

Adrenaline FX Guida all'uso

Versione 0.1 alpha

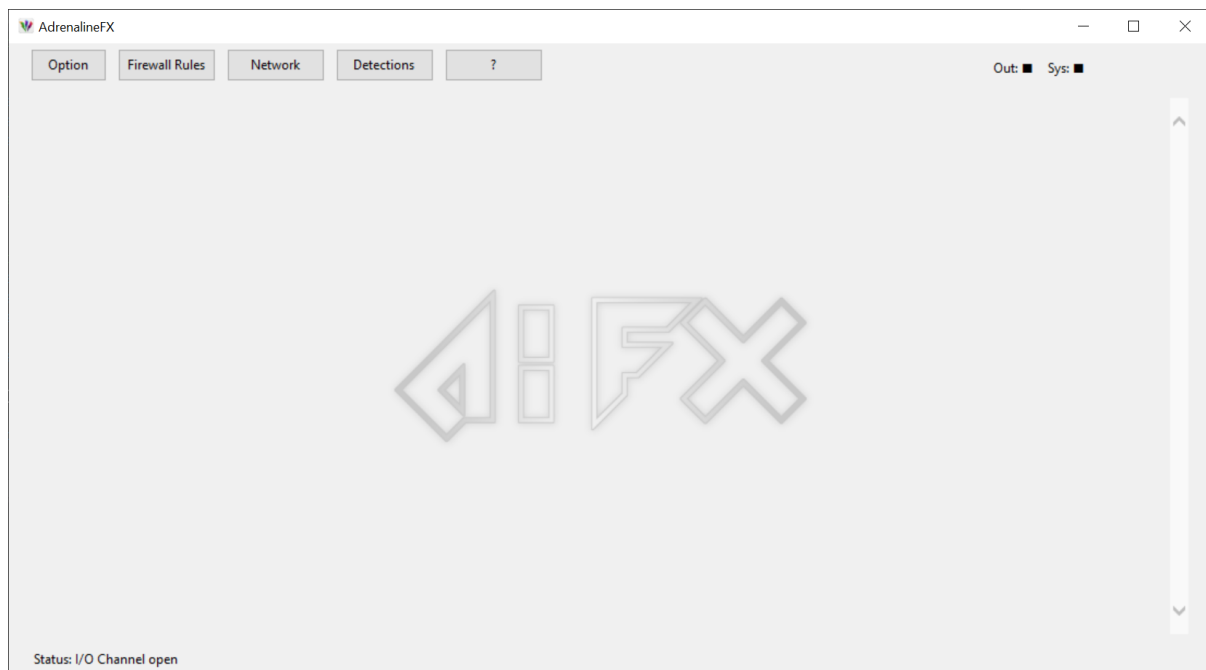
Requirements : MS Windows 10/11 x64, pcap driver, sysmon64

Tipo di Monitoraggio: Multi-Score Machine Learning

Dissezione Header / Payload : DNS, ICMP, NETBIOS (AntiSmuggler)

Conversione offline: IP > ASN / IP > ISO_COUNTRY_CODE

Servizi installati: AdrenalineMon5, AdrenalineFX_Service, AdrenalineFX_Firewall



Manuale Utente di AdrenalineFX

Introduzione

AdrenalineFX è uno strumento progettato per il monitoraggio e l'analisi del traffico di rete, con un focus particolare sulla rilevazione e prevenzione dell'esfiltrazione di dati.

Questo manuale vi guiderà attraverso le funzionalità principali del software.

