

IOC nella sicurezza informatica: limiti e approccio ibrido alla bonifica logica

L'intercettazione nasce come problema di analisi del segnale: individuare una presenza attraverso le sue emissioni. Per lungo tempo ciò ha significato lavorare su radiofrequenze e trasmettitori, in un contesto in cui la minaccia era esterna al dispositivo.

Nel quadro contemporaneo del Metodo SPECTRA questa separazione non esiste più. La sorveglianza può essere interna al sistema operativo, integrata nei flussi di dati e mascherata nel traffico cifrato. Il problema si sposta dal segnale al comportamento del sistema.

Le tecniche TSCM tradizionali restano necessarie sul piano fisico, ma non coprono più l'intero dominio della minaccia. In questo scenario emerge anche il limite degli IOC: ciò che non è catalogato non è visibile. Da qui il passaggio ai pattern, con lo smartphone come nodo centrale.

Nel passaggio conclusivo, il punto critico è chiaro: una bonifica basata solo su indicatori noti è strutturalmente incompleta. Molte minacce moderne restano fuori campo perché non ancora classificate.

L'ultimo approfondimento si colloca in questa transizione: dagli IOC ai pattern, dalla verifica del noto alla lettura di comportamenti e anomalie nel tempo.

Cosa sono gli IOC e il limite delle

signature

Nella bonifica logica moderna, soprattutto in ambito smartphone e PC, uno degli errori metodologici più frequenti è affidarsi esclusivamente agli Indicatori di Compromissione (IOC). Gli IOC sono uno strumento fondamentale nell'analisi forense e nella risposta agli incidenti, ma diventano pericolosi quando utilizzati come unico criterio decisionale.

Gli IOC sono elementi osservabili che indicano una possibile compromissione: hash di file malevoli, domini o IP associati a infrastrutture C2, nomi di processi noti, certificati digitali specifici, stringhe di firma binaria, pattern di traffico già classificati. Sono, di fatto, tracce riconosciute di minacce già identificate, e il loro funzionamento si basa su una logica semplice: se compare qualcosa già noto come malevolo, si segnala la compromissione. È il paradigma alla base di antivirus tradizionali, EDR basati su firme, database di *spyware* noti, blacklist DNS/IP e *scanner* mobile commerciali.

I sistemi basati su *signature* funzionano per confronto tra il campione osservato e un database di firme conosciute. Se il campione non è presente nel database, non viene rilevato e tende a essere classificato come pulito. Da qui un limite strutturale: un sistema basato su firme riconosce solo ciò che già conosce. In ambito TSCM logico questo è critico, perché uno *spyware* custom non sarà presente nei database pubblici, un'operazione mirata può usare infrastrutture dedicate e non tracciate, un captatore istituzionale non compare nelle blacklist commerciali e un malware evoluto può mutare hash a ogni build.

Database incompleti e minacce evolute

I database pubblici contengono indicatori relativi a *spyware* commerciali diffusi, trojan Android/iOS noti, famiglie malware catalogate e infrastrutture già smantellate, ma presentano limiti evidenti: lag temporale (l'indicatore viene pubblicato

solo dopo analisi e disclosure), visibilità parziale (non tutte le operazioni vengono rese pubbliche), bias commerciale (i tool mostrano ciò che possono rilevare, non ciò che esiste) e cecità verso le operazioni mirate (una campagna altamente selettiva può non lasciare tracce pubbliche).

Il problema diventa evidente con minacce *zero-day*, malware polimorfico, captatori custom, infrastrutture temporanee, C2 su CDN legittime e uso di servizi cloud comuni. In questi casi l'IP può sembrare legittimo, il dominio neutro, il traffico cifrato HTTPS e il processo dotato di un nome innocuo. Dal punto di vista IOC puro non esiste alcun indicatore classificato come malevolo; dal punto di vista comportamentale possono invece emergere persistenza anomala, flussi dati costanti in orari atipici, connessioni ripetitive verso ASN non coerenti con l'uso dell'utente e pattern di esfiltrazione compatibili con sorveglianza remota.

L'illusione del “nessun risultato”

Uno dei rischi operativi maggiori è l'inferenza “non abbiamo trovato IOC, quindi il dispositivo è pulito”. L'affermazione è metodologicamente scorretta: l'assenza di IOC equivale solo a “non sono stati trovati indicatori già noti”, non ad “assenza di compromissione”. In ambito TSCM logico questo errore può portare a falsi negativi critici. Un approccio esclusivamente IOC-based è infatti reattivo, dipendente da intelligence esterna, non autonomo e non investigativo: non analizza il comportamento, non studia i pattern, non costruisce una baseline e non misura le anomalie relative al contesto. Si limita a confrontare.

IOC e minacce moderne: perché l'analisi da sola non è sufficiente

Nonostante i limiti, gli IOC restano preziosi: utili per identificare minacce note, fondamentali in ambito incident

response, indispensabili per la correlazione OSINT e validi come primo filtro rapido. Il problema non è l'uso degli IOC, ma il loro uso esclusivo. In un contesto caratterizzato da *spyware* custom, captatori evoluti, infrastrutture dinamiche, cifratura end-to-end e servizi cloud legittimi, un'analisi basata solo su IOC è insufficiente. La vera differenza metodologica risiede nella capacità di analizzare ciò che non è ancora classificato, e richiede l'integrazione tra analisi degli indicatori noti e analisi dei pattern comportamentali, oggetto del capitolo seguente.

