Adrenaline CryptoSentinel

Summary:

Adrenaline CryptoSentinel

Proactive Anti-Data-Exfiltration and Reactive Anti-Ransomware

Version 1.0 Release Candidate

Requirements:

- Microsoft Windows 10/11 x64
- PCAP Driver
- Sysmon64

Technologies Used:

- **Type of ADX**: Multi-Score Machine Learning / Proactive
- **Type of Anti-Ransomware**: Reactive
- **Network Layers**: Layer 3 / Layer 4
- **Conversions**: IP to ASN, IP to COUNTRY

Installed Services:

- AdrenalineMon5
- AdrenalineFX_Service
- AdrenalineFX_Firewall

Introduction

Adrenaline CryptoSentinel is an advanced software tool designed specifically to address two critical cybersecurity challenges:

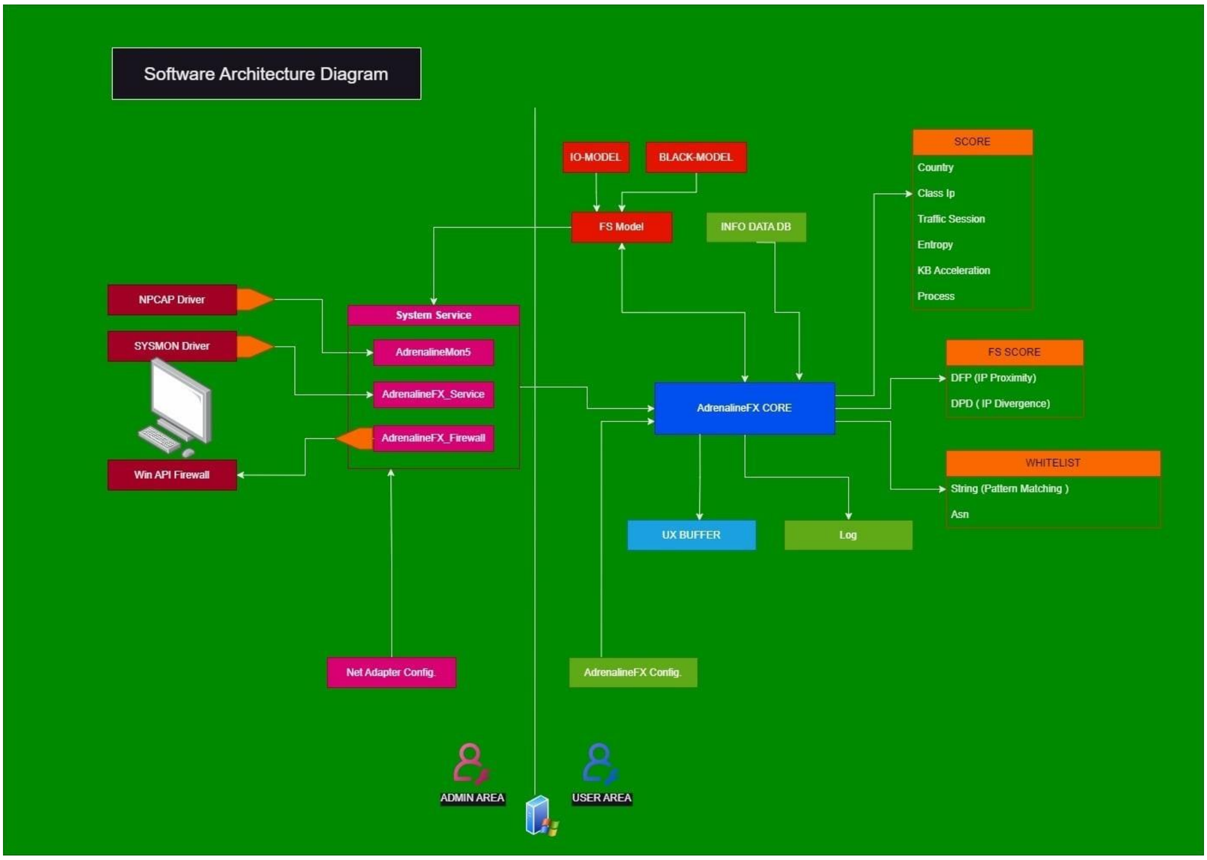
1. Detecting and preventing **data exfiltration**.
2. Mitigating **ransomware attacks**.

This manual will guide you through the core functionalities of the software, offering step-by-step instructions to effectively configure, monitor, and optimize its use in your environment.

With its cutting-edge architecture and features such as machine learning-based traffic analysis, dynamic data modeling, and reactive containment measures, **Adrenaline CryptoSentinel** serves as a robust solution to safeguard modern IT infrastructures against evolving threats.

System Architecture

The architecture of **Adrenaline CryptoSentinel** consists of several key components designed to work seamlessly together for monitoring and analyzing network traffic. Its modular structure enables precise and timely detection of network anomalies and potential threats.



Core Components:

1. **AdrenalineFX Engine**:
    a. The core system for detecting and mitigating **data exfiltration** attempts.
    b. Utilizes **dynamic models** to analyze network patterns in real time.
2. **AdrenalineRX Engine**:
    a. Focused on **ransomware detection** and mitigation.
    b. Uses a combination of **file entropy analysis**, **canary files**, and I/O monitoring.
3. **Network Traffic Monitor**:
    a. Captures and inspects traffic on **DNS**, **ICMP**, **NETBIOS**, and other protocols.

   b. Works at **Layer 3 (Network)** and **Layer 4 (Transport)** for deep packet inspection.