Architettura del Sistema

AdrenalineFX è composto da diversi componenti chiave che lavorano insieme per monitorare e analizzare il traffico di rete. La sua architettura è progettata per garantire un'analisi dettagliata e tempestiva delle attività di rete:

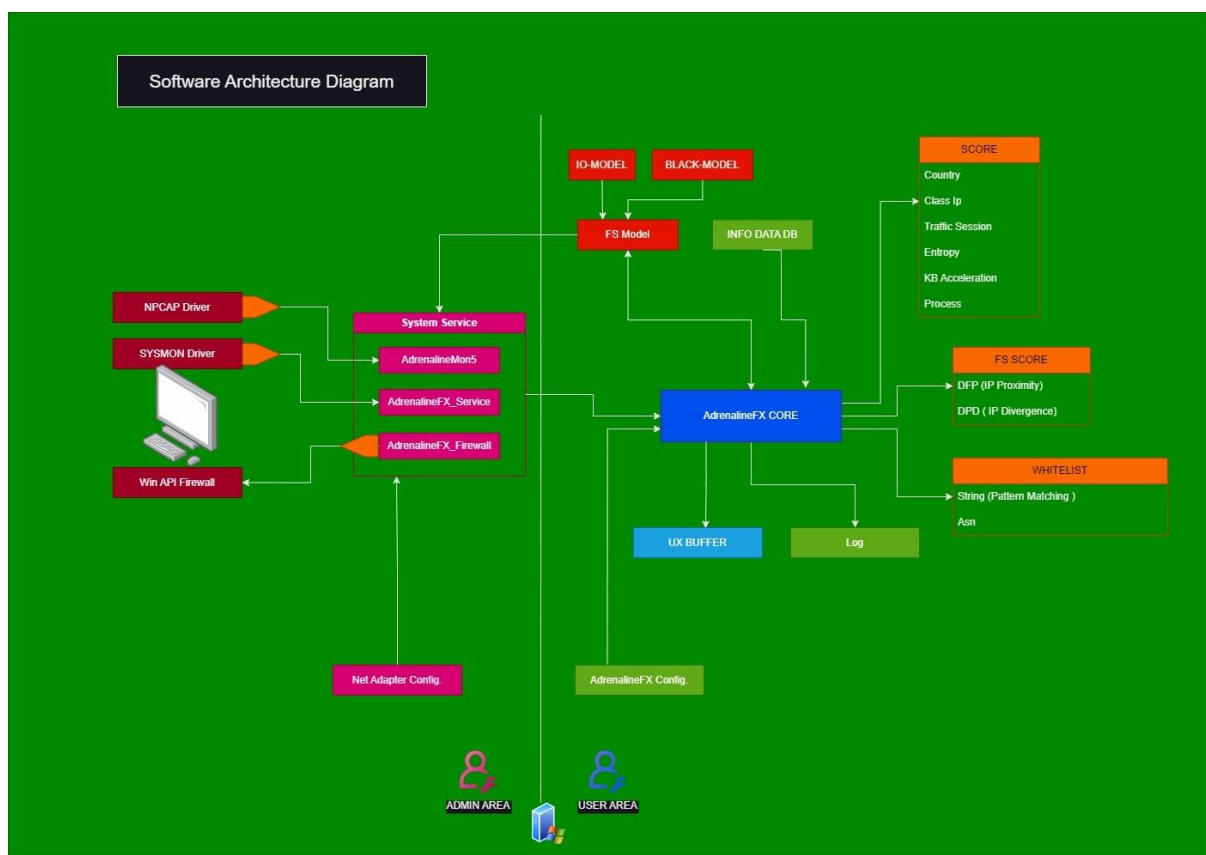
NPCAP Driver: Gestisce la comunicazione di rete a basso livello e permette al software di catturare e analizzare i pacchetti di dati in tempo reale.

Sysmon64 Service: Interagisce con i servizi di sistema per raccogliere dati necessari all'analisi.

AdrenalineFX Service: Il servizio principale che esegue le analisi e calcola gli score di potenziale esfiltrazione.

AdrenalineFX CORE: Il nucleo del software, dove avviene l'elaborazione dei dati e l'applicazione dei modelli di rilevazione.

UX BUFFER: Gestisce i dati visualizzati nell'interfaccia utente.