Approccio ibrido: IOC e analisi pattern-centrica

Nell'analisi del traffico acquisito durante attività di bonifica è frequente osservare dispositivi che mantengono connessioni periodiche verso un numero ristretto di *endpoint* dominanti. La distinzione tra servizi legittimi e possibili architetture di controllo remoto richiede quindi un'analisi quantitativa dei flussi nel tempo. Questo capitolo rappresenta il cuore metodologico della bonifica logica moderna.

In uno scenario caratterizzato da minacce evolute, infrastrutture distribuite e strumenti di sorveglianza sempre più modulari, nessun singolo approccio analitico è sufficiente. La metodologia efficace si fonda su un modello ibrido che integra analisi basata su IOC (Indicator of Compromise) e analisi pattern-centrica comportamentale. L'integrazione di queste due prospettive consente di ridurre i falsi negativi, aumentare la capacità di individuare minacce non catalogate e mantenere un impianto metodologico tecnicamente difendibile.

Analisi basata su IOC

L'analisi IOC individua indicatori noti, già associati a campagne di sorveglianza o malware documentati: indirizzi IP

noti per attività C2, domini associati a infrastrutture di sorveglianza, hash di file malevoli, certificati digitali anomali, pattern di *User-Agent* riconducibili a tool specifici, processi o servizi riconosciuti come *spyware* commerciali. I vantaggi sono la rapidità di identificazione delle minacce già catalogate, l'alta affidabilità quando l'indicatore è verificato e la facilità di documentazione tecnica.

I limiti strutturali sono altrettanto netti: funziona solo su minacce note, è inefficace contro infrastrutture custom o dedicate ed è eludibile tramite rotazione IP, domini dinamici, CDN e tunneling. Nel contesto della sorveglianza professionale o statale, l'infrastruttura può essere dedicata, temporanea, non riutilizzata e priva di indicatori pubblici: in tali scenari l'analisi IOC può risultare formalmente corretta ma operativamente cieca.

Analisi basata su pattern

L'approccio pattern-centrico non cerca etichette, ma comportamenti. Non si domanda "questo IP è noto?", ma "questo comportamento è coerente con un uso legittimo del dispositivo?". L'osservazione comportamentale studia i flussi in termini di frequenza, durata, periodicità, volume e direzionalità, con l'obiettivo di individuare regolarità anomale: connessioni periodiche a intervalli costanti, trasmissioni notturne ripetitive, sincronizzazioni non giustificate dall'uso dell'utente.

In assenza di Deep Packet Inspection (DPI), l'analisi si basa su conteggi, distribuzioni e correlazioni temporali. Un flusso persistente è una comunicazione che si ripete nel tempo, mantiene *endpoint* stabili e mostra comportamento strutturato; la persistenza è un parametro chiave nella valutazione di compatibilità con scenari di monitoraggio remoto.

Un nodo dominante è un *endpoint* che concentra una percentuale significativa dei flussi, mantiene relazioni multiple e mostra

comportamento di aggregazione: in un contesto di sorveglianza può rappresentare un server di raccolta, un *relay* o un punto di orchestrazione, ma la sua identificazione resta strutturale, non attributiva. L'analisi temporale è spesso decisiva: attività in assenza di interazione utente, picchi in orari specifici, variazioni cicliche e incrementi improvvisi di *uplink*. Nel contesto TSCM logico, l'*uplink* anomalo persistente è uno degli elementi più significativi, in quanto compatibile con scenari di esfiltrazione.

Integrazione operativa

L'approccio ibrido non è una semplice somma di tecniche, ma una sequenza logica: ricerca IOC per l'esclusione rapida di minacce note; analisi strutturale dei flussi; studio della persistenza; identificazione dei nodi dominanti; valutazione temporale; separazione tra traffico infrastrutturale normale e pattern compatibili con monitoraggio. L'analisi non produce certezze assolute, ma gradi di compatibilità, scenari probabilistici e valutazioni tecnicamente argomentabili.

Esempio illustrativo

Lo scenario seguente ha finalità esclusivamente didattiche. Non descrive un caso reale, ma serve a mostrare l'applicazione della separazione tra dato, analisi e ipotesi.

Si supponga di acquisire passivamente, per un periodo di osservazione di sette giorni, il traffico di rete di uno smartphone presente in un ambiente sensibile.

Il **dato** è l'insieme degli elementi osservabili e verificabili: lo smartphone stabilisce connessioni verso un medesimo *endpoint* a intervalli regolari di circa quindici minuti, anche nelle ore notturne e in assenza di interazione utente; il volume in *uplink* verso tale *endpoint* è costante e superiore al *downlink*; il flusso si mantiene su HTTPS e l'*endpoint* non compare in alcuna blacklist pubblica.

L'**analisi** interpreta questi elementi in relazione tra loro: la regolarità dell'intervallo è compatibile con un meccanismo di *beaconing*; la prevalenza dell'*uplink* in assenza di attività dell'utente è coerente con un trasferimento di dati verso l'esterno; la persistenza notturna esclude una correlazione con l'uso applicativo dichiarato. Il confronto con la baseline degli altri dispositivi dell'ambiente mostra che nessuno presenta un profilo analogo. Allo stesso tempo, l'analisi registra le spiegazioni alternative legittime: notifiche push, sincronizzazione cloud, telemetria di sistema o *keep-alive* di un'applicazione di messaggistica possono produrre pattern simili.

L'**ipotesi**, esplicitamente condizionale, è che il comportamento osservato risulti tecnicamente compatibile con uno scenario di esfiltrazione remota persistente, qualora le spiegazioni alternative vengano escluse attraverso la correlazione con il dispositivo e la verifica delle applicazioni installate. L'output corretto non è quindi "il dispositivo è intercettato", ma una valutazione di compatibilità tecnica, argomentata e subordinata all'esclusione delle ipotesi fisiologiche.

