MODULAR SENSORS FUNCTIONS

LOG FORWARDER

Ensure logs are collected in one place.
Enhances the ability to detect, investigate, and respond to potential security threats afficiently

TRAFFIC METADATA

Enables detailed visibility into network activities.
Facilitates the identification of malicious behaviour

DEEP PACKET INSPECTION (DPI)

Can identify and classify protocols, applications, and even specific content within the packets, allowing for advanced network monitoring and security analysis.

IDS (60K + RULES)

Utilizes advanced analytics.
Detects a wide range of threats.
Analyzes traffic patterns and signatures.

MALWARE SANDBOX

Mimics real user environments.
Observes behaviors and outcomes of executed files.
Identifies malicious activities and signatures.

LOG PARSER

Involves extracting meaningful information from raw logs to identify security events or incidents.

NORMALIZATION

Facilitates efficient analysis, correlation, and alerting.
Enables the SIEM to accurately compare and link related security events across different systems and applications.

INTERFLOW CREATION

Enhances visibility.
Streamlines threat-detection processes
Facilitates rapid response to identified security incidents.

CONNECTORS

Enable seamless data ingestion and interaction with the platform.
Users can automate the collection, normalization, and analysis of data from disparate systems.

Linux Server Sensors

Windows Server Sensors

Modular Server Sensors