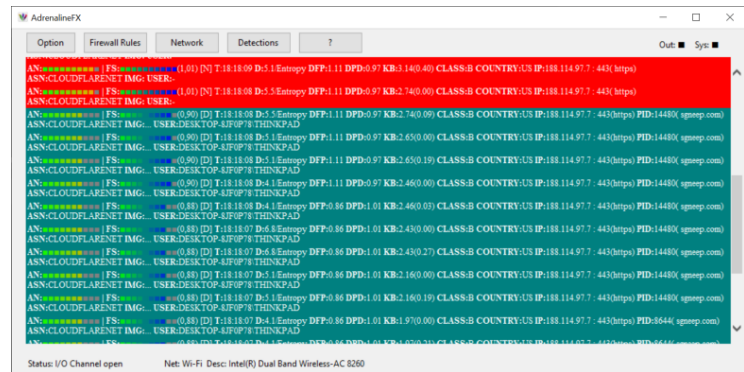


Interfaccia Utente

L'interfaccia di AdrenalineFX è progettata per essere intuitiva e facile da usare, permettendo un monitoraggio e un controllo efficaci del traffico di rete:

La schermata principale mostra gli ultimi dati di log (fino a 25 righe) che scorrono dall'alto verso l'alto il basso.

Ogni riga dell'UX-BUFFER fornisce informazioni dettagliate sul traffico di rete:



FS: Flow Score, rappresenta la gravità del flusso di dati. Deve essere abilitato (finestra "opzioni"--> "FS(flow score)" --> "Use")

T: Orario del rilevamento.

D: Entropia del pacchetto, un'indicazione di dati cifrati o compressi.

DPD: Divergenza calcolata dal modello.

DFP: Indicatore di prossimità calcolata dal modello

KB: Volume di dati trasferiti nella sessione di rilevamento.

CLASS: Classe dell'IP.

COUNTRY: Paese di destinazione del pacchetto.

IP: Indirizzo IP e porta.

ASN: Sistema autonomo di rete, è numero univoco che viene assegnato alle reti locali dall'American Registry for Internet Numbers (ARIN).

IMG: Immagine del sistema. Indica l'applicazione o servizio che ha inviato i dati.

USER: Utente del sistema.

Descrizione dell'Interfaccia Principale

L'interfaccia principale comprende diverse schede e opzioni per una gestione e monitoraggio ottimale del traffico di rete:

Bottoni:

- “Options”
- “Firewall Rules”
- “Network ID”
- “Detections”
- “Info”

Virtual LEDs: Due indicatori che mostrano lo stato dei dati in output (Out) e il traffico Sysmon (Sys).

UX-Buffer: Visualizza un log con voci codificate a colori.

Status: La stringa di stato/informazioni.

Firewall Rules

La finestra “Firewall Rules” permette di gestire le regole del firewall. AdrenalineFX inserisce automaticamente regole per bloccare IP o processi quando viene rilevato uno score di rischio elevato.

Le regole del firewall sono generate automaticamente da AdrenalineFX per bloccare il traffico sospetto.

AdrenalineFX crea le regole in uscita con bloccando l'esfiltrazione a livello di IP o Applicazione.

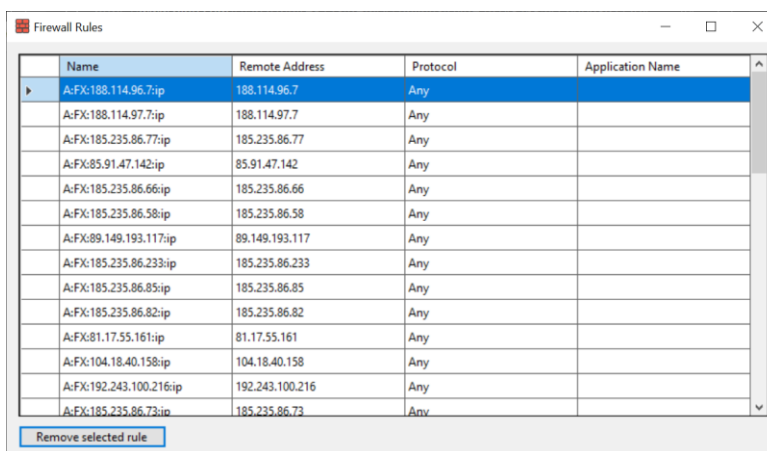
Rimozione della regola:
seleziona la linea di
interesse e premi “Remove
selected rule”.