Perché l'approccio combinato è necessario

Un modello solo IOC è insufficiente; un modello solo comportamentale rischia un'eccessiva interpretazione. La robustezza metodologica deriva dal confronto tra dato noto e comportamento osservato e dalla distinzione netta tra dato oggettivo, pattern e ipotesi. La bonifica logica moderna richiede analisi passiva, assenza di attribuzione prematura e separazione tra evidenza tecnica e narrativa.

L'intelligenza artificiale come supporto analitico

Nel contesto della bonifica logica moderna, l'analisi di

traffico di rete, *log* di sistema, metadati di comunicazione e osservazioni provenienti da domini differenti può generare una quantità elevata di dati tecnici eterogenei. In tali scenari, strumenti basati su intelligenza artificiale possono rappresentare un supporto utile all'attività dell'analista, soprattutto nelle fasi di normalizzazione, correlazione e prioritizzazione delle anomalie.

L'intelligenza artificiale non deve tuttavia essere intesa come sostituzione dell'operatore, né come meccanismo decisionale autonomo. Nel metodo SPECTRA, il suo ruolo è quello di intelligenza aumentata: un sistema di supporto capace di assistere l'analista nell'individuazione di pattern ricorrenti, nella comparazione tra eventi tecnici e nell'evidenziazione di comportamenti che meritano approfondimento.

In ambito TSCM logico, l'intelligenza artificiale può essere utile in particolare per aggregare grandi volumi di dati provenienti da PCAP, *log* di sistema, eventi RF, traffico Wi-Fi, traffico cellulare e metadati di rete; per individuare ricorrenze temporali non immediatamente evidenti all'osservazione manuale; per evidenziare nodi dominanti, flussi persistenti e comunicazioni ripetitive; per correlare eventi appartenenti a domini diversi (ad esempio attività RF, *uplink* cellulare e traffico dati); per supportare la costruzione di baseline ambientali o dispositive; e per assegnare priorità agli elementi da verificare, riducendo il carico cognitivo dell'analista.

Sul piano delle tecniche, questo supporto si traduce in famiglie di metodi già consolidate nell'analisi del traffico e dei *log*. Algoritmi di *anomaly detection* (per esempio Isolation Forest o autoencoder) possono segnalare flussi che si discostano da una baseline appresa, evidenziando *uplink* anomali o connessioni in fasce orarie atipiche.

Tecniche di *clustering* non supervisionato (per esempio DBSCAN

o k-means su feature di flusso quali frequenza, volume, durata e periodicità) consentono di raggruppare comunicazioni con comportamento simile e di isolare i flussi che non rientrano in alcun raggruppamento atteso. Modelli linguistici di grandi dimensioni (LLM) possono assistere nella normalizzazione e nella correlazione di *log* eterogenei, nella sintesi di sequenze di eventi e nella generazione di ipotesi da sottoporre a verifica. In tutti i casi si tratta di strumenti di supporto alla lettura del dato, non di moduli decisionali autonomi.

Il valore dell'intelligenza artificiale non risiede quindi nella capacità di decidere se un dispositivo sia compromesso, ma nella capacità di rendere più leggibili strutture complesse di dati. Un sistema di analisi può, ad esempio, segnalare che un determinato *endpoint* compare con frequenza anomala, che un flusso si ripete in assenza di interazione utente, oppure che un'attività di rete coincide temporalmente con eventi radio osservati nello stesso ambiente. Questi output non costituiscono prove autonome: rappresentano indicatori analitici che devono essere interpretati all'interno del contesto operativo.

Per essere realmente utile, l'intelligenza artificiale deve essere integrata in una metodologia strutturata. Un utilizzo generico, non contestualizzato o basato su prompt isolati rischia di produrre risultati apparentemente convincenti ma metodologicamente deboli. In particolare, nel dominio della bonifica tecnica, l'intelligenza artificiale deve operare su dati normalizzati, criteri espliciti e categorie analitiche coerenti con il modello di riferimento: dato, pattern, ipotesi e valutazione.

Il rischio principale è l'automazione dell'interpretazione. Un'anomalia statistica non equivale a una compromissione; un flusso persistente non equivale automaticamente a un canale di esfiltrazione; un *endpoint* dominante non è necessariamente un server di comando e controllo. L'intelligenza artificiale può

evidenziare correlazioni, ma non può sostituire la valutazione tecnica dell'analista, che deve distinguere tra comportamento fisiologico, anomalia contestuale e scenario compatibile con sorveglianza remota.

Nel metodo SPECTRA l'intelligenza artificiale assume quindi una funzione di supporto su tre livelli. Sul piano descrittivo, organizza i dati osservati, li sintetizza e li rende consultabili in modo più rapido. Sul piano correlativo, evidenzia relazioni temporali o strutturali tra eventi appartenenti a domini differenti. Sul piano prioritario, aiuta l'analista a individuare quali elementi meritano verifica ulteriore. Non assume invece funzione attributiva o conclusiva: non stabilisce l'autore di un'attività, non identifica con certezza una compromissione e non sostituisce la validazione umana.

In questa prospettiva, l'intelligenza artificiale può diventare uno strumento rilevante per la bonifica moderna, ma solo se subordinata a una metodologia rigorosa. Il suo impiego deve rafforzare la separazione tra dato, analisi e ipotesi, non indebolirla. Il processo decisionale resta responsabilità dell'analista umano, che deve valutare gli output alla luce del contesto, delle spiegazioni alternative e dei limiti tecnici dell'osservazione passiva. L'intelligenza artificiale non trasforma la bonifica tecnica in un processo automatico: la rende più scalabile, più ordinata e più efficiente, ma non elimina la necessità di competenza tecnica, interpretazione critica e validazione metodologica.