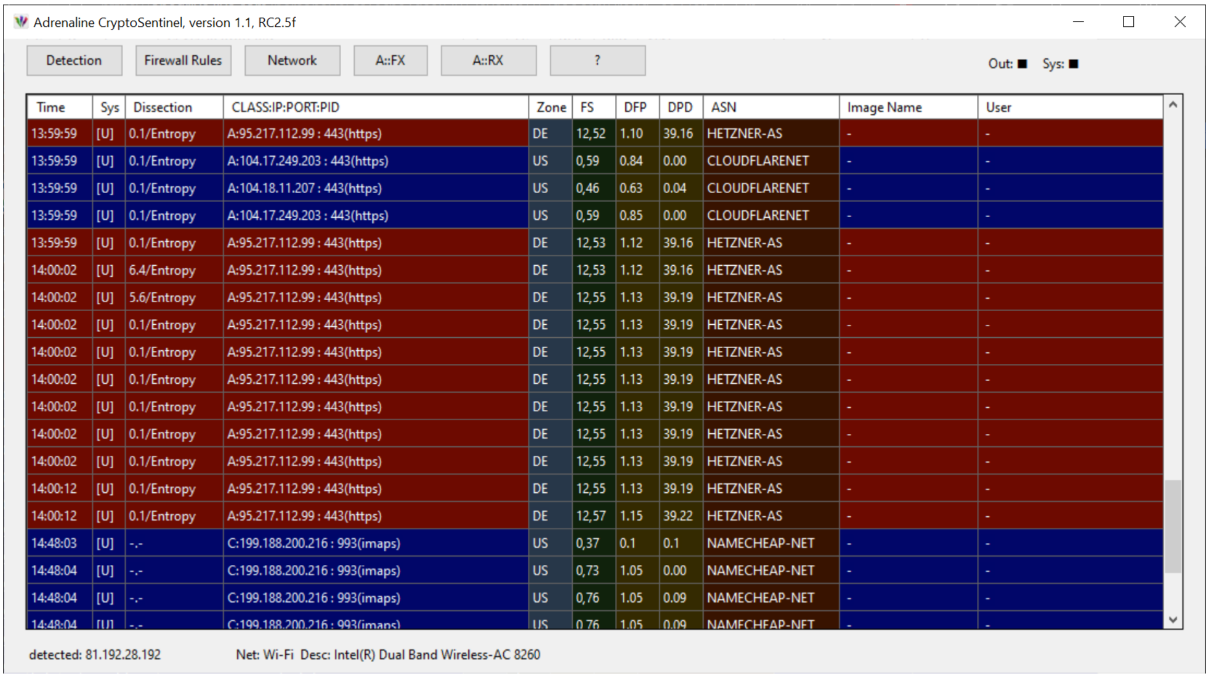
4. **Firewall Rule Manager**:
   a. Dynamically updates Windows Firewall rules to block suspicious IPs or applications.
5. **Machine Learning Models**:
   a. Multi-score evaluation system combining **DFD (Data Flow Divergence)** and **DPD (Data Pattern Divergence)** metrics.
6. **User Interface (UX Buffer)**:
   a. Displays up-to-date logs of network traffic and system activity.
   b. Color-coded entries to quickly identify critical events.

Key Benefits of the Architecture:

- **Proactive Detection**: Identifies suspicious behavior before it escalates into critical incidents.
- **Scalability**: Modular design ensures the system can adapt to various network sizes and configurations.
- **Dynamic Modeling**: Continuously updates traffic baselines to reflect current network conditions.
- **Ease of Use**: Offers an intuitive interface for configuring, monitoring, and responding to threats.

User Interface

The **Adrenaline CryptoSentinel** user interface is designed to provide intuitive access to system controls and real-time monitoring of network traffic. The main screen displays key operational metrics and enables quick navigation between different configuration and analysis panels.



Time	Sys	Dissection	CLASS:IP:PORT:PID	Zone	FS	DFP	DPD	ASN	Image Name	User
13:59:59	[U]	0.1/Entropy	A:95.217.112.99 : 443(https)	DE	12,52	1.10	39.16	HETZNER-AS	-	-
13:59:59	[U]	0.1/Entropy	A:104.17.249.203 : 443(https)	US	0,59	0.84	0.00	CLOUDFLARENET	-	-
13:59:59	[U]	0.1/Entropy	A:104.18.11.207 : 443(https)	US	0,46	0.63	0.04	CLOUDFLARENET	-	-
13:59:59	[U]	0.1/Entropy	A:104.17.249.203 : 443(https)	US	0,59	0.85	0.00	CLOUDFLARENET	-	-
13:59:59	[U]	0.1/Entropy	A:95.217.112.99 : 443(https)	DE	12,53	1.12	39.16	HETZNER-AS	-	-
14:00:02	[U]	6.4/Entropy	A:95.217.112.99 : 443(https)	DE	12,53	1.12	39.16	HETZNER-AS	-	-
14:00:02	[U]	5.6/Entropy	A:95.217.112.99 : 443(https)	DE	12,55	1.13	39.19	HETZNER-AS	-	-
14:00:02	[U]	0.1/Entropy	A:95.217.112.99 : 443(https)	DE	12,55	1.13	39.19	HETZNER-AS	-	-
14:00:02	[U]	0.1/Entropy	A:95.217.112.99 : 443(https)	DE	12,55	1.13	39.19	HETZNER-AS	-	-
14:00:02	[U]	0.1/Entropy	A:95.217.112.99 : 443(https)	DE	12,55	1.13	39.19	HETZNER-AS	-	-
14:00:02	[U]	0.1/Entropy	A:95.217.112.99 : 443(https)	DE	12,55	1.13	39.19	HETZNER-AS	-	-
14:00:02	[U]	0.1/Entropy	A:95.217.112.99 : 443(https)	DE	12,55	1.13	39.19	HETZNER-AS	-	-
14:00:02	[U]	0.1/Entropy	A:95.217.112.99 : 443(https)	DE	12,55	1.13	39.19	HETZNER-AS	-	-
14:00:12	[U]	0.1/Entropy	A:95.217.112.99 : 443(https)	DE	12,55	1.13	39.19	HETZNER-AS	-	-
14:00:12	[U]	0.1/Entropy	A:95.217.112.99 : 443(https)	DE	12,57	1.15	39.22	HETZNER-AS	-	-
14:48:03	[U]	-.-	C:199.188.200.216 : 993(imaps)	US	0,37	0.1	0.1	NAMECHEAP-NET	-	-
14:48:04	[U]	-.-	C:199.188.200.216 : 993(imaps)	US	0,73	1.05	0.00	NAMECHEAP-NET	-	-
14:48:04	[U]	-.-	C:199.188.200.216 : 993(imaps)	US	0,76	1.05	0.09	NAMECHEAP-NET	-	-
14:48:04	[U]	-.-	C:199.188.200.216 : 993(imaps)	US	0,76	1.05	0.09	NAMECHEAP-NET	-	-

detected: 81.192.28.192

Net: Wi-Fi Desc: Intel(R) Dual Band Wireless-AC 8260

UX-BUFFER

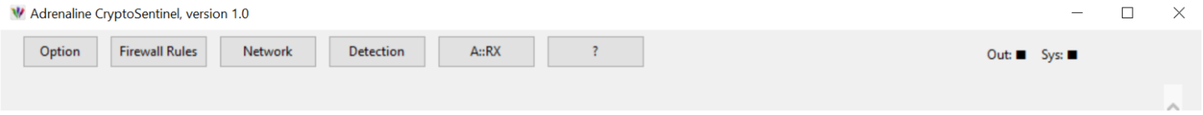
The **UX-BUFFER** displays the last 25 log entries in a scrolling format. Each entry provides detailed information about the analyzed network traffic, including:

- **FS (Flow Score)**: Represents the severity of the data flow.
  - To enable: *Options → FS (Flow Score) → "Use"*
- **T (Time)**: Timestamp of the detected event.
- **Entropy**: Measures whether the packet contains encrypted or compressed data.
- **DPD (Data Pattern Divergence):** Indicates deviation from the expected behavior.
- **DFP (Data Flow Proximity)**: Shows proximity to a known IP model over a defined time frame.
- **CLASS**: IP classification.
- **COUNTRY**: Destination country of the IP.
- **IP**: Displays the IP address and port of the flow.
- **ASN (Autonomous System Number)**: Uniquely identifies the network associated with the IP.

