Riconoscimento Pattern CPF: Elenco Esempi Tecnici

Contents

PATTERN TEMPORALI [2.x]

Pattern: Curva di Procrastinazione delle Patch

Dati: Età CVE al momento del patching: 0-10 giorni (5%), 11-30 giorni (10%), 31-90 giorni (20%), >90 giorni (65%) **Stato**: Sconto iperbolico - minacce future percepite come astratte **Predizione**: Violazione via CVE di 60-90 giorni (punto ottimale tra conoscenza attaccante e negazione organizzativa)

Pattern: Risposta di Panico al PoC

Dati: Velocità patching pre-PoC: 0,5 patch/giorno, Post-PoC: 15 patch/giorno per 48 ore, poi ritorno a 0,5 **Stato**: Ciclo di sicurezza maniaco-depressivo, verifica della realtà solo durante fase maniacale **Predizione**: Vulnerabile a minacce senza PoC pubblico per finestre di 28 giorni tra cicli di panico

Pattern: Dissolvenza del Venerdì

Dati: Tasso successo patch Lunedì: 94%, Martedì-Giovedì: 91%, Venerdì: 67%, Venerdì dopo le 15:00: 41% **Stato**: Dissoluzione del super-io nel tempo liminale, deplezione dell'ego **Predizione**: Successo spear phishing 3x superiore Venerdì 14-17

Pattern: Picchi Guidati dagli Audit

Dati: Tasso patch normale: 10/settimana, Settimana pre-audit: 180/settimana, Post-audit: 2/settimana per 30 giorni **Stato**: Ansia da prestazione con collasso post-audit **Predizione**: Massima vulnerabilità 15-45 giorni post-audit

Pattern: Finestre di Vulnerabilità Festive

Dati: CVE critici non patchati aumentano del 400% dal 20 dic al 5 gen **Stato**: Assenza psicologica collettiva, inconscio organizzativo dormiente **Predizione**: Stabilimento di persistenza APT durante periodi festivi

Pattern: Decadimento Time-to-Patch

Dati: Mese 1: media 3 giorni, Mese 6: media 18 giorni, Mese 12: media 45 giorni **Stato**: Deplezione cronica dell'ego che porta a impotenza appresa **Predizione**: Violazione critica entro 90 giorni quando il decadimento supera media di 30 giorni

PATTERN DI AUTORITÀ [1.x]

Pattern: Sindrome dell'Eccezione Esecutiva

Dati: Sistemi C-suite: 89% vulnerabilità non patchate, Staff generale: 23% non patchate **Stato**: Dinamiche edipiche - impossibilità di sfidare i sistemi della figura paterna **Predizione**: Attacchi

CEO fraud/whaling avranno successo via sistemi esecutivi

Pattern: Deferenza verso i Vendor

Dati: Patch da Microsoft: media 48h, da vendor piccoli: 180+ giorni o mai **Stato**: Transfert di autorità verso grandi vendor come figure genitoriali **Predizione**: Attacchi supply chain via software di vendor piccoli

Pattern: Gerarchia di Override degli Alert

Dati: Alert di sicurezza ignorati: da staff junior (2%), da manager (31%), da executive (94%) **Stato**: Gradiente di autorità sovrasta la realtà tecnica **Predizione**: Minaccia insider da account privilegiati non rilevata

Pattern: Teatro della Conformità

Dati: Patch pre-visita-auditor: 200, Patch regolari: 10/mese **Stato**: Proiezione del super-io sugli auditor, performance per l'autorità **Predizione**: Vulnerabilità reali nascoste, fix cosmetici prominenti

PATTERN DI SPLITTING [4.x]

Pattern: Sistema Buono/Sistema Cattivo

Dati: CRM legacy: 0 patch in 2 anni, Nuovo ERP: ogni patch entro 24 ore **Stato**: Splitting - CRM è "oggetto buono" che non può essere cattivo **Predizione**: Violazione via CRM legacy, organizzazione negherà che fosse vulnerabile

Pattern: Divisione Interno/Esterno

Dati: Rete interna: 1.200 CVE non patchati, DMZ: 3 CVE non patchati **Stato**: Proiezione di tutto il pericolo sul perimetro, interno = sicuro **Predizione**: Movimento laterale banale una volta violato il perimetro