Bonifica logica nella cybersecurity: limiti degli IOC e importanza dell'approccio combinato

La bonifica logica non può basarsi esclusivamente su liste di indicatori, né su intuizioni comportamentali isolate. Richiede

un approccio combinato, strutturato e tecnicamente difendibile. L'analisi IOC individua ciò che è già conosciuto; l'analisi pattern-centrica individua ciò che si comporta in modo anomalo. Solo l'integrazione delle due consente una valutazione coerente nel contesto della sorveglianza contemporanea.

Principi della metodologia di analisi passiva

Questo capitolo definisce l'impianto metodologico alla base dell'analisi tecnica applicata alla bonifica logica dei dispositivi e delle comunicazioni. Non si tratta di una procedura operativa, ma di un modello concettuale strutturato che consente di interpretare correttamente i fenomeni osservabili senza alterare il contesto tecnico analizzato. L'obiettivo non è trovare uno *spyware*, ma stabilire se il comportamento tecnico di un sistema sia compatibile o incompatibile con scenari di sorveglianza remota.

Analisi passiva del traffico

Il primo principio è la passività assoluta dell'osservazione. L'analisi si fonda sull'acquisizione e l'esame di traffico di rete già generato, metadati di comunicazione, distribuzione protocollare, persistenza dei flussi, frequenza e periodicità delle connessioni. Non viene generato traffico di test, non vengono effettuate interrogazioni forzate, non si inducono risposte dal dispositivo. Questo approccio garantisce integrità forense del contesto, assenza di alterazioni comportamentali e riduzione dei falsi positivi dovuti a stimolazione artificiale. In altre parole, si osserva il sistema mentre si comporta naturalmente.

Nessuna interazione attiva con il dispositivo

L'analisi non prevede installazione di software di scansione invasivi, esecuzione di exploit di verifica, test di penetrazione sul dispositivo oggetto di analisi né interrogazioni dirette verso *endpoint* sospetti. L'interazione attiva può modificare i *log*, attivare meccanismi di autodifesa, alterare i pattern di comunicazione e compromettere la validità dell'analisi. Il dispositivo viene trattato come una sorgente di dati, non come un bersaglio da stimolare.

Approccio non attributivo

Un principio fondamentale è la non attribuzione. L'analisi non identifica un autore, non attribuisce responsabilità, non formula accuse e non costruisce narrative investigative. Si limita a rispondere a una domanda tecnica: il comportamento osservato è compatibile con un'architettura di sorveglianza remota? Qualsiasi riferimento a soggetti, organizzazioni o presunti attori rimane fuori dall'ambito metodologico, riducendo bias interpretativi, derive speculative e sovrainterpretazioni.

Priorità ai pattern comportamentali

Il fulcro metodologico è l'analisi dei pattern. Non si parte da un indicatore di compromissione predefinito, ma dall'osservazione di nodi dominanti, flussi persistenti, distribuzione anomala dei protocolli, ricorrenza temporale e volumi incoerenti rispetto all'uso dichiarato. L'analisi è orientata a frequenza, durata, periodicità e topologia delle comunicazioni. Un singolo evento isolato non ha valore diagnostico; un comportamento ripetitivo, strutturato e coerente nel tempo può invece assumere significato tecnico. L'attenzione si concentra sulla coerenza del sistema, non

sull'eccezione.

Separazione tra dato, analisi e ipotesi

Il metodo impone una distinzione netta tra tre livelli. Il dato è un elemento osservabile, numerico, verificabile e riproducibile. L'analisi è l'interpretazione tecnica del dato, la correlazione tra più elementi e l'identificazione di pattern. L'ipotesi è un possibile scenario compatibile, sempre condizionale e mai affermato come certezza. Questa separazione evita che l'ipotesi influenzi la lettura del dato, che il sospetto diventi conclusione e che l'interpretazione si trasformi in narrativa. Il dato resta autonomo, l'analisi è dichiarata, l'ipotesi è esplicitamente condizionale.

Coerenza con il paradigma contemporaneo

La sorveglianza moderna non si manifesta necessariamente con segnali evidenti o comportamenti plateali. Può essere silente, intermittente, a basso volume e distribuita su più *endpoint*. Per questo motivo l'approccio metodologico non è orientato alla firma, ma alla struttura comportamentale del sistema. La domanda centrale non è "c'è uno *spyware* noto?", ma "il comportamento complessivo del dispositivo è compatibile con un modello di controllo remoto?".

Metodologia di analisi passiva: principi fondamentali per la sicurezza informatica moderna

La metodologia di analisi passiva si fonda su cinque principi cardine: osservazione non intrusiva, assenza di stimolazione attiva, neutralità attributiva, centralità dei pattern e separazione rigorosa tra dato e ipotesi. È un modello che privilegia la solidità tecnica rispetto alla spettacolarizzazione del risultato. In un contesto in cui la

sorveglianza si è spostata dal perimetro fisico al dispositivo, la qualità dell'analisi dipende dalla disciplina metodologica: non dalla ricerca dell'effetto, ma dalla coerenza del metodo.

Limiti tecnici e ambiguità dell'analisi

Ogni analisi tecnica, sia essa RF, logica o di traffico di rete, opera entro limiti strutturali che devono essere esplicitati con chiarezza. L'obiettivo di una bonifica moderna non è produrre certezze assolute, ma valutare la compatibilità tecnica dei pattern osservati con scenari di sorveglianza.