- **IMG (Image):** Indicates the application or service sending the data.
- **USER**: Displays the username of the system operator.

Main Interface Description

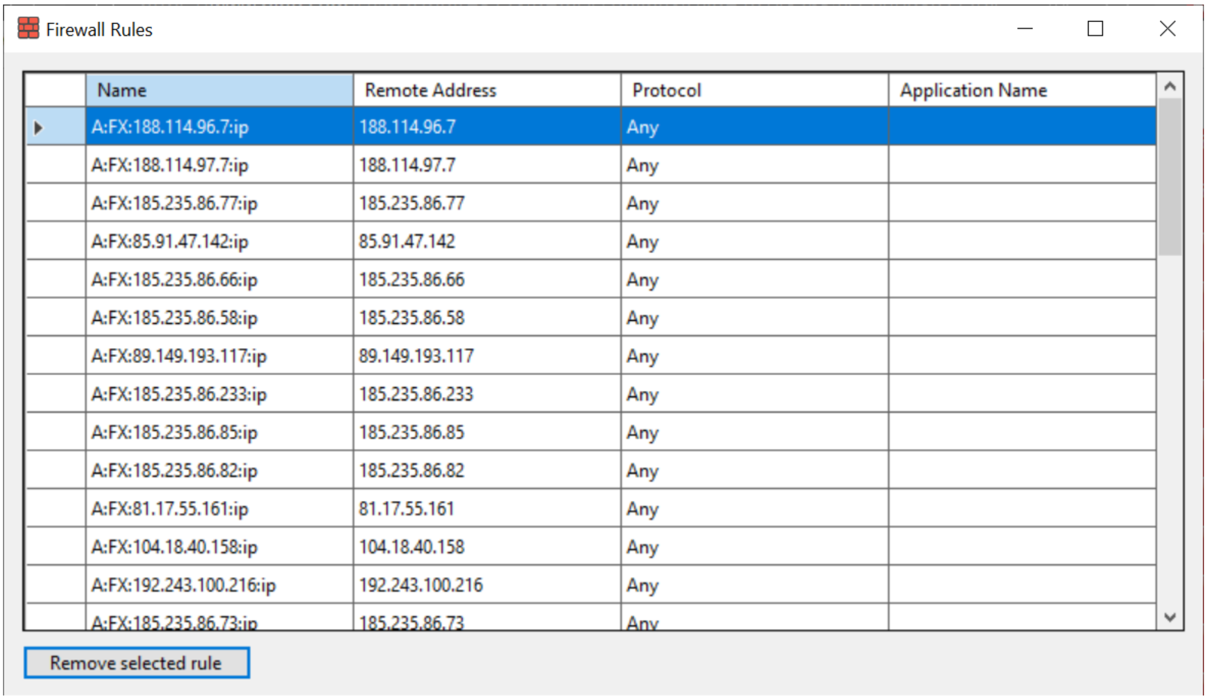
The main interface includes various tabs and buttons to optimize the monitoring and management of network traffic:



1. **Buttons**:
    a. **Options**: Opens the configuration panel.
    b. **Firewall Rules**: Accesses and manages firewall rule settings.
    c. **Network ID**: Allows interface selection.
    d. **Detections**: Displays logged detection events.
    e. **A::RX**: Opens the anti-ransomware control panel.
    f. **?**: Provides access to help and documentation.
2. **Virtual LEDs**:
    a. Status indicators for incoming and outgoing data.
3. **UX-BUFFER**:
    a. Logs entries with a color-coded system for critical events.
4. **Status Bar**:
    a. Displays system status and relevant information.

Firewall Rules Management

The **Firewall Rules** panel allows users to configure and manage the firewall settings applied by **Adrenaline CryptoSentinel**. The system automatically creates rules to block IP addresses or processes when a high-risk score is detected. These rules are customizable through the interface for better control and adaptability.



	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	

Key Features:

- **Automatic Rule Creation**:
  - AdrenalineFX generates outbound firewall rules to block suspicious traffic at the **IP** or **application** level.
- **Rule Removal**:
  - Users can select and remove unwanted firewall rules directly from the panel.

Panel Layout:

- **Name**: Displays the rule name and the associated user.
- **Remote Address**: Shows the remote IP address targeted by the rule.
- **Protocol**: Indicates the protocol used (e.g., TCP, UDP).

- **Application Name**: Specifies the blocked application's name.

How to Remove a Rule:

1. Open the **Firewall Rules** panel.
2. Select the rule you wish to remove.
3. Click the **Remove Selected Rule** button at the bottom of the panel.

How It Works:

1. AdrenalineFX dynamically monitors network traffic for suspicious behavior.
2. When an anomaly is detected, the system generates a blocking rule targeting either:
    a. The specific **IP address** involved in the suspicious activity.
    b. The **application** responsible for the outbound connection.
3. These rules are enforced at the operating system level via **Windows Firewall**, ensuring immediate containment.

Best Practices:

- **Whitelist Management**:
    - If an IP is whitelisted, ensure the corresponding firewall rule is removed to avoid conflicts.
- **Regular Rule Review**:
    - Periodically check the list of active rules to ensure no critical connections are unintentionally blocked.

Network Interface Selection

The **Select Network Interface** panel allows you to choose the network interface to monitor. This is essential for configuring **Adrenaline CryptoSentinel** to capture traffic from the correct source.

How to Select a Network Interface:

