## Policies

The policy feature analyzes collected data to detect threats according to established policies. The policy functionalities described in this section include:

* **[Stream Rule](section-stream-rule)**: A feature that analyzes correlations based on patterns or specific conditions in real-time collected data to detect threats.
* **[Batch Rule](section-batch-rule)**: A feature that detects threats by correlating different events that occur over time.
* **[Playbook](section-playbook)**: A feature that automatically responds to detected threats based on real-time/batch detection scenarios.

The following functionalities manage threat intelligence and related data and asset information necessary for security monitoring, utilized in real-time/batch detection and playbooks:

* **[ML Models](section-ml-model)**: A feature that analyzes and learns from data using Random Forest and Anomaly Detection Forest algorithms to predict data and identify/detect anomalous behavior.
* **[Threat Intelligence](section-threat-intelligence)**: Management functionality for threat intelligence provided through Logpresso CTI or applications.
* **[Behavior Profiles](section-behavior-profile)**: A feature that periodically profiles past behaviors, enabling behavior-based detection.
* **[ML Datasets](section-ml-input)**: Data management functionality for training machine learning models.
* **[Sites](section-site)**: Management functionality for sites subject to security monitoring.
* **[Assets IP](section-asset-ip)**: Management functionality for the IP addresses of assets that need protection from threats.
* **[Address Groups](section-address-group)**: Management functionality for IP address groups that can be utilized for blocking/allowing purposes.
* **[Subnet Groups](section-subnet-group)**: Management functionality for IP network groups that can be utilized for blocking/allowing purposes.
* **[Port Groups](section-port-group)**: Management functionality for TCP/UDP service port groups that can be utilized for blocking/allowing purposes.
* **[User-Defined Filters](section-udf)**: Management functionality for filters that can be used in real-time/batch scenarios.
* **[Pattern Groups](section-pattern-group)**: Management functionality for defining pattern groups that specify what to search for in the data.
* **[Alarm Groups](section-alarm-group)**: Management functionality for accounts that will receive alerts upon threat detection through real-time/batch detection scenarios.
* **[Indicators](section-indicator)**: Management functionality for user-defined indicators of compromise.