Traffico cifrato

L'evoluzione delle comunicazioni digitali ha portato a un uso quasi totale della cifratura end-to-end: TLS 1.3, HTTPS obbligatorio, DNS over HTTPS e DNS over TLS, VPN commerciali, protocolli proprietari cifrati. Dal punto di vista forense passivo (PCAP, log di rete, metadata), il contenuto del traffico non è analizzabile, il payload non è interpretabile e l'ispezione profonda (DPI) è spesso inefficace o tecnicamente inappropriata. L'analisi si concentra quindi su pattern di persistenza, frequenza delle connessioni, distribuzione temporale, nodi dominanti e anomalie rispetto alla baseline. Un flusso cifrato verso un *endpoint* remoto non è di per sé indicativo di attività malevola: è un dato compatibile con molteplici scenari, inclusi quelli pienamente legittimi.

Servizi cloud legittimi

Le infrastrutture cloud moderne (CDN, storage distribuito, push notification, telemetria) rendono complessa l'attribuzione tecnica. Un dispositivo può comunicare costantemente con infrastrutture di aggiornamento sistema, servizi di sincronizzazione, backup automatici, piattaforme di

messaggistica e servizi di analytics. Molti captatori informatici, commerciali o statali, utilizzano infrastrutture cloud per mascherare il traffico, ma lo stesso vale per applicazioni legittime. Ne consegue che la presenza di traffico verso IP di grandi provider non è di per sé indicativa, la reputazione dell'IP non è elemento decisivo e l'assenza di blacklist non equivale a innocuità. L'analisi deve quindi basarsi sulla coerenza comportamentale, non sulla mera destinazione.

Falsi positivi

Ogni metodologia orientata ai pattern comporta il rischio di falsi positivi: applicazioni che mantengono socket persistenti per notifiche push, sistemi di backup che generano upload periodici, servizi VoIP con *keep-alive* frequenti, sincronizzazioni in background dopo inattività. Un pattern di traffico persistente, notturno o ricorrente può essere compatibile sia con un captatore sia con un servizio cloud legittimo. La distinzione richiede correlazione temporale, analisi del contesto operativo, confronto con baseline e validazione su più fonti di dato (rete, sistema, comportamento utente). L'errore metodologico più grave è interpretare un'anomalia come prova.

Impossibilità di certezza assoluta

In ambito tecnico-forense passivo non si dispone sempre del controllo dell'infrastruttura, delle chiavi di cifratura, dell'accesso ai server remoti né dei log lato controparte. L'analisi può quindi stabilire la compatibilità tecnica con uno scenario di sorveglianza, l'incompatibilità tecnica con determinate ipotesi e la probabilità relativa di determinati comportamenti, ma non può, nella maggior parte dei casi, stabilire con certezza assoluta l'identità dell'operatore remoto, la finalità esatta della comunicazione o la presenza di un captatore specifico in assenza di artefatti diretti.

L'analisi tecnica moderna non produce verità assolute, ma valutazioni strutturate, classificazione dei pattern, analisi di coerenza e scenari compatibili. L'output corretto non è "il dispositivo è intercettato", ma "i pattern osservati risultano tecnicamente compatibili con uno scenario di esfiltrazione remota persistente, in assenza di spiegazioni alternative coerenti". Questa distinzione non è debolezza metodologica: è rigore scientifico.

```
*]:pointer-events-auto R6Vx5W_threadScrollVars scroll-mb-  
[calc(var(-scroll-root-safe-area-inset-  
bottom,0px)+var(-thread-response-height))] scroll-mt-  
[calc(var(-header-height)+min(200px,max(70px,20svh)))]"  
dir="auto" data-turn-id="request-WEB:682d75ad-1a93-4a84-  
a500-1107d75a41a8-92" data-turn-id-container="request-  
WEB:682d75ad-1a93-4a84-a500-1107d75a41a8-92" data-  
testid="conversation-turn-60" data-turn="assistant">
```

Bonifica logica e analisi di traffico: limiti, probabilità e compatibilità tecnica nelle moderne indagini digitali

La bonifica logica e l'analisi di traffico devono essere presentate per ciò che sono: strumenti probabilistici ad alta competenza tecnica, non strumenti di certezza assoluta. La credibilità di un'analisi non deriva dall'enfasi conclusiva, ma dalla chiarezza con cui vengono dichiarati i suoi limiti. L'analisi individua compatibilità tecniche, non prove definitive.

Implicazioni per la bonifica moderna

Il percorso tecnico sviluppato nei capitoli precedenti conduce a una conclusione chiara: la bonifica moderna non può più essere intesa come una semplice attività di scansione radio o ispezione manuale, ma come un processo analitico integrato,

multidimensionale e continuativo. Le tecniche di rilevazione radio rimangono fondamentali, così come l'ispezione manuale dell'ambiente e la verifica fisica delle infrastrutture; tuttavia, l'evoluzione delle tecnologie di sorveglianza ha progressivamente ampliato il dominio della minaccia, che oggi può manifestarsi anche a livello software, di rete o di comportamento dei dispositivi. La bonifica tecnica moderna richiede quindi un approccio metodologico capace di integrare analisi provenienti da domini differenti: spettro radio, infrastrutture di rete e sistemi digitali.

Integrazione tra analisi RF e analisi logica

La bonifica RF tradizionale rimane uno strumento fondamentale. L'analisi dello spettro consente di individuare trasmettitori attivi in ambiente, rilevare segnali anomali per potenza, persistenza o modulazione, identificare *uplink* sospetti su bande note e analizzare comportamenti radio incompatibili con la semplice ricezione passiva. Accanto all'analisi RF deve essere sempre affiancata l'ispezione manuale dell'ambiente: la verifica fisica degli spazi, degli oggetti e delle infrastrutture rimane una componente essenziale delle attività TSCM, consentendo di individuare dispositivi elettronici occultati anche in assenza di emissioni radio attive.

