CPF Pattern Recognition: Technical Examples List

TEMPORAL PATTERNS [2.x]

Pattern: Patch Procrastination Curve

Data: CVE age at patch time: 0-10 days (5%), 11-30 days (10%), 31-90 days (20%), >90 days (65%) **State**: Hyperbolic discounting - future threats perceived as abstract **Prediction**: Breach via CVEs aged 60-90 days (sweet spot of attacker knowledge vs organizational denial)

Pattern: PoC Panic Response

Data: Patch velocity pre-PoC: 0.5 patches/day, Post-PoC: 15 patches/day for 48 hours, then back to 0.5 **State**: Manic-depressive security cycle, reality testing only during manic phase **Prediction**: Vulnerable to threats without public PoC for 28-day windows between panic cycles

Pattern: Friday Fade

Data: Patch success rate Monday: 94%, Tuesday-Thursday: 91%, Friday: 67%, Friday after 3PM: 41% **State**: Superego dissolution in liminal time, ego depletion **Prediction**: Spear phishing success 3x higher Friday 2-5PM

Pattern: Audit-Driven Surges

Data: Normal patch rate: 10/week, Pre-audit week: 180/week, Post-audit: 2/week for 30 days **State**: Performance anxiety with post-audit collapse **Prediction**: Maximum vulnerability 15-45 days post-audit

Pattern: Holiday Vulnerability Windows

Data: Unpatched critical CVEs increase 400% Dec 20-Jan 5 **State**: Collective psychological absence, organizational unconscious dormant **Prediction**: APT persistence establishment during holiday periods

Pattern: Time-to-Patch Decay

Data: Month 1: avg 3 days, Month 6: avg 18 days, Month 12: avg 45 days **State**: Chronic ego depletion leading to learned helplessness **Prediction**: Critical breach within 90 days when decay exceeds 30-day average

AUTHORITY PATTERNS [1.x]

Pattern: Executive Exception Syndrome

Data: C-suite systems: 89% unpatched vulnerabilities, General staff: 23% unpatched **State**: Oedipal dynamics - cannot challenge father figure's systems **Prediction**: CEO fraud/whaling attacks will succeed via executive systems

Pattern: Vendor Deference

Data: Patches from Microsoft: 48hr average, from small vendors: 180+ days or never **State**: Authority transference to large vendors as parental figures **Prediction**: Supply chain attacks via small vendor software

Pattern: Alert Override Hierarchy

Data: Security alerts overridden: by junior staff (2%), by managers (31%), by executives (94%) **State**: Authority gradient overrides technical reality **Prediction**: Insider threat from privileged accounts goes undetected

Pattern: Compliance Theater

Data: Pre-auditor-visit patches: 200, Regular patches: 10/month **State**: Superego projection onto auditors, performing for authority **Prediction**: Real vulnerabilities hidden, cosmetic fixes prominent

SPLITTING PATTERNS [4.x]

Pattern: Good System/Bad System

Data: Legacy CRM: 0 patches in 2 years, New ERP: every patch within 24 hours **State**: Splitting - CRM is "good object" that can't be bad **Prediction**: Breach via legacy CRM, organization will deny it was vulnerable

Pattern: Internal/External Division

Data: Internal network: 1,200 unpatched CVEs, DMZ: 3 unpatched CVEs **State**: Projection of all danger onto perimeter, internal = safe **Prediction**: Lateral movement trivial once perimeter breached

Pattern: Department Favoritism

Data: Sales servers: 5% vulnerable, IT servers: 78% vulnerable **State**: IT as "bad object" containing organizational anxiety **Prediction**: IT infrastructure used as pivot point by attackers

Pattern: Binary Security States

Data: Systems either 100% patched or 0% patched, no middle ground **State**: Inability to hold ambivalent position, all-or-nothing defense **Prediction**: "Abandoned" systems become persistence points

REPETITION COMPULSION PATTERNS [8.x]

Pattern: The Returning CVE

Data: Same SQL injection CVE patched 6 times in 18 months, reappears each time **State**: Repetition compulsion around specific trauma **Prediction**: This exact CVE will be breach vector despite awareness

Pattern: Cyclical Exposure

Data: Port 445 closed → reopened → closed → reopened on 90-day cycle **State**: Unconscious return to vulnerable state **Prediction**: Attack succeeds during "open" phase of cycle