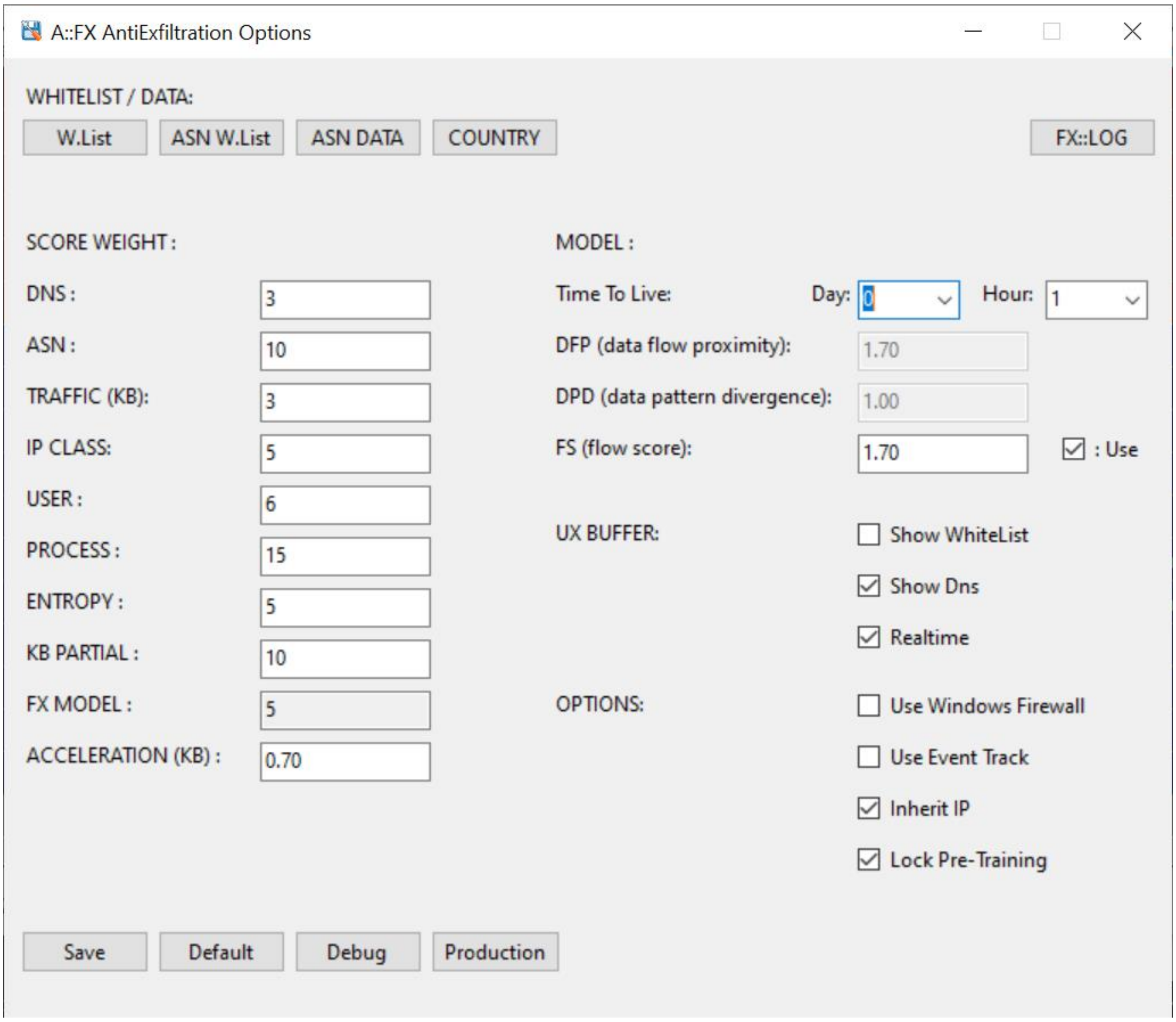
1. Open the **Network Interface Selection** panel.
2. Review the list of available interfaces.
3. Select the appropriate interface for your monitoring needs.
4. Click the **Select** button to confirm.
    a. The control panel will close automatically.
    b. Within a few seconds, the selected interface's status will update in the main interface.

Important Notes:

- **Administrative Privileges**:
    - Only users with administrator rights can modify network interface settings in **Adrenaline CryptoSentinel**.
- **Status Updates**:
    - After selecting an interface, verify that status changes appear in the main interface to ensure proper configuration.

Options Panel

The **Options Panel** provides advanced configuration settings for **AdrenalineFX**, allowing you to tailor the software's behavior to specific operational needs.



WHITELIST / DATA:

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 :

Time To Live: Day: 0 Hour: 1

DFP (data flow proximity): 1.70

DPD (data pattern divergence): 1.00

FS (flow score): 1.70 ☑ : Use

UX BUFFER:

☐ Show WhiteList

☑ Show Dns

☑ Realtime

OPTIONS:

☐ Use Windows Firewall

☐ Use Event Track

☑ Inherit IP

☑ Lock Pre-Training

UX_BUFFER Parameters

These settings control how the **UX_BUFFER** displays and logs network traffic data:

1. **Show WhiteList**:
    a. Enables the display of packets marked as legitimate.
    b. Disable this option to reduce noise in the UX_BUFFER output.
2. **Show DNS**:
    a. Displays DNS-related logs generated by Sysmon (Event ID 22).
    b. Recommended to disable this option in production environments.
3. **Realtime UX**:

    a. Enables real-time packet visualization in the UX_BUFFER.
    b. Recommended to disable this in production to improve performance.

Note:

The **UX_BUFFER** consists of 25 real-time rows to aid debugging and alarm management. For detailed analysis, refer to the log files.

Options Parameters

These global settings control the behavior of **AdrenalineFX**:

1. **Use Windows Firewall**:
    a. Enables automatic rule generation and insertion into **Windows Defender Firewall** to block suspicious traffic.
2. **Inherit IP**:
    a. Allows IP addresses previously whitelisted to remain whitelisted for subsequent detections.
3. **Lock Pre-Training**:
    a. Freezes the pre-training phase to maintain the current model without further adjustments.
    b. See the **Pre-Training** section for more details.

Using AdrenalineFX to Detect Data Exfiltration

The **AdrenalineFX engine**, integrated into **Adrenaline CryptoSentinel**, is designed to detect potential data exfiltration attempts through in-depth network traffic analysis. Follow these steps to effectively utilize the software for detecting suspicious activity:

Setup and Preparation

1. **Verify Prerequisites**:
    a. Ensure the **npcap** or **win10cap** driver is installed and operational.
    b. Confirm that **Sysmon** is correctly installed and running.
2. **Select the Network Interface**:
    a. Use the **Network** tab to choose the appropriate interface for monitoring.
3. **Start Monitoring**:

   a. Activate the monitoring process and verify that traffic logs appear in the **UX_BUFFER**.

Monitoring Data

1. **Log Overview**:
   a. Use the **Detections** tab to monitor blocked IPs and other detection events.
   b. Refer to the **Firewall Rules** tab to review IPs or applications flagged and blocked by the system.
2. **Whitelist Management**:
   a. If an IP is added to the whitelist, remember to manually remove it from the firewall to avoid blocking legitimate traffic.

Detection Indicators

The following metrics are key to interpreting data in the **Model Viewer** and **UX_BUFFER**:

1. **AN (Anomaly Score)**:
   a. Experimental metric that indicates the overall risk level associated with a data flow.
2. **FS (Flow Score)**:
   a. Represents the severity of a particular data flow.
3. **Entropy**:
   a. Identifies encrypted or compressed data within the traffic.
4. **DPD (Data Pattern Divergence)**:
   a. Measures deviations from expected network behavior over a defined time period.
5. **DFP (Data Flow Proximity)**:
   a. Indicates the proximity of the traffic to known IP models over a defined time period.

Adjusting Detection Parameters

- The **Flow Score (FS)** threshold can be customized in the **Options** panel to better align with your environment.
- The **DPD** and **DFP** parameters can also be fine-tuned individually to improve detection accuracy.

Pre-Training

The **Pre-Training** process in **Adrenaline CryptoSentinel** leverages **Sysmon data** and cross-references it with entries in the whitelist (**W.List**) to establish a baseline for legitimate network activity. This helps the system filter out noise and focus on identifying genuine threats.