Name: Nome della regola e
utente.

Remote Address: Indirizzo
remoto.

Protocol: Protocollo utilizzato (any).

Application Name: Nome dell'applicazione bloccata (nel firewall viene bloccata esclusivamente la connessione in uscita di un dato ip o applicazione.



Name	Remote Address	Protocol	Application Name
A:FX:188.114.96.7:ip	188.114.96.7	Any	
A:FX:188.114.97.7:ip	188.114.97.7	Any	
A:FX:185.235.86.77:ip	185.235.86.77	Any	
A:FX:85.91.47.142:ip	85.91.47.142	Any	
A:FX:185.235.86.66:ip	185.235.86.66	Any	
A:FX:185.235.86.58:ip	185.235.86.58	Any	
A:FX:89.149.193.117:ip	89.149.193.117	Any	
A:FX:185.235.86.233:ip	185.235.86.233	Any	
A:FX:185.235.86.85:ip	185.235.86.85	Any	
A:FX:185.235.86.82:ip	185.235.86.82	Any	
A:FX:81.17.55.161:ip	81.17.55.161	Any	
A:FX:104.18.40.158:ip	104.18.40.158	Any	
A:FX:192.243.100.216:ip	192.243.100.216	Any	
A:FX:185.235.86.73:ip	185.235.86.73	Any	

Remove selected rule

Integrazione con il Registro di Sicurezza di Windows

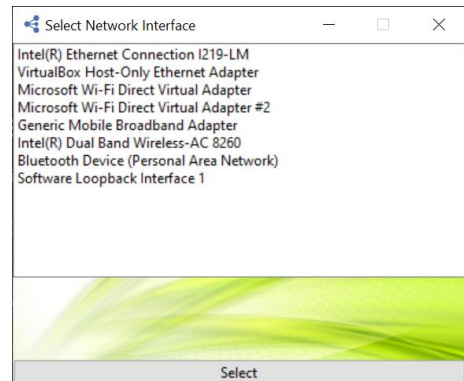
Da fare

Selezione dell'Interfaccia di Rete

La finestra "Select Network Interface" consente di scegliere l'interfaccia di rete da monitorare.

Attenzione: solo gli account "amministratore" sono abilitati a cambiare la rete.

Selezionate l'interfaccia appropriata e confermate la scelta con il pulsante "Select".



Opzioni

Il finestra opzioni consente di configurare vari parametri di AdrenalineFX .

Show WhiteList : abilita la visualizzazione dei pacchetti che sono stati contrassegnati come leciti. (questa funzione viene rimossa nella prossima versione)

Show Dns: abilita la visualizzazione dei log generati da Sysmon con id22.

Realtime UX: abilita la visualizzazione in tempo reale dei pacchetti (disabilitarla in produzione)

Options

W.List ASN W.List ASN DATA COUNTRY

SCORE WEIGHT :

DNS : 3

ASN : 10

TRAFFIC (KB): 3

IP CLASS: 5

USER : 6

PROCESS : 15

ENTROPY : 5

KB PARTIAL : 10

FX MODEL : 5

ACCELERATION (KB) : 0.70

Model duration: Days: 1 Hour: 1

DFP (data flow proximity): 0.50

DPD (data pattern divergence): 0.30

FS (flow score): 1.00 ☒ : Use

UX Buffer: ☐ Show WhiteList ☒ Show Dns ☐ Realtime

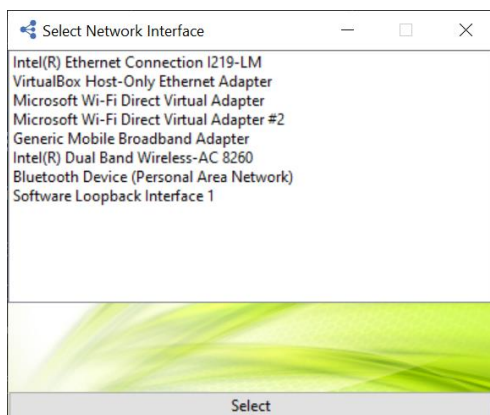
Salva per aggiornare Default Values

NFX

Utilizzo per Rilevare esfiltrazioni di dati tramite protocollo di rete.