Pattern: Favoritismo Dipartimentale

Dati: Server vendite: 5% vulnerabili, Server IT: 78% vulnerabili **Stato**: IT come "oggetto cattivo" contenente l'ansia organizzativa **Predizione**: Infrastruttura IT usata come punto di pivot dagli attaccanti

Pattern: Stati di Sicurezza Binari

Dati: Sistemi o 100% patchati o 0% patchati, nessuna via di mezzo **Stato**: Incapacità di mantenere posizione ambivalente, difesa tutto-o-niente **Predizione**: Sistemi "abbandonati" diventano punti di persistenza

PATTERN DI COAZIONE A RIPETERE [8.x]

Pattern: Il CVE che Ritorna

Dati: Stesso CVE di SQL injection patchato 6 volte in 18 mesi, riappare ogni volta **Stato**: Coazione a ripetere intorno a trauma specifico **Predizione**: Questo esatto CVE sarà vettore di violazione nonostante consapevolezza

Pattern: Esposizione Ciclica

Dati: Porta 445 chiusa → riaperta → chiusa → riaperta su ciclo di 90 giorni **Stato**: Ritorno inconscio allo stato vulnerabile **Predizione**: Attacco ha successo durante fase "aperta" del ciclo

Pattern: Deriva Ricorrente della Configurazione

Dati: Hardening sicurezza applicato → degrada → riapplicato ogni 4 mesi **Stato**: Ripetizione organizzativa del ciclo sicurezza/insicurezza **Predizione**: Violazione durante fase di degradazione mese 3

Pattern: Loop Patch-Rollback

Dati: Patch critica applicata → problemi sistema → rollback → attesa → ripeti (5x) **Stato**: Ripetizione compulsiva evitando conflitto centrale **Predizione**: Vulnerabilità permanente, organizzazione non può risolvere

PATTERN DI DINAMICA DI GRUPPO [6.x]

Pattern: Cluster di Shadow IT

Dati: Marketing: 47 app cloud non autorizzate, Finanza: 52, IT: 0 **Stato**: Dipartimenti in attacco-fuga contro autorità IT **Predizione**: Ingresso ransomware via SaaS non autorizzato

Pattern: Patching di Gregge

Dati: Nessuna patch per settimane, poi 80% dei sistemi patchati in 2 ore **Stato**: Pensiero di gruppo, nessun processo decisionale individuale **Predizione**: Patch critiche mancate che non sono "di tendenza"

Pattern: Diffusione di Responsabilità

Dati: Sistemi condivisi: 92% vulnerabili, Sistemi a proprietario singolo: 31% vulnerabili **Stato**: Effetto spettatore in forma digitale **Predizione**: Infrastruttura condivisa diventa percorso di attacco

Pattern: Proliferazione di Strumenti di Sicurezza

Dati: 47 strumenti di sicurezza diversi, 12% funzionalità utilizzate **Stato**: Accumulo maniacale come difesa contro l'ansia **Predizione**: Cecità agli alert, attacchi reali persi nel rumore

PATTERN DI SOVRACCARICO COGNITIVO [5.x]

Pattern: Curva di Affaticamento da Alert

Dati: Settimana 1: 94% alert investigati, Settimana 12: 31%, Settimana 24: 8% **Stato**: Esaurimento cognitivo progressivo **Predizione**: Attacchi reali ignorati come falsi positivi dopo settimana 20

Pattern: Paralisi da Complessità

Dati: Sistemi con <10 CVE: 89% patchati, >100 CVE: 12% patchati **Stato**: Paralisi decisionale da sovraccarico di scelta **Predizione**: Sistemi complessi rimangono permanentemente vulnerabili

Pattern: Confusione da Proliferazione Strumenti

Dati: 5+ strumenti di scansione mostrano risultati diversi, tasso patch: 15% degli identificati **Stato**: Dissonanza cognitiva da informazioni contrastanti **Predizione**: Paralisi da analisi, nessuna azione intrapresa

Pattern: Inversione di Priorità

Dati: CVE bassi patchati: 78%, CVE critici patchati: 34% **Stato**: Sovraccarico cognitivo causa selezione casuale invece che razionale **Predizione**: Violazione via CVE critici noti