How Pre-Training Works

1. **Initialization**:
   a. Pre-training automatically starts when **Adrenaline CryptoSentinel** is launched.
   b. It uses Sysmon data to learn and classify benign activity during the initial operation phase.
2. **Whitelist Integration**:
   a. The whitelist accepts any string that matches entries appearing in the **UX_BUFFER** or logs.
   b. Legitimate network traffic is excluded from detection during this training phase.
3. **Locking Pre-Training**:
   a. Once sufficient training data has been collected (typically within seconds), the process can be locked by enabling the **Lock Pre-Training** option in the **Options** panel.

Usage Tips

- **Enable Inheritance**:
  - Ensure the **inherit IP** option is active for the system to retain whitelisted entries and reduce noise.
- **End Pre-Training When Ready**:
  - Stop pre-training once the system has learned your network's normal activity. This minimizes the risk of legitimate traffic being flagged as suspicious.

Note: Pre-training can be disabled entirely by unchecking the **inherit IP** option in the configuration settings.

Configuration Options

The configuration options in **Adrenaline CryptoSentinel** allow users to fine-tune the system for optimal performance based on specific network environments. These settings help improve detection accuracy, reduce false positives, and adapt to dynamic traffic patterns.

Accessing the Options Menu

1. Open the **Options Panel** from the main interface.
2. Navigate through the different parameters to adjust settings as needed.

Key Configuration Parameters

1. **TimeToLive (TTL)**:
   a. Determines the lifespan of the system's traffic analysis models.
   b. A shorter TTL ensures frequent updates, which improves sensitivity to changes in network behavior.
   c. A longer TTL provides more robust baseline models for networks with stable traffic patterns.
2. **DPD (Data Pattern Divergence) and DFP (Data Flow Proximity)**:
   a. These metrics dynamically adapt to network traffic, helping identify deviations or anomalies.
   b. Adjust the sensitivity of these parameters to reflect your network's typical activity.
3. **Flow Score (FS)**:
   a. Combines DFP and DPD to generate an overall threat score.
   b. Thresholds can be adjusted in the **Options Panel** to match your preferred sensitivity levels.

Best Practices

- **Dynamic Adjustment**:
  - In environments with rapidly changing traffic, use a shorter TTL for real-time updates.

    - In more stable environments, extend the TTL to focus on long-term anomalies.
- **Fine-Tuning Sensitivity**:
    - Test different FS thresholds during initial deployment to find the optimal balance between sensitivity and false positives.
- **Regular Model Updates**:
    - Ensure the dynamic models (DPD/DFP) are recalibrated periodically, especially after significant network changes.

Event Generation in MS Windows

AdrenalineFX integrates seamlessly with Microsoft Windows to log critical security events. These events provide detailed insights into network traffic anomalies and system activities, aiding in threat detection and forensic analysis.

How Events Are Generated

1. **Integration with Sysmon**:
    a. Events are captured and logged using **Sysmon**, a powerful tool for monitoring system-level activities.
    b. Specific event types, such as DNS queries or network connections, are recorded for further analysis.
2. **Dynamic Event Logging**:
    a. **AdrenalineFX** generates events based on the detected severity level of network traffic anomalies.
    b. Events are categorized to prioritize critical alerts, such as high-risk data flows or potential ransomware activities.
3. **Windows Event Viewer**:
    a. Logs are available in the **Windows Event Viewer** under custom entries created by AdrenalineFX.
    b. Each event includes comprehensive details such as timestamp, IP addresses, protocols, and scores (e.g., FS, DPD, DFP).

Benefits of Event Logging

- **Real-Time Monitoring**:

    - Events are logged as soon as anomalies are detected, ensuring timely visibility into potential threats.
- **Forensic Analysis**:
    - Detailed logs provide critical information for investigating incidents post-detection.
- **System Adaptability**:
    - Logged events help refine detection models, improving system performance over time.

Optimizing Event Generation

- **Log Filtering**:
    - Adjust Sysmon configuration files to exclude low-priority events, reducing noise in the logs.
- **Severity-Based Alerts**:
    - Customize the system to generate alerts only for events exceeding specific threat thresholds.
- **Export for Analysis**:
    - Export logs to external SIEM (Security Information and Event Management) systems for centralized analysis.

Time-to-Live (TTL) Management in AdrenalineFX

The **Time-to-Live (TTL)** parameter plays a critical role in real-time traffic monitoring and anomaly detection in **AdrenalineFX**. By ensuring that the system continuously evaluates current network conditions, TTL helps maintain accurate and relevant analysis.

What is Time-to-Live (TTL)?

In networking, **TTL** is a value assigned to data packets to define their lifespan. Each time a packet passes through a router, its TTL decreases. Once the TTL reaches zero, the packet is discarded. This mechanism prevents packets from circulating indefinitely in a network.

In the context of AdrenalineFX, TTL determines the active lifespan of analysis models used to evaluate network traffic patterns.

Importance of TTL in AdrenalineFX

1. **Removing Obsolete Data**:
    a. TTL ensures that outdated traffic data is discarded, keeping the analysis focused on recent activity.
2. **Reducing False Positives**:
    a. By avoiding the evaluation of expired packets, TTL minimizes the risk of flagging irrelevant traffic as suspicious.
3. **Continuous Updates**:
    a. TTL-driven model refreshes ensure the system adapts to changing network conditions, enhancing detection accuracy.

How TTL Works in AdrenalineFX

1. **Model Refresh**:
    a. When the TTL of a model expires, AdrenalineFX regenerates the analysis model, incorporating only valid and current data.
2. **Dynamic Adaptation**:
    a. TTL settings can be adjusted to suit different environments:
        i. Shorter TTL: Ideal for high-traffic, dynamic networks.

        ii. Longer TTL: Suitable for stable environments where changes occur less frequently.

Best Practices for TTL Configuration

1. **Short TTL for Dynamic Networks**:
    a. Use shorter TTL values in environments with fluctuating traffic patterns, such as cloud-based systems or high-activity enterprise networks.
2. **Long TTL for Stable Networks**:
    a. Configure longer TTL values for static environments, such as small office networks, to maintain consistent baselines.
3. **Regular Adjustments**:
    a. Periodically review TTL settings to ensure they align with network behavior and reduce the risk of false positives or missed detections.

Dynamic Models and DFP/DPD Variability

AdrenalineFX utilizes dynamic traffic models to continuously adapt and respond to the evolving network environment. The dynamic models help ensure that network behavior is accurately monitored, and anomalies are detected in real-time. This section explains how these models work and how the **DFP (Data Flow Proximity)** and **DPD (Data Pattern Divergence)** metrics are used to monitor network traffic.

Dynamic Reference Models

In **Adrenaline CryptoSentinel**, the **dynamic reference models** serve as benchmarks for evaluating ongoing network activity. These models are continuously updated and replaced at regular intervals defined by the user. This constant refresh ensures that the analysis remains accurate and reflects current traffic patterns.