Pattern: Recurring Configuration Drift

Data: Security hardening applied → degrades → reapplied every 4 months **State**: Organizational repetition of security/insecurity cycle **Prediction**: Breach during degradation phase month 3

Pattern: Patch-Rollback Loop

Data: Critical patch applied → system issues → rollback → wait → repeat (5x) **State**: Compulsive repetition avoiding core conflict **Prediction**: Permanent vulnerability, organization cannot resolve

GROUP DYNAMIC PATTERNS [6.x]

Pattern: Shadow IT Clusters

Data: Marketing: 47 unauthorized cloud apps, Finance: 52, IT: 0 **State**: Departments in fight-flight against IT authority **Prediction**: Ransomware entry via unauthorized SaaS

Pattern: Herd Patching

Data: No patches for weeks, then 80% of systems patched in 2 hours **State**: Group think, no individual decision-making **Prediction**: Missed critical patches that aren't "trending"

Pattern: Responsibility Diffusion

Data: Shared systems: 92% vulnerable, Single-owner systems: 31% vulnerable **State**: Bystander effect in digital form **Prediction**: Shared infrastructure becomes attack pathway

Pattern: Security Tool Proliferation

Data: 47 different security tools, 12% utilized features **State**: Manic accumulation as defense against anxiety **Prediction**: Alert blindness, real attacks missed in noise

COGNITIVE OVERLOAD PATTERNS [5.x]

Pattern: Alert Fatigue Curve

Data: Week 1: 94% alerts investigated, Week 12: 31%, Week 24: 8% **State**: Progressive cognitive exhaustion **Prediction**: Real attacks ignored as false positives after week 20

Pattern: Complexity Paralysis

Data: Systems with <10 CVEs: 89% patched, >100 CVEs: 12% patched **State**: Decision paralysis from choice overload **Prediction**: Complex systems remain permanently vulnerable

Pattern: Tool Sprawl Confusion

Data: 5+ scanning tools showing different results, patch rate: 15% of identified **State**: Cognitive dissonance from conflicting information **Prediction**: Analysis paralysis, no action taken

Pattern: Priority Inversion

Data: Low CVEs patched: 78%, Critical CVEs patched: 34% **State**: Cognitive overload causes random rather than rational selection **Prediction**: Breach via known critical CVEs

STRESS RESPONSE PATTERNS [7.x]

Pattern: Incident Response Decay

Data: 1st incident: 4hr resolution, 5th incident same month: 47hr resolution **State**: Acute stress response degradation **Prediction**: Attacker persistence if multiple incidents triggered

Pattern: Panic Patching Errors

Data: Emergency patches: 34% cause system failures vs 3% for planned patches **State**: Fight-flight response overrides careful process **Prediction**: Attackers exploit broken systems post-panic-patch

Pattern: Security Team Turnover Signal

Data: Patch quality drops 60% in month before security staff departure **State**: Unconscious withdrawal before conscious decision **Prediction**: 90-day vulnerability window around staff changes

Pattern: Cortisol Pattern Matching

Data: Monday morning: high false positives, Friday afternoon: missed true positives **State**: Stress hormone cycles affecting perception **Prediction**: Real attacks missed in high-stress periods

ATTACHMENT PATTERNS [4.x]

Pattern: Legacy System Clinging

Data: Windows XP machine: 847 days without patches, still in production **State**: Transitional object attachment, cannot separate **Prediction**: This specific system will be breach point

Pattern: Tool Loyalty Blindness

Data: Continue using compromised tool for 180+ days after vendor breach notification **State**: Object constancy failure, cannot see good object as bad **Prediction**: Supply chain compromise via trusted tool

Pattern: Password Attachment

Data: Same password pattern detected across 89% of systems despite policy **State**: Security blanket behavior, comfort in familiarity **Prediction**: Password spray attacks succeed

AI-INTERACTION PATTERNS [9.x]

Pattern: AI Overdependence

Data: Manual review rate: Pre-AI: 73%, Post-AI: 11% **State**: Maternal transference to AI as caretaker **Prediction**: AI-suggested false negatives become breaches

Pattern: Anthropomorphic Trust

Data: AI recommendations followed 94%, Human expert recommendations: 67% **State**: AI as idealized parent figure **Prediction**: Adversarial AI inputs accepted without question

Pattern: Automation Comfort Zone

Data: Automated patches: 91% success, Manual intervention when automation fails: 8% **State**: Learned helplessness when AI unavailable **Prediction**: Failures during AI downtime become breaches