PATTERN DI RISPOSTA ALLO STRESS [7.x]

Pattern: Decadimento Risposta agli Incidenti

Dati: 1° incidente: risoluzione 4h, 5° incidente stesso mese: risoluzione 47h **Stato**: Degradazione risposta stress acuto **Predizione**: Persistenza attaccante se innescati incidenti multipli

Pattern: Errori da Panic Patching

Dati: Patch emergenza: 34% causano guasti sistema vs 3% per patch pianificate **Stato**: Risposta attacco-fuga sovrasta processo accurato **Predizione**: Attaccanti sfruttano sistemi rotti post-panic-patch

Pattern: Segnale di Turnover Team Sicurezza

Dati: Qualità patch cala 60% nel mese prima partenza staff sicurezza **Stato**: Ritiro inconscio prima di decisione cosciente **Predizione**: Finestra vulnerabilità 90 giorni intorno a cambi di staff

Pattern: Pattern Matching Cortisolo

Dati: Lunedì mattina: alti falsi positivi, Venerdì pomeriggio: veri positivi mancati **Stato**: Cicli ormoni stress influenzano percezione **Predizione**: Attacchi reali mancati in periodi alto stress

PATTERN DI ATTACCAMENTO [4.x]

Pattern: Attaccamento a Sistema Legacy

Dati: Macchina Windows XP: 847 giorni senza patch, ancora in produzione **Stato**: Attaccamento a oggetto transizionale, impossibilità di separazione **Predizione**: Questo sistema specifico sarà punto di violazione

Pattern: Cecità da Fedeltà allo Strumento

Dati: Continua uso strumento compromesso per 180+ giorni dopo notifica violazione vendor **Stato**: Fallimento costanza oggetto, impossibilità vedere oggetto buono come cattivo **Predizione**: Compromissione supply chain via strumento fidato

Pattern: Attaccamento alla Password

Dati: Stesso pattern password rilevato su 89% dei sistemi nonostante policy **Stato**: Comportamento coperta di sicurezza, comfort nella familiarità **Predizione**: Attacchi password spray hanno successo

PATTERN DI INTERAZIONE AI [9.x]

Pattern: Overdipendenza dall'AI

Dati: Tasso revisione manuale: Pre-AI: 73%, Post-AI: 11% **Stato**: Transfert materno verso AI come caregiver **Predizione**: Falsi negativi suggeriti da AI diventano violazioni

Pattern: Fiducia Antropomorfica

Dati: Raccomandazioni AI seguite 94%, Raccomandazioni esperto umano: 67% **Stato**: AI come figura genitoriale idealizzata **Predizione**: Input AI avversariali accettati senza domande

Pattern: Zona Comfort Automazione

Dati: Patch automatizzate: 91% successo, Intervento manuale quando automazione fallisce: 8% **Stato**: Impotenza appresa quando AI non disponibile **Predizione**: Fallimenti durante downtime AI diventano violazioni

PATTERN DI IDENTIFICAZIONE INCONSCIA [8.x]

Pattern: Segnale di Ammirazione per Hacker

Dati: Team sicurezza legge forum attaccanti 3+ ore/giorno, patch calano 40% **Stato**: Identificazione inconscia con aggressore **Predizione**: Minaccia insider o abilitazione inconscia

Pattern: Identificazione con Vittima

Dati: Aziende post-violazione menzionate 10x di più in discussioni sicurezza **Stato**: Identificazione con organizzazioni vittime **Predizione**: Ricreare inconsciamente vulnerabilità simili

Pattern: Performance Teatro Sicurezza

Dati: Misure sicurezza visibili: 100% implementate, invisibili: 20% implementate **Stato**: Performance sicurezza per pubblico immaginario **Predizione**: Violazione via vulnerabilità non visibili

PATTERN DI NEGAZIONE [8.x]

Pattern: Gioco di Rinomina Vulnerabilità

Dati: Vuln critiche riclassificate come "medie" senza base tecnica: 67% **Stato**: Distorsione realtà per ridurre ansia **Predizione**: CVE classificati "medi" diventano vettori di violazione