Adjusting the Model's Time-to-Live (TTL)

1. **TTL of the Model**:
    a. The TTL for dynamic models determines how long a model remains active before being replaced. This directly impacts the sensitivity of **DFP** and **DPD** metrics.

2. **TTL Impact**:
    a. A shorter TTL will cause the models to refresh more frequently, ensuring they remain aligned with recent traffic. However, this may result in more frequent updates that could increase processing time in dynamic environments.
    b. A longer TTL allows for more stability in the models, ideal for environments with relatively stable network traffic.

Behavior of DFP and DPD Values

The **DFP (Data Flow Proximity)** and **DPD (Data Pattern Divergence)** metrics are used to monitor deviations in network traffic. These metrics adjust dynamically based on the traffic patterns observed.

1. **DFP (Data Flow Proximity)**:
    a. Measures how closely current data flows resemble known, legitimate traffic models.
    b. **Higher values** indicate that the current traffic deviates from expected models, suggesting potential anomalies.
    c. **Lower values** indicate that the traffic closely matches the normal pattern, signaling no suspicious activity.
2. **DPD (Data Pattern Divergence)**:
    a. Measures the divergence of the current traffic from expected network behavior over a specified time period.
    b. **Increased DPD** values indicate significant deviations from the normal pattern, often associated with potential threats like data exfiltration or ransomware.
    c. **Decreased DPD** values suggest that the traffic is behaving normally according to the model.

Adjusting DFP and DPD Sensitivity

1. **Dynamic Adjustment**:
    a. **DFP** and **DPD** can be adjusted based on the desired sensitivity.
    b. Use these adjustments to fine-tune detection for environments with rapidly changing traffic or for more stable, low-traffic networks.
2. **Thresholds**:

    a. Set threshold values for **DFP** and **DPD** to trigger alerts when traffic exceeds normal levels. These thresholds can be tailored based on your network's traffic behavior and security needs.

Best Practices for Dynamic Models

1. **Shorter TTL for Dynamic Networks**:
    a. In environments where traffic patterns change frequently (e.g., cloud-based systems), use a shorter TTL to ensure models are always up to date.
2. **Longer TTL for Stable Environments**:
    a. In stable, low-traffic environments, use a longer TTL to avoid excessive model refreshing, which may not be necessary.
3. **Adjust DFP and DPD Sensitivity**:
    a. Continuously monitor and adjust the DFP and DPD thresholds to ensure they are sensitive enough to detect threats while avoiding false positives.

Multi-Score Machine Learning

The **Multi-Score Machine Learning** approach in **AdrenalineFX** provides an advanced method for detecting and preventing data exfiltration by evaluating network traffic through multiple metrics. This approach ensures higher accuracy and faster detection by combining different indicators to create a comprehensive view of the network's security posture.

How Multi-Score Machine Learning Works

1. **Combination of Metrics**:
    a. Instead of relying on a single metric, **AdrenalineFX** uses a combination of **DFD (Data Flow Divergence)**, **DPD (Data Pattern Divergence)**, and **FS (Flow Score)** to assess the network traffic comprehensively.
    b. These combined metrics provide a more nuanced and accurate evaluation of potential threats.
2. **Continuous Learning**:
    a. The system continuously updates its models to reflect the most recent network traffic, improving its ability to detect new and evolving threats.
    b. Machine learning algorithms adapt based on past behaviors and current traffic patterns to optimize detection accuracy.

Metrics Used in Multi-Score Machine Learning

1. **DFD (Data Flow Divergence)**:
    a. Measures the distance between the current data flow and established legitimate patterns using the **Euclidean distance**.
    b. Useful for identifying large deviations in packet behavior that may indicate malicious activity.
2. **DPD (Data Pattern Divergence)**:
    a. Monitors subtle, gradual changes in network behavior.
    b. Helps detect anomalies that are not immediately obvious but could indicate long-term data exfiltration or compromised traffic.
3. **FS (Flow Score)**:
    a. A composite score that combines the outputs of DPD and DFD, offering a holistic view of the security of the network flow.
    b. Provides a comprehensive risk score, making it easier to identify potential threats.

Benefits of Multi-Score Machine Learning

1. **Precision**:
    a. The combination of multiple metrics ensures that the system can detect a wide range of anomalies, from major attacks to subtle, ongoing exfiltration attempts.
    b. Reduces false positives by cross-referencing multiple indicators before triggering an alarm.
2. **Adaptability**:
    a. The system continuously learns from new traffic patterns, allowing it to adjust to the dynamic nature of modern networks.
    b. Regular updates to reference models ensure that the detection algorithms remain effective against evolving threats.
3. **Timely Detection**:
    a. By using multiple metrics, **AdrenalineFX** can detect both immediate threats and long-term anomalies, allowing for timely responses to attacks in progress.

Best Practices for Using Multi-Score Machine Learning

1. **Fine-Tuning Thresholds**:
    a. Regularly adjust the **FS** threshold to balance between sensitivity and false positives. Lower thresholds may increase the detection rate but may also trigger more alerts.
2. **Monitoring and Adjusting Metrics**:
    a. Continuously monitor the performance of **DFD** and **DPD** in real-time traffic. Adjust these values based on the traffic behavior of your network for the most accurate results.
3. **Use in Combination with Other Detection Techniques**:
    a. Combine the multi-score approach with other detection methods, such as **DNS** or **ICMP analysis**, for a more comprehensive security posture.

Sysmon Installation

Sysmon (System Monitor) is a powerful tool from the **Sysinternals Suite** that provides detailed logs of system activity. It is essential for monitoring system processes, network connections, and detecting suspicious activities. **Adrenaline CryptoSentinel** uses Sysmon to enhance data exfiltration detection and provide detailed information for forensic analysis.

Downloading and Installing Sysmon

1. **Download Sysmon**:
   a. Visit the **Sysinternals website** to download the Sysmon package.
2. **Extract the Package**:
   a. After downloading the ZIP file, extract it to a temporary directory of your choice.
   b. Move the extracted contents to the **C:\Sysinternals\Sysmon** folder.
3. **Open Command Prompt as Administrator**:
   a. Search for **"cmd"** or **"Command Prompt"** in the Start menu.
   b. Right-click and select **"Run as Administrator"**.
4. **Install Sysmon**:
   a. Navigate to the folder where Sysmon is located:

```
cd C:\Sysinternals\Sysmon
```

   b. Run the following command to install Sysmon with the configuration file:

```
Sysmon64.exe -accepteula -i dns.xml
```

Configuring Sysmon with Custom Settings

1. **Create the `dns.xml` File**:
   a. Sysmon uses configuration files to define which events to monitor.
   b. Create an empty **dns.xml** file and copy the following content:

```
<Sysmon schemaversion="4.90">
  <EventFiltering>
    <DnsQuery onmatch="exclude"/>
    <NetworkConnect onmatch="exclude"/>
  </EventFiltering>
</Sysmon>
```

2. **Modify the Configuration File**:
    a. If needed, modify the **dns.xml** file to include additional event types you want to monitor (e.g., network connections or process creations).
    b. Ensure the configuration file is located in the same folder as the Sysmon executable.