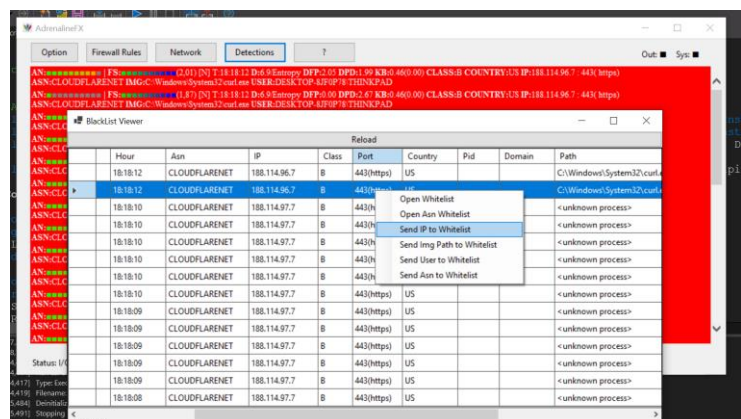
AdrenalineFX è progettato per rilevare potenziali esfiltrazioni di dati attraverso un'analisi approfondita del traffico di rete. Ecco alcuni passaggi per utilizzare efficacemente il software:

Avvio del Software: Assicurarsi che il driver npcap sia correttamente installato e funzionante.



Selezione dell'Interfaccia di Rete: Utilizzare la scheda "Network" per selezionare l'interfaccia di rete da monitorare.

Visualizzazione dei rilevamenti a cui è stato disabilitato l'accesso: Nella scheda "Detections", monitorare le voci di log per informazioni appartenenti all'IP, nella scheda "Firewall Rules" vedere gli ip contrassegnati come bloccati.



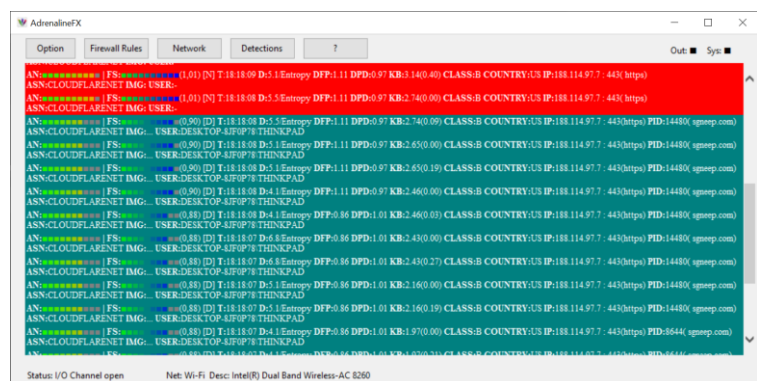
Attenzione! Se viene inserito l'ip nella whitelist ricordarsi di eliminare quell'ip dal firewall.

Interpretazione dei Dati nel Model Viewer e UX-Buffer

- AN (Anomaly Score): Indica il rischio associato a un flusso di dati.(experimental)
- FS (Flow Score): Rappresenta la gravità del flusso di dati.
- ENTROPIA: Identifica dati cifrati o compressi, indicativi di possibili esfiltrazioni.
- DPD (Data Pattern Divergence): Misura la deviazione dal comportamento in un arco temporale definito.
- DFP (Data Flow Proximity): Indica la prossimità su di un modello di ip noto in un arco temporale definito
- KB: Indica l'aumento del volume di dati nelle sessioni dei pacchetti. Ogni sessione rappresenta una serie di pacchetti inviati all'IP di destinazione.

Nella figura sotto il valore di soglia FS è impostato ad 1.0 ,regolare questo valore secondo le preferenze nel pannello “Option” alla voce “FS (flow score)”.

Puoi regolare i parametri DFP e DPD anche singolarmente, in FS(flow score) disabilita il checkbox “Use”.



Utilizzo delle Opzioni di Configurazione

Accesso al Menu Opzioni: Configurare le opzioni per adattare il software alle esigenze specifiche.