UNCONSCIOUS IDENTIFICATION PATTERNS [8.x]

Pattern: Hacker Admiration Signal

Data: Security team reads attacker forums 3+ hours/day, patches drop 40% **State**: Unconscious identification with aggressor **Prediction**: Insider threat or unconscious enabling

Pattern: Victim Identification

Data: Post-breach companies mentioned 10x more in security discussions **State**: Identification with victim organizations **Prediction**: Unconsciously recreate similar vulnerabilities

Pattern: Security Theater Performance

Data: Visible security measures: 100% implemented, invisible: 20% implemented **State**: Performing security for imaginary audience **Prediction**: Breach via non-visible vulnerabilities

DENIAL PATTERNS [8.x]

Pattern: Vulnerability Rename Game

Data: Critical vulns reclassified as "medium" without technical basis: 67% **State**: Reality distortion to reduce anxiety **Prediction**: "Medium" classified CVEs become breach vectors

Pattern: False Positive Inflation

Data: 70% of true positives marked as false after initial detection **State**: Denial through misclassification **Prediction**: Real attacks marked as false positives

Pattern: Risk Acceptance Acceleration

Data: Month 1: 0 risks accepted, Month 12: 847 risks accepted without review **State**: Progressive denial of threat reality **Prediction**: Accepted risks become actual breaches

MERGER/ACQUISITION PATTERNS

Pattern: Post-Merger Fragmentation

Data: Acquired company systems: 90% unpatched after 180 days **State**: Organizational splitting, rejection of foreign body **Prediction**: Breach via acquired infrastructure

Pattern: Identity Crisis Paralysis

Data: Patch velocity drops 75% during merger **State**: Organizational identity confusion **Prediction**: 6-month vulnerability window during integration

BOUNDARY PATTERNS

Pattern: Perimeter Fixation

Data: Perimeter systems: 99% patched, Internal: 23% patched **State**: Boundary as container for all anxiety **Prediction**: Trivial internal lateral movement

Pattern: VPN Exception Sprawl

Data: VPN exceptions grow 300% over 12 months **State**: Boundary dissolution, inside/outside confusion **Prediction**: VPN becomes primary attack vector

PROJECTION PATTERNS [8.x]

Pattern: Vendor Blame Preparation

Data: Documentation of vendor issues: 500 pages, internal issues: 3 pages **State**: Projection of internal failures onto vendors **Prediction**: Internal misconfigurations cause breach, vendor blamed

Pattern: Attribution Fantasy

Data: Every incident attributed to "APT" regardless of simplicity **State**: Projection of competence onto attackers **Prediction**: Basic attacks succeed while hunting advanced threats

NARCISSISTIC PATTERNS

Pattern: Special Snowflake Syndrome

Data: "Our environment is unique" used to avoid 78% of security standards **State**: Narcissistic exceptionalism **Prediction**: Standard attacks work despite "uniqueness"

Pattern: Security Metrics Manipulation

Data: Metrics show improvement while vulnerabilities increase **State**: Narcissistic false self presentation **Prediction**: Breach during "best metrics" period

TRAUMA RESPONSE PATTERNS

Pattern: Post-Breach Paralysis

Data: Patching stops completely for 30-60 days after breach **State**: Traumatic freezing response **Prediction**: Second breach during paralysis period

Pattern: Hypervigilance Exhaustion

Data: Post-incident: 1000% increase in alerts, then complete crash **State**: Trauma response cycle **Prediction**: Vulnerability during exhaustion phase

REGRESSION PATTERNS

Pattern: Crisis Regression

Data: During crisis: revert to 2-year-old security configurations **State**: Organizational regression to earlier developmental stage **Prediction**: Old vulnerabilities reappear during stress

Pattern: Magical Thinking Emergence

Data: "Security through obscurity" returns despite training **State**: Regression to magical thinking under pressure **Prediction**: Obscurity assumptions lead to exposure

DISSOCIATION PATTERNS

Pattern: Security Amnesia

Data: Same security incidents "discovered" multiple times as "new" **State**: Organizational dissociation from threatening memories **Prediction**: Unlearned lessons lead to repeat breaches

Pattern: Alert Dissociation

Data: Critical alerts acknowledged but no memory of them later **State**: Dissociative defense against overwhelming threat **Prediction**: Known attacks succeed despite alerts