Uninstalling and Updating Sysmon

1. **Uninstall Sysmon**:
    a. To uninstall Sysmon, run the following command:

```
sysmon -u
```

2. **Updating Sysmon**:
    a. To update Sysmon, uninstall the previous version and follow the installation steps again with the new version.

Verifying Sysmon Installation

1. **Check Windows Event Viewer**:
    a. Sysmon logs events in the **Windows Event Viewer**.
    b. Open the Event Viewer and navigate to **Applications and Services Logs** → **Microsoft** → **Windows** → **Sysmon** to check for event entries.
2. **Verify Services**:
    a. Ensure that the **Sysmon** service is running properly by checking the list of services or using the **task manager**.

PCAP Driver Installation for Windows 10

The **PCAP Driver** (Packet Capture Driver) is essential for capturing network traffic on Windows systems. It is used by **Adrenaline CryptoSentinel** to inspect incoming and outgoing network packets for suspicious activity. This section explains how to download, install, and configure the PCAP driver for use with **AdrenalineFX**.

Installing WinPcap

1. **Download WinPcap**:
   a. Visit the official **WinPcap website** and download the latest version of the driver.
   b. You can download it from: https://www.winpcap.org/
2. **Run the Installer**:
   a. Open the downloaded installer and follow the on-screen instructions to complete the installation.
   b. Ensure that the installation completes successfully and that the **WinPcap** driver is installed on your system.

Installing Npcap (for Windows 10 and newer)

While **WinPcap** is still supported, it is recommended to install **Npcap** as it provides improved performance and security features. **Npcap** is compatible with **Windows 10/11** and works better with modern network interfaces.

1. **Download Npcap**:
   a. Visit the **Npcap website**: https://nmap.org/npcap/
   b. Download the latest version of Npcap.
2. **Run the Installer**:
   a. Launch the downloaded installer and follow the instructions.
   b. During installation, select the option **"Install Npcap in WinPcap API-compatible Mode"** to maintain compatibility with WinPcap-based applications.

Network Traffic Analysis Setup

The **Network Traffic Analysis Setup** is an essential step in configuring **Adrenaline CryptoSentinel** to monitor and analyze network traffic for potential threats. This section outlines how to configure the system to capture, analyze, and interpret network data to detect anomalies, including data exfiltration and ransomware attempts.

Initial Setup

1. **Select the Network Interface**:
   a. Open the **Network Interface Selection** panel and choose the correct network interface for monitoring.
   b. Ensure the interface selected is the one responsible for the traffic you wish to analyze (e.g., Ethernet, Wi-Fi).
2. **Configure Packet Capture Settings**:
   a. In the **Options Panel**, enable the packet capture settings for the protocols you want to monitor (DNS, ICMP, NETBIOS, etc.).
   b. For optimal analysis, ensure that **AdrenalineFX** is configured to monitor at **Layer 3 (Network)** and **Layer 4 (Transport)**.
3. **Verify Capture Path**:
   a. Ensure that the path for packet capture is correctly configured. This path determines where the captured data will be stored temporarily.
   b. **AdrenalineFX** uses a **PCAP driver** to intercept network packets. Ensure that **WinPcap** or **Npcap** is installed and functioning correctly.

Monitoring and Analyzing Network Traffic

1. **Traffic Log Visualization**:
   a. After setting up the capture path, use the **UX_BUFFER** to visualize the traffic in real-time. The buffer will display network packets with associated metrics like **FS (Flow Score)**, **Entropy**, and **DPD (Data Pattern Divergence)**.
   b. Pay close attention to **high-risk flows**, where the **FS** score exceeds predefined thresholds.
2. **Identify Suspicious Patterns**:
   a. Look for unusual data patterns or irregular packet sizes. For instance, **DNS tunneling** often involves packets that are unusually large for DNS queries or exhibit strange encoding patterns in the payload.

    b. **ICMP** traffic may be indicative of **data exfiltration**, especially if the flow is abnormally frequent or carries excessive payload data.

3. **Inspect Network Alerts**:
    a. When suspicious behavior is detected, **AdrenalineFX** will trigger alerts in the **Detections** panel. Each alert includes details such as the source and destination IPs, traffic type, and risk score.
    b. Review these alerts and check if the flagged traffic corresponds to legitimate network activity or potential threats.

Customizing Traffic Analysis

1. **Set Protocol-Specific Filters**:
    a. In the **Options Panel**, configure **protocol filters** to focus on specific types of traffic, such as DNS, ICMP, or HTTP.
    b. **AdrenalineFX** provides customizable filtering to analyze traffic from known attack vectors like **DNS tunneling** or **ICMP flooding**.
2. **Advanced Settings**:
    a. Adjust the **Flow Score** threshold to fine-tune the detection sensitivity. Lowering the threshold will increase the likelihood of detecting suspicious traffic but may also raise the number of false positives.
    b. Increase the threshold for environments with stable network traffic to reduce unnecessary alerts.

Real-Time Analysis and Alerts

1. **Real-Time Monitoring**:
    a. Once network traffic analysis is configured, **AdrenalineFX** will continuously monitor incoming and outgoing data flows. The system will use **dynamic models** to evaluate deviations from normal patterns in real-time.
2. **Alerts and Actions**:
    a. If the system detects an anomaly above a set threshold, it will generate an alert. Actions such as blocking the suspicious IP or application can be automatically triggered via the **Firewall Rules**.
3. **Event Logs**:
    a. Log entries related to network traffic anomalies can be accessed through the **Windows Event Viewer** under the **Sysmon** logs. These entries provide detailed information for forensic analysis.

Best Practices for Traffic Analysis

1. **Regular Review of Logs**:
    1. Regularly review traffic logs to identify emerging threats or unusual activity patterns. Pay special attention to any new traffic behavior that deviates from established baselines.
2. **Use Alerts Wisely**:
    1. Fine-tune alert thresholds to ensure only critical anomalies are flagged. Set **Flow Score** thresholds high enough to avoid overwhelming the system with non-critical events.
3. **Adjust Protocol-Specific Rules**:
    1. Customize protocol monitoring rules to match your network's characteristics. If your environment is more likely to experience **DNS tunneling**, increase the sensitivity for DNS traffic analysis.

Response to Detected Threats

AdrenalineFX provides tools to not only detect network anomalies and suspicious traffic but also to respond proactively to these threats. This section explains the steps you should take when a threat is detected, including mitigation strategies and how to configure automatic responses.

Automatic Threat Response

1. **Triggering Firewall Rules**:
    1. When suspicious traffic is detected, **AdrenalineFX** can automatically generate **firewall rules** to block the source IP or the application associated with the threat.
    2. The system uses the **Flow Score (FS)** and **Data Pattern Divergence (DPD)** metrics to determine the severity of the detected threat. If the traffic exceeds predefined thresholds, it triggers an automatic rule to block the suspicious connection.
2. **Blocking Suspicious IPs**:
    1. When **high-risk traffic** is detected, the system will automatically add the offending **IP address** to the blocklist. This helps prevent further communication with malicious sources.
    2. The **Firewall Rule Manager** allows you to review and remove any IP block if false positives are detected.