Configurazione del TimeToLive: Nel pannello di controllo, è possibile impostare la durata di vita del modello. Questo parametro determina per quanto tempo un modello rimane attivo prima di essere rigenerato, influenzando la frequenza degli aggiornamenti e la sensibilità del sistema.

Configurazione di DPD e DFP: Questi parametri vengono utilizzati per monitorare e analizzare il traffico di rete. DPD (Data Pattern Divergence) e DFP (Data Flow Proximity) si adattano dinamicamente al traffico di rete, aggiornando i modelli di riferimento per riflettere le condizioni attuali.

Calcolo dello Score (FS): Il parametro FS (Flow Score) rappresenta il risultato combinato delle analisi di DFP e DPD. Questo score fornisce una valutazione complessiva della sicurezza del traffico di rete, aiutando a identificare potenziali minacce.

Capitolo: Gestione del Time-to-Live (TTL) in Adrenaline

Il Time-to-Live (TTL) è un parametro fondamentale nel monitoraggio del traffico di rete e nella rilevazione delle esfiltrazioni di dati. In AdrenalineFX, il TTL viene utilizzato per garantire che l'analisi del traffico sia sempre aggiornata e rilevante. Questo capitolo spiega l'importanza del TTL e come viene gestito all'interno del sistema.

Cos'è il Time-to-Live (TTL)?

Il TTL è un valore che indica la durata di vita di un pacchetto di dati in una rete. Ogni pacchetto ha un TTL che viene decrementato di uno ogni volta che attraversa un router. Quando il TTL raggiunge zero, il pacchetto viene scartato. Questo meccanismo impedisce che i pacchetti rimangano indefinitamente in circolazione nella rete.

Importanza del TTL in AdrenalineFX

In AdrenalineFX, il TTL è utilizzato per mantenere l'analisi del traffico di rete focalizzata sui dati più recenti e rilevanti. Ecco perché il TTL è cruciale:

Rimozione dei Dati Obsoleti: Il TTL aiuta a eliminare i pacchetti di dati che hanno superato la loro utilità, garantendo che l'analisi si concentri solo sui pacchetti attuali.

Prevenzione dei Falsi Positivi: Monitorare pacchetti con TTL scaduto può portare a falsi positivi. Utilizzando il TTL, AdrenalineFX riduce il rischio di segnalare attività sospette basate su dati non più rilevanti.

Aggiornamento Continuo: Il TTL assicura che il sistema sia costantemente aggiornato, migliorando la precisione e l'efficacia del rilevamento delle anomalie.

Gestione del TTL in AdrenalineFX

Quando il TTL di un pacchetto scade, AdrenalineFX esegue un "refresh" del modello di analisi. Questo processo garantisce che solo i pacchetti con un TTL valido siano considerati nell'analisi, mantenendo il sistema agile e reattivo.

Modelli Dinamici e Variabilità dei Valori (DFP / DPD)

Modelli di Riferimento Dinamici

In AdrenalineFX, i modelli di traffico fungono da benchmark per valutare l'attività corrente sulla rete. Questi modelli, denominati "Modelli di Riferimento Dinamici", vengono costantemente aggiornati e sostituiti a intervalli regolari definiti dall'utente. Questo processo garantisce che l'analisi sia sempre basata su dati pertinenti e recenti, migliorando l'accuratezza del rilevamento delle anomalie.

Regolazione del "TimeToLive" del Modello

La durata di vita del modello, configurabile dall'utente, determina per quanto tempo un modello rimane attivo prima di essere rigenerato. La scelta del "TimeToLive" (TTL) influisce direttamente sul comportamento dei parametri DFP e DPD.

Durata Breve (Esempio: 1 ora):

- **Contesti di Utilizzo:** Ideale per ambienti dove il traffico è altamente variabile, come in ambito domestico o web.
- **Vantaggi:** Permette di adattare rapidamente i modelli alle nuove condizioni, riducendo la probabilità di falsi positivi. I modelli si aggiornano frequentemente, consentendo un'accettazione più fluida dei pacchetti prima che gli allarmi scattino.

