponibilità dei Dati

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

Conflitto di Interessi

L'autore dichiara l'assenza di conflitti di interesse.

A Campione di Strumento di Valutazione CPF

Lo strumento completo di valutazione 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 documento è stata marcata temporalmente su blockchain per la protezione della proprietà intellettuale e il controllo versione:

- **Piattaforma**: OpenTimestamps.org
- **Hash**: dfb55fc21e1b204c342aa76145f1329fa6f095ceddc3aad8486dca91a580fa96
- **Altezza Blocco**: 909232
- **ID Transazione**: dfb55fc21e1b204c342aa76145f1329fa6f095
- ceddc3aad8486dca91a580fa9693a7e6d57f08942718b80ccda74d9f74
- **Timestamp**: 2025-08-09 CET

References

[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.