3. **Stopping Malicious Applications**:
    a. **AdrenalineFX** can block the application that generated suspicious traffic. For example, if a legitimate application suddenly starts generating abnormal data flows (e.g., DNS tunneling or large ICMP requests), it can be blocked at the application level.
    b. This process is integrated with the **Windows Firewall**, allowing the application to be quarantined or completely blocked.

Manual Response Actions

While automated responses are crucial, there are situations where manual intervention may be necessary. Here's how you can manually respond to a detected threat:

1. **Review the Threat Logs**:
    a. Navigate to the **Detections** panel and carefully review the details of the detected threat. Information such as **Flow Score**, **IP addresses**, and **Protocol type** will help you assess the severity of the threat.
    b. For a more detailed analysis, review the **Sysmon logs** for event IDs related to the anomaly.
2. **Whitelist Trusted Traffic**:
    a. If legitimate traffic has been mistakenly flagged, you can whitelist the corresponding **IP address** or **application** to prevent future alerts.
    b. Whitelisted items can be reviewed and managed in the **Options Panel**.
3. **Respond Using Firewall Rules**:
    a. You can manually add or modify firewall rules based on the threat you are reviewing.
    b. Go to the **Firewall Rules** section to block or allow specific IP addresses or applications.
4. **Investigation and Forensics**:
    a. If you suspect that the detected threat is part of a larger attack, start an investigation by analyzing the captured network traffic.
    b. Export the **Sysmon logs** and **packet capture data** (PCAP) for deeper forensic analysis. This can help you identify patterns or behaviors that were missed during the initial detection phase.

Best Practices for Threat Response

1. **Fine-Tune Thresholds and Sensitivity**:

    a. Adjust **Flow Score (FS)** and **DPD** thresholds to avoid triggering unnecessary responses. Set higher thresholds for stable environments and lower ones for dynamic environments where fast detection is crucial.

2. **Regularly Update Whitelist**:
    a. Keep your whitelist up to date to ensure that trusted traffic is not mistakenly flagged as suspicious. Add known safe IPs or applications after reviewing the context and ensuring they pose no risk.
3. **Collaborate with SIEM**:
    a. Export threat logs to your **Security Information and Event Management (SIEM)** system for centralized monitoring and incident response. This enables more efficient tracking and management of alerts across your entire network.

Post-Threat Mitigation

After a threat has been mitigated, it's important to follow these post-response steps:

1. **Review and Adjust Detection Models**:
    a. Ensure that the detection models (e.g., **Data Flow Divergence** and **Data Pattern Divergence**) are updated to reflect the new baseline established after the threat is resolved. This ensures that the system is ready for future detection.
2. **Incident Reporting**:
    a. Document the detected threat, your response actions, and any changes made to system configurations. This report can be useful for future training, audits, and refining the system.
3. **Test the System**:
    a. After mitigating the threat, run a series of tests to ensure the system is functioning correctly. Simulate normal and malicious traffic patterns to validate that the system is properly identifying and responding to both.

Final Recommendations

To maximize the effectiveness of **Adrenaline CryptoSentinel** and ensure your network remains secure, here are some final recommendations. These tips will help you optimize performance, improve detection accuracy, and maintain a proactive security posture.

1. Regular Updates and Maintenance

- **Keep Software Updated**:
    - Regularly update **AdrenalineFX**, **Sysmon**, and any related components to benefit from the latest security patches, performance improvements, and feature enhancements.
    - Enable automatic updates, if available, or manually check for updates at regular intervals to ensure that your system is up to date.
- **Update Detection Models**:
    - Continuously refine and update your traffic models based on evolving network conditions. This helps **AdrenalineFX** adapt to new patterns of normal behavior and improve its ability to detect unknown threats.

2. Optimize Sensitivity Settings

- **Fine-Tune Flow Score (FS)**:
    - Adjust the **Flow Score (FS)** threshold to balance detection sensitivity and reduce false positives. Fine-tuning this setting ensures that the system responds quickly to real threats without overwhelming the user with too many alerts.
- **Adjust DPD and DFP Sensitivity**:
    - Depending on your network's traffic patterns, adjust **Data Pattern Divergence (DPD)** and **Data Flow Proximity (DFP)** settings to either increase or decrease the sensitivity of detection. Use lower thresholds for high-traffic environments to ensure rapid threat detection.

3. Regularly Review and Manage Alerts

- **Monitor Detections Panel**:
    - Regularly check the **Detections** panel for new alerts. Reviewing and responding to these alerts promptly can help prevent threats from escalating.
    - Pay special attention to high-risk traffic, such as unusually large DNS queries or frequent ICMP requests, as they are often indicative of data exfiltration attempts.
- **Use Customizable Filters**:
    - Leverage the ability to filter alerts based on **Flow Score (FS)**, **IP address**, or **protocol type** to quickly identify and address the most critical threats.

4. Whitelist Trusted Entities

- **Manage the Whitelist**:
  - Regularly update the **whitelist** to ensure that trusted applications and IP addresses are not mistakenly flagged as suspicious.
  - Make sure to add legitimate systems or users that may generate unusual traffic but are not part of an active threat.
- **Review Whitelist Regularly**:
  - Periodically review entries in the **whitelist** to ensure they remain valid and relevant. Remove entries that are no longer needed to reduce potential attack surfaces.

5. Use Comprehensive Security Practices

- **Implement Layered Security**:
  - Combine **AdrenalineFX** with other security tools, such as firewalls, intrusion detection systems (IDS), and antivirus software, to create a layered defense strategy.
  - Use these systems in conjunction to provide deeper visibility into your network and ensure that threats are detected at multiple levels.
- **Maintain Good Security Hygiene**:
  - Regularly review your system configurations, enforce strong password policies, and ensure that your network is segmented to prevent lateral movement in case of an attack.

6. Training and Awareness

- **Train Your Team**:
  - Educate your security team on how to use **Adrenaline CryptoSentinel** effectively. Provide training on how to interpret alerts, adjust sensitivity settings, and respond to different types of threats.
- **Stay Informed on Emerging Threats**:
  - Keep yourself and your team updated on the latest cyber threats and attack methods. Subscribe to cybersecurity news sources and threat intelligence feeds to stay ahead of potential threats.

7. Backup and Recovery

- **Ensure Regular Backups**:
    - Regularly back up critical data and configurations, including system settings and firewall rules, to ensure you can quickly recover in the event of an attack.
- **Create a Response Plan**:
    - Develop an incident response plan that outlines steps to take in the event of a detected threat, including containment, mitigation, and recovery procedures.

Author: (c)2024 Mazzoni Roberto