Durata Lunga (Esempio: 1 giorno):

- **Contesti di Utilizzo:** Indicata per ambienti aziendali dove il traffico è più stabile e prevedibile.
- **Vantaggi:** Mantiene una visione continuativa e coerente del traffico, utile per rilevare anomalie più sottili e pericolose che potrebbero emergere solo su periodi più estesi.

Comportamento dei Valori di DFP e DPD

I valori di DFP e DPD possono variare in risposta al traffico di rete (in uscita), in base a quanto questo traffico diverge dai modelli attuali. L'algoritmo adatta dinamicamente questi valori per riflettere l'aderenza o la deviazione rispetto ai modelli, facendo sì che la soglia di allarme possa variare in base all'analisi continua del traffico.

- **Aumento dei Valori:** Quando il traffico di rete diverge significativamente dai modelli di riferimento, i valori di DFP e DPD aumentano, indicando una potenziale anomalia.

- **Diminuzione dei Valori:** Se il traffico di rete rientra nei parametri previsti dai modelli, i valori di DFP e DPD diminuiscono, segnalando un comportamento normale.

Multi-Score Machine Learning

AdrenalineFX utilizza un approccio avanzato di machine learning chiamato “Multi-Score Machine Learning” per rilevare e prevenire l'esfiltrazione dei dati. Questo metodo si basa sull'uso di più metriche per valutare e analizzare il traffico di rete, garantendo un rilevamento accurato e tempestivo delle anomalie.

Metriche Utilizzate

DFD:

- **Descrizione:** Utilizza la distanza euclidea per misurare la dissimilarità tra i pacchetti di dati. Questa metrica è particolarmente utile per identificare pacchetti che si discostano significativamente dal comportamento normale.

DPD:

- **Descrizione:** Misura la prossimità dei pacchetti di dati rispetto ai modelli di riferimento dinamici. Questa metrica aiuta a rilevare deviazioni sottili e gradualmente nel traffico di rete.

Multi-Score Machine Learning

- **Precisione:** L'uso di più metriche consente di ottenere una visione più completa e accurata del traffico di rete, riducendo il rischio di falsi positivi.
- **Adattabilità:** I modelli di riferimento dinamici vengono costantemente aggiornati, permettendo al sistema di adattarsi rapidamente alle nuove condizioni di rete.
- **Rilevamento Tempestivo:** La combinazione di DPD e DFP permette di rilevare sia anomalie evidenti che sottili, migliorando la capacità di prevenire esfiltrazioni di dati.

La gestione dinamica dei modelli di riferimento e la regolazione del TimeToLive (TTL) sono fondamentali per mantenere l'efficacia del monitoraggio del traffico di rete in AdrenalineFX. Configurando correttamente questi parametri, gli utenti possono ottimizzare il sistema per adattarsi alle specifiche esigenze del loro

ambiente di rete, migliorando la precisione del rilevamento delle anomalie e riducendo i falsi positivi.

Conclusioni e Consigli per l'Uso

La configurazione ottimale del “TimeToLive” del modello dipende dalle esigenze specifiche dell'utente. In ambienti dove il traffico è soggetto a rapide variazioni, un “TimeToLive” più breve può ridurre i falsi positivi e migliorare la reattività del sistema. In contesti aziendali più stabili, un “TimeToLive” esteso fornisce una visione più robusta e coerente, ideale per identificare attività anomale che si sviluppano lentamente.

L'utente dovrebbe scegliere il “TimeToLive” in base al comportamento tipico del traffico della propria rete, bilanciando la sensibilità agli allarmi e la necessità di adattabilità nel monitoraggio delle potenziali esfiltrazioni di dati.

AdrenalineFX è uno strumento avanzato per la prevenzione dell'esfiltrazione di dati, fornendo gli strumenti necessari per monitorare, analizzare e reagire a potenziali minacce di sicurezza. Con una configurazione appropriata e un'analisi attenta, è possibile proteggere efficacemente la rete da tentativi di esfiltrazione di dati.

AdrenalineFX BenchMark

da completare