L'evoluzione delle minacce ha però spostato una parte significativa del rischio dal dominio ambientale al dominio digitale. Oggi la sorveglianza può manifestarsi attraverso dispositivi mobili compromessi, software di controllo remoto, configurazioni improprie di rete, flussi dati anomali ma apparentemente legittimi e pattern di comunicazione compatibili con esfiltrazione silente. Di conseguenza, la bonifica moderna deve integrare analisi RF ambientale, analisi di rete locale, analisi logica dei dispositivi e correlazione tra livelli fisico e digitale. La separazione netta tra bonifica ambientale e bonifica informatica non è più coerente

con lo scenario operativo attuale.

Evoluzione delle minacce: dall'emissione alla mimetizzazione

Le microspie analogiche classiche erano relativamente semplici da individuare: trasmissione continua, modulazione riconoscibile, comportamento stabile. Le minacce moderne si caratterizzano invece per trasmissioni intermittenti, uso di infrastrutture esistenti (rete cellulare, Wi-Fi), cifratura dei contenuti, attivazione condizionata (trigger remoto) e integrazione in dispositivi apparentemente legittimi. Il paradigma non è più semplicemente cercare una frequenza, ma interpretare un comportamento.

Un segnale su una banda nota non è automaticamente innocuo, così come un flusso dati cifrato non è automaticamente malevolo. La distinzione avviene attraverso l'analisi del contesto: potenza rispetto all'ambiente, persistenza nel tempo, coerenza con l'uso dichiarato dello spazio, correlazione con eventi o presenze, distribuzione temporale delle attività. La minaccia moderna tende alla mimetizzazione, e la bonifica deve quindi evolversi verso l'interpretazione dei comportamenti tecnici.

Il ruolo dell'analisi comportamentale

Il passaggio concettuale più rilevante riguarda l'introduzione dell'analisi comportamentale. Non si tratta di attribuire intenzioni, ma di osservare pattern oggettivi: flussi dati ricorrenti in determinate fasce orarie, attivazioni RF non coerenti con l'uso dell'ambiente, *uplink* persistenti senza traffico visibile, dispositivi che mantengono comunicazioni costanti anche in stato di apparente inattività. L'analisi comportamentale non sostituisce la tecnica, ma la completa, e richiede raccolta strutturata dei dati, comparazione temporale, definizione di baseline ambientali e capacità di

distinguere traffico infrastrutturale da trasmissione locale. In questo modello la bonifica diventa un processo ciclico: acquisizione, classificazione, correlazione, interpretazione, validazione. Il risultato non è un semplice “assenza di segnali”, ma una valutazione tecnica argomentata del rischio.

Il metodo SPECTRA: formalizzazione della metodologia multidominio

Posizionamento rispetto allo stato dell'arte

Le attività di Technical Surveillance Countermeasures (TSCM) sono da tempo descritte in letteratura tecnica e in ambito istituzionale attraverso linee guida operative consolidate. Documenti riconducibili a contesti governativi, come quelli sviluppati in ambito National Security Agency e Dipartimento della Difesa statunitense, definiscono in modo strutturato le procedure di bonifica ambientale, con particolare enfasi sull'analisi radioelettrica, sull'ispezione fisica e sulla rilevazione di dispositivi elettronici.

Parallelamente, negli ultimi anni si sono sviluppate metodologie tecniche avanzate orientate all'analisi dei dispositivi e dei captatori informatici: in questo ambito, i lavori di Amnesty International Security Lab e Citizen Lab hanno introdotto approcci forensi e di network analysis basati su indicatori tecnici, analisi dei log e correlazione delle infrastrutture di comunicazione, contribuendo in modo significativo alla comprensione delle moderne tecnologie di sorveglianza software.

Nonostante l'elevato livello tecnico, questi approcci risultano generalmente strutturati per dominio: le metodologie TSCM tradizionali operano prevalentemente sul piano fisico e radio, mentre le metodologie forensi moderne si concentrano sul dispositivo e sul traffico di rete. Il metodo SPECTRA si inserisce in questo contesto come formalizzazione di un approccio integrato.

Non introduce nuove tecniche di rilevazione, ma organizza in modo esplicito un modello analitico multidominio in cui analisi ambientale e radioelettrica, ispezione fisica, analisi dei dispositivi e osservazione del traffico di rete vengono trattate come componenti interdipendenti di un unico processo. L'elemento distintivo del metodo non è quindi lo strumento utilizzato, ma la logica di integrazione: il valore analitico non è attribuito alla singola evidenza, ma alla correlazione tra evidenze eterogenee osservate nel tempo.

La differenza metodologica è netta. Nei framework tradizionali il dato viene analizzato principalmente all'interno del proprio dominio di origine; nel metodo SPECTRA il dato assume significato solo attraverso la relazione con altri domini e la sua evoluzione temporale. Questo comporta due elementi metodologici espliciti: il pattern multidominio come unità minima di analisi e la correlazione temporale come criterio interpretativo. In questo senso, SPECTRA non rappresenta un rebranding di pratiche esistenti, ma la formalizzazione di un modello analitico che integra in modo strutturato domini tecnici tradizionalmente trattati separatamente.

Il confronto sintetico con i principali riferimenti dello stato dell'arte chiarisce il contributo specifico del metodo.



