NewEvol

Threat Detection
& Monitoring in **Real-time**

SIEM Datasheet

Empowers Security Operations

What is NewEvol SIEM?

NewEvol SIEM is a NextGen security monitoring tool to protect your critical assets. It helps analysts understand the real impact and context of the attack by providing enhanced visibility across the enterprise's IT functions. It is more powerful when integrated with SOAR. It delivers effective results by facilitating quick alert remediation.

WHY DO YOU NEED NEWEVOL SIEM?

- Limited log retention
- Large volume of alerts
- No open API
- Limited functionality with multiple consoles

KEY FEATURES OF NEWEVOL SIEM

- Risk based alerting
- Log Management
- End to end visibility
- Integrated MITRE Attack Mapping
- Custom Log Parsing

KEY BENEFITS

- Real-Time Event Correlation
- Integration with Threat Intelligence
- Scalable and flexible architecture
- Advance Customizable dashboards
- Flexible log collection

NextGen Security Monitoring

COMPREHENSIVE VISUALIZATION

NewEvol SIEM provides you with total control over your IT environment through enhanced visualization of the security logs, events and alerts. Created with powerful technologies such as AI algorithms and Machine Learning, it can generate an auto analysis of the logs and flows ensuring a secure IT environment by enabling analysts to detect and prioritize alerts.

BEFOREHAND THREAT DETECTION

NewEvol SIEM's data lake can correlate data to provide actionable insights. It provides visualization of early-stage and probable threats, and low and slow attacks before it disrupts the digital ecosystem.

SINGLE, COLLABORATIVE PLATFORM

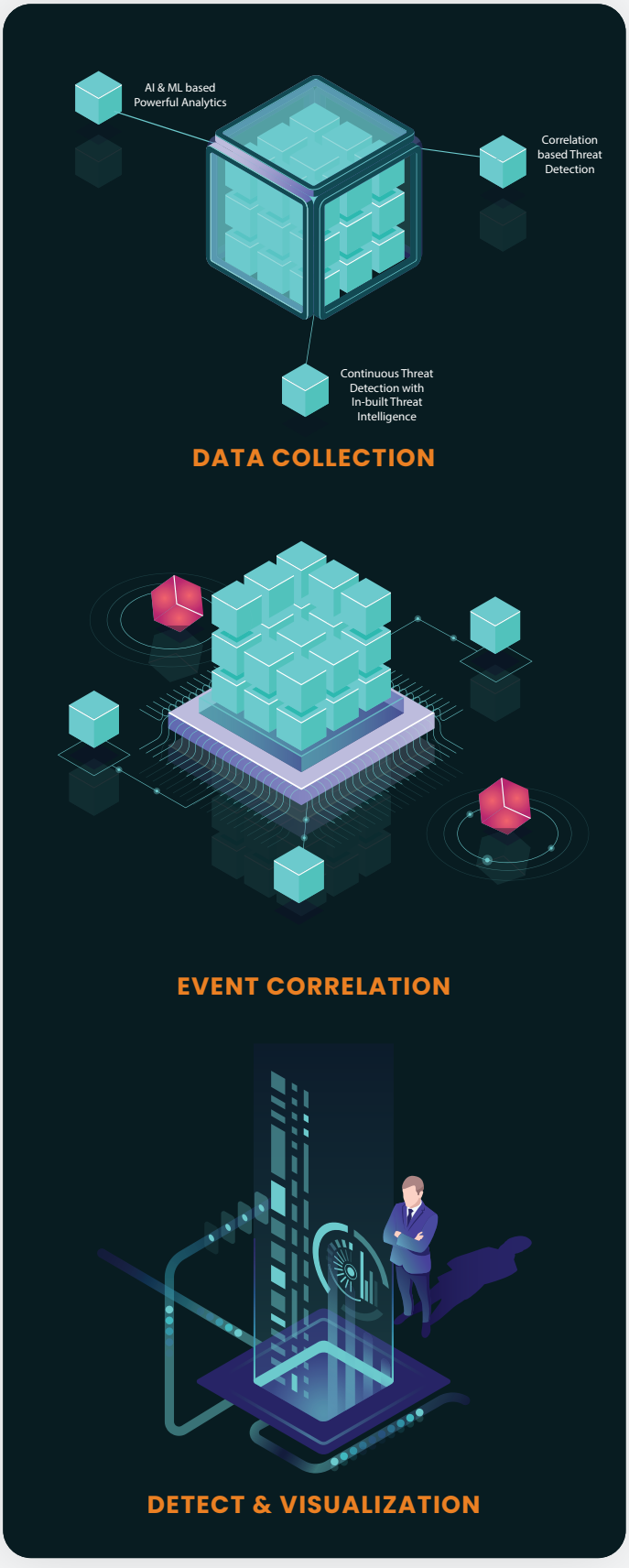
NewEvol SIEM facilitates security operations tasks from a single console. It delivers great results by enabling the analysts to monitor and remediate the alerts from a single console.

CONTACT US

1 Parklane Blvd, STE 729 E,
Dearborn, MI 48126

+1 (325) 515-4107

info@newevol.io



How Does it Work?

NewEvol SIEM works in three phases

COLLECT

NewEvol Collector collects logs from diverse data sources such as security devices, cloud applications etc. It then ingests these logs into the NewEvol SIEM data lake.

CORRELATE

NewEvol SIEM data lake correlates the ingested data in real-time. Following the MITRE attack framework, NewEvol's advanced correlation engine then bifurcates the data in the most effective manner. The data is then utilized for further analysis.

DETECT

Once the data gets corelated, NewEvol SIEM performs the detection mechanism using the out of the box rules to detect the anomalies and potential threats that try to enter the network environment.

VISUALIZE

The methodically correlated data is pushed to an advanced dashboard for comprehensive visualization. It highlights detected alerts with in-depth analysis, intuitive charts and diagrams to prompt quick action.

INFRASTRUCTURE REQUIREMENT

NewEvol SIEM is designed to work efficiently with minimum hardware requirements. The hardware sizes may vary as per the requirements.

SERVER	CORE	RAM	HDD	OS
Namenode 1	16	32 GB	500 GB	Ubuntu 16.04
Namenode 2	16	32 GB	500 GB	Ubuntu 16.04
Datanode	32	256 GB	2 TB	Ubuntu 16.04
Web Server	16	128 GB	500 GB	Ubuntu 16.04

info@newevol.io | +1 (325) 515-4107