Pattern: Inflazione Falsi Positivi

Dati: 70% di veri positivi marcati come falsi dopo rilevamento iniziale **Stato**: Negazione attraverso misclassificazione **Predizione**: Attacchi reali marcati come falsi positivi

Pattern: Accelerazione Accettazione Rischi

Dati: Mese 1: 0 rischi accettati, Mese 12: 847 rischi accettati senza revisione **Stato**: Negazione progressiva della realtà minaccia **Predizione**: Rischi accettati diventano violazioni effettive

PATTERN MERGER/ACQUISIZIONE

Pattern: Frammentazione Post-Merger

Dati: Sistemi azienda acquisita: 90% non patchati dopo 180 giorni **Stato**: Splitting organizzativo, rifiuto di corpo estraneo **Predizione**: Violazione via infrastruttura acquisita

Pattern: Paralisi da Crisi di Identità

Dati: Velocità patch cala 75% durante merger **Stato**: Confusione identità organizzativa **Predizione**: Finestra vulnerabilità 6 mesi durante integrazione

PATTERN DI CONFINE

Pattern: Fissazione sul Perimetro

Dati: Sistemi perimetrali: 99% patchati, Interni: 23% patchati **Stato**: Confine come contenitore per tutta l'ansia **Predizione**: Movimento laterale interno banale

Pattern: Proliferazione Eccezioni VPN

Dati: Eccezioni VPN crescono 300% in 12 mesi **Stato**: Dissoluzione confini, confusione dentro/fuori **Predizione**: VPN diventa vettore di attacco primario

PATTERN DI PROIEZIONE [8.x]

Pattern: Preparazione Colpa Vendor

Dati: Documentazione problemi vendor: 500 pagine, problemi interni: 3 pagine **Stato**: Proiezione fallimenti interni su vendor **Predizione**: Misconfigurazioni interne causano violazione, vendor incolpato

Pattern: Fantasia di Attribuzione

Dati: Ogni incidente attribuito ad "APT" indipendentemente dalla semplicità **Stato**: Proiezione competenza sugli attaccanti **Predizione**: Attacchi base hanno successo mentre si cercano minacce avanzate

PATTERN NARCISISTICI

Pattern: Sindrome del Fiocco di Neve Speciale

Dati: "Il nostro ambiente è unico" usato per evitare 78% standard sicurezza **Stato**: Eccezionalismo narcisistico **Predizione**: Attacchi standard funzionano nonostante "unicità"

Pattern: Manipolazione Metriche Sicurezza

Dati: Metriche mostrano miglioramento mentre vulnerabilità aumentano **Stato**: Presentazione falso sé narcisistico **Predizione**: Violazione durante periodo "migliori metriche"

PATTERN DI RISPOSTA AL TRAUMA

Pattern: Paralisi Post-Violazione

Dati: Patching si ferma completamente per 30-60 giorni dopo violazione **Stato**: Risposta di congelamento traumatico **Predizione**: Seconda violazione durante periodo di paralisi

Pattern: Esaurimento da Ipervigilanza

Dati: Post-incidente: aumento 1000% in alert, poi crash completo **Stato**: Ciclo risposta trauma **Predizione**: Vulnerabilità durante fase esaurimento

PATTERN DI REGRESSIONE

Pattern: Regressione da Crisi

Dati: Durante crisi: ritorno a configurazioni sicurezza di 2 anni prima **Stato**: Regressione organizzativa a stadio evolutivo precedente **Predizione**: Vecchie vulnerabilità riappaiono durante stress

Pattern: Emergenza Pensiero Magico

Dati: "Sicurezza per oscurità" ritorna nonostante formazione **Stato**: Regressione a pensiero magico sotto pressione **Predizione**: Assunzioni oscurità portano a esposizione

PATTERN DI DISSOCIAZIONE

Pattern: Amnesia di Sicurezza

Dati: Stessi incidenti sicurezza "scoperti" multiple volte come "nuovi" **Stato**: Dissociazione organizzativa da memorie minacciose **Predizione**: Lezioni non apprese portano a violazioni ripetute

Pattern: Dissociazione da Alert

Dati: Alert critici riconosciuti ma nessuna memoria di essi in seguito **Stato**: Difesa dissociativa contro minaccia schiacciante **Predizione**: Attacchi noti hanno successo nonostante alert