Va inoltre osservato che la stessa metodologia forense di Amnesty riconosce esplicitamente un principio coerente con l'impianto di questo lavoro: la mancata corrispondenza con indicatori pubblici noti non conferma l'assenza di compromissione, ma indica soltanto che non sono stati trovati riscontri con indicatori già catalogati. È la stessa logica che, al capitolo 7, motiva il superamento di un approccio basato esclusivamente su IOC.

Definizione estesa

SPECTRA (Security Pattern Environment Correlation Technical

Reconnaissance & Analysis) è una metodologia multidominio per attività di Technical Surveillance Countermeasures (TSCM) basata sull'integrazione coordinata di tecniche eterogenee e sulla correlazione di pattern tecnici nel tempo. Il metodo non introduce una singola tecnica, ma formalizza un sistema integrato di analisi in cui ogni componente contribuisce alla riduzione del rischio di sorveglianza tecnica.

Principio cardine

Nessuna tecnica, isolatamente, è sufficiente a garantire una bonifica efficace. La sicurezza deriva esclusivamente da integrazione, correlazione e continuità temporale. La mancanza di uno di questi elementi introduce inevitabilmente zone cieche analitiche.

Architettura del metodo

SPECTRA è composto da sei componenti operative, da applicare congiuntamente.

1. **Analisi ambientale fisica:** ispezione strutturale, verifica di accessi e punti sensibili, individuazione di modifiche o anomalie.
2. **Analisi spettro RF:** scansione *wideband* e mirata, identificazione di segnali persistenti e *burst*, valutazione della potenza rispetto al contesto.
3. **Rilevazione elettronica (giunzioni non lineari):** individuazione di circuiti attivi/passivi, rilevamento di dispositivi spenti o non trasmettenti, attività conforme alle tecniche TSCM tradizionali.
4. **Analisi dispositivi autorizzati:** smartphone, PC, IoT; verifica logica e comportamentale; analisi del traffico dati e delle attività anomale; individuazione di compatibilità con captatori informatici.
5. **Gestione dispositivi non bonificabili:** dispositivi esterni (ospiti, fornitori, terzi) per i quali è impossibile una verifica tecnica diretta; misure di isolamento controllato, esclusione dall'ambiente

sensibile e messa in sicurezza attiva (per esempio saturazione acustica dei microfoni).

6. **Monitoraggio temporale:** osservazione a breve, medio e lungo termine; correlazione degli eventi nel tempo; identificazione di pattern ricorrenti.



Figura 1. Schema concettuale del metodo SPECTRA. Il metodo integra domini tecnici differenti (ambiente fisico, spettro RF, rilevazione elettronica, dispositivi, gestione del rischio residuo e osservazione temporale) all'interno di un processo di correlazione multidominio e analisi pattern-centrica finalizzato alla valutazione tecnica del rischio di sorveglianza.

Logica unificante

Il metodo si basa su un principio operativo preciso: il valore analitico non è nella singola rilevazione, ma nella correlazione tra domini e nel tempo. Per esempio: RF più traffico dati indica una possibile attività di esfiltrazione; dispositivo più comportamento anomalo indica una possibile compromissione; segnale più persistenza indica una possibile sorgente locale.

Approccio pattern-centrico

SPECTRA introduce un cambio di paradigma. Non si cerca il singolo dispositivo, la singola frequenza o l'indicatore statico, ma si analizzano pattern tecnici, coerenza con il contesto e anomalie multidominio. Il pattern rappresenta l'unità minima di significato analitico nel metodo.

Dimensione temporale

Il metodo opera su tre scale: breve termine (rilevazioni immediate), medio termine (comportamento nel tempo) e lungo

termine (persistenza e ricorrenza).

Gestione del rischio residuo

Elemento fondamentale del metodo: ciò che non è verificabile deve essere controllato. Questo riguarda in particolare i dispositivi non autorizzati, i dispositivi non analizzabili e gli ambienti non completamente isolabili. La soluzione è il contenimento del rischio, la riduzione della capacità di acquisizione (audio/dati) e il controllo delle condizioni operative. L'assenza di rilevazioni non equivale all'assenza di capacità di acquisizione.

Distinzione metodologica rispetto alla TSCM tradizionale

SPECTRA non sostituisce la TSCM: la include, la estende e la integra. Supera il limite di una visione orientata solo all'RF, solo al piano fisico o solo al dispositivo, introducendo correlazione strutturata, analisi comportamentale e integrazione multidominio.

Limite delle tecniche isolate

Il metodo formalizza un punto chiave: la bonifica RF da sola è insufficiente, così come lo sono l'analisi dei dispositivi da sola, l'isolamento dei dispositivi da solo e il monitoraggio RF continuativo da solo. La sicurezza emerge solo dalla combinazione delle tecniche. La sicurezza non è funzione della tecnica utilizzata, ma del grado di integrazione tra tecniche.

Output del metodo

SPECTRA non produce certezza assoluta, ma una valutazione tecnica strutturata basata su anomalie rilevate, pattern identificati e coerenza con il contesto. Il risultato è sempre espresso in termini probabilistici e contestuali, non deterministici.

Formalizzazione dell'acronimo

- **S, Security:** finalità di protezione dalla sorveglianza tecnica.
- **P, Pattern:** analisi basata su pattern tecnici, non su eventi isolati.
- **E, Environment:** ambiente fisico come dominio operativo.
- **C, Correlation:** correlazione multidominio e temporale.
- **T, Technical:** approccio tecnico, non teorico.
- **R, Reconnaissance:** ricognizione sistematica dell'ambiente.
- **A, Analysis:** analisi strutturata dei dati raccolti.

Definizione conclusiva

SPECTRA è una metodologia multidominio che integra tecniche di analisi ambientale, RF, elettronica, dispositiva e comportamentale, basata sulla correlazione di pattern nel tempo, finalizzata all'identificazione di anomalie tecniche compatibili con attività di sorveglianza o acquisizione non autorizzata di informazioni.

Contesto operativo e livelli di minaccia

Le attività di sorveglianza tecnica possono manifestarsi su livelli profondamente differenti in termini di capacità, risorse e obiettivi. In via generale è possibile distinguere lo spionaggio statale (elevata capacità tecnica, accesso a risorse avanzate come exploit *zero-day* e infrastrutture dedicate), lo spionaggio privato professionale (investigatori, aziende, competitor), lo spionaggio mirato a basso/medio livello (strumenti commerciali avanzati), lo spionaggio amatoriale/opportunistico (dispositivi a basso costo, software facilmente accessibile) e la sorveglianza in ambito personale (partner, familiari, soggetti interni). Il fattore discriminante tra questi scenari è rappresentato principalmente da budget operativo, livello tecnico

dell'attore e obiettivi della sorveglianza.

Nel contesto operativo TSCM/SPECTRA, tali differenze non modificano il principio metodologico fondamentale. L'analisi del contesto orienta la valutazione del rischio, ma non riduce il perimetro della bonifica.

Durante la fase preliminare vengono raccolte informazioni sul contesto, stimato lo scenario di minaccia e definito il livello di rischio; in fase operativa, però, la bonifica deve comunque essere completa e multidominio. Una microspia da 50 euro e un sistema avanzato condividono lo stesso spazio operativo, un captatore software e un trasmettitore RF possono coesistere, e una minaccia apparentemente semplice può produrre effetti critici. Di conseguenza, il metodo SPECTRA prescinde dal livello dell'attaccante nella fase di verifica tecnica: il contesto serve a interpretare i risultati, a pesare le anomalie e a formulare ipotesi, ma non giustifica mai una riduzione dell'analisi.

Conclusioni

L'evoluzione della sorveglianza tecnica ha determinato uno spostamento strutturale del punto di acquisizione delle informazioni: dall'ambiente fisico al dispositivo personale, e dall'hardware dedicato al software residente. Questo cambiamento non è esclusivamente tecnologico, ma profondamente metodologico. Le tecniche di bonifica tradizionali, basate su analisi radioelettrica, ispezione fisica e rilevazione elettronica, rimangono strumenti fondamentali, ma non sono più sufficienti a descrivere l'intero dominio della minaccia.

Nel contesto contemporaneo la sorveglianza può manifestarsi attraverso dispositivi legittimi compromessi, traffico di rete cifrato, pattern comportamentali distribuiti nel tempo e infrastrutture apparentemente indistinguibili da quelle ordinarie. Di conseguenza, la bonifica tecnica non può più essere intesa come una singola attività, ma come un processo

analitico multidominio. Il metodo SPECTRA si inserisce in questo contesto come formalizzazione di tale approccio, integrando analisi ambientale, analisi RF, rilevazione elettronica, analisi dei dispositivi, osservazione del traffico e correlazione comportamentale all'interno di un unico modello metodologico coerente.

Il contributo principale del metodo non consiste nell'introduzione di nuove tecnologie, ma nella definizione di un principio operativo chiaro: la sicurezza non è il risultato di una tecnica, ma dell'integrazione strutturata di più domini analitici. In questo paradigma il dato isolato perde significato, il pattern diventa unità analitica, il tempo diventa variabile critica e la certezza lascia spazio alla valutazione probabilistica. La bonifica tecnica moderna non consiste quindi nel trovare una microspia, ma nel determinare se un sistema tecnico, nel suo complesso, presenti comportamenti compatibili con scenari di sorveglianza. Questo passaggio rappresenta il vero punto di discontinuità rispetto ai modelli tradizionali e definisce il perimetro operativo della contro-sorveglianza tecnica contemporanea.

Il presente lavoro si basa principalmente su esperienza tecnica operativa e sull'analisi di casi documentati nella letteratura tecnica e giornalistica internazionale relativi all'utilizzo di captatori informatici e spyware commerciali.

Il lavoro mette in luce un cambiamento strutturale: la sorveglianza non è più un elemento esterno, riconoscibile tramite segnali dedicati, ma una funzione integrata nei sistemi digitali. Oggi il software può operare direttamente all'interno del sistema operativo dello smartphone, acquisendo dati alla sorgente e rendendo spesso invisibile il tradizionale punto di intercettazione.

Di conseguenza, anche la contro-sorveglianza deve adattare il proprio paradigma: le tecniche classiche restano fondamentali, ma non sono più sufficienti a descrivere un contesto in cui

traffico cifrato e processi interni si sovrappongono al comportamento ordinario del dispositivo.

Il Metodo SPECTRA nasce in questo scenario, proponendo un approccio che non si basa solo su segnali e indicatori noti, ma sulla lettura dei pattern e delle dinamiche comportamentali nel tempo.

Profilo Autore



Titolare delle licenze EJPT e ECPPT (Professional Penetration Tester) della società eLearnSecurity. Svolge attività di Network Security in particolare Penetration Test & VA – Vulnerability Assessment.

Nel 2019 fonda la società ISK (www.isksecurity.it), partner strategico ed esterno per attività di Security specializzata. Svolge attività di bonifiche ambientali da microspie, attività di Security Assessment e Mobile Security.

Condividi sui Social Network:

<https://www.ictsecuritymagazine.com/articoli/ioc-bonifica-logica/>