

# Advanced Machine Learning Analytics



## What is NewEvol Analytics?

NewEvol Analytics is the ultimate tool for threat hunting and risk mitigation. It helps security teams identify attacks before they disrupt business operations. It is infused with all the capabilities like threat intelligence and contextual correlations to detect even the most complex cyberattacks to ensure the security of the digital ecosystem.

### CHALLENGES

- > Detection of Unknown threats
- > Absence of analytics-based threat hunting
- > Trend and pattern analysis of threats
- > Absence of advanced features like the MITRE framework

### WHY NEWEVOL ANALYTICS?

- > Integrated MITRE framework
- > Analytics-based threat hunting
- > Machine learning-based correlation
- > Data visualization in 2D and 3D

### KEY BENEFITS

- > In-depth analysis of alerts with MITRE classification
- > Comprehensive visualization of alerts with correlate fields
- > Automated Threat Hunting
- > Improved forensics capabilities

## Analytical Uniqueness

### PROACTIVE SECURITY

NewEvol analytics correlates events based on combined data from logs and other sources, in near real-time, detecting indicators of suspicious activity. The result is proactive security that helps organizations detect threats earlier in the attack chain and significantly improve response times.

### ANALYTICS-BASED THREAT HUNTING

NewEvol analytics employs cutting-edge technologies like AI (Artificial Intelligence) and ML (Machine Learning) to determine outliers and calculate the frequency of each event. It almost works like an intuitive and experienced professional to detect threats even in the hyper-connected digital ecosystem.

### BACKED BY ML AND AI TECHNOLOGIES

NewEvol Analytics delivers advance analytical capability across the data to detect threat well in advance. Backed by advance technologies like Machine Learning and Artificial Intelligence algorithms, NewEvol Analytics helps detect unknown threats.

## CONTACT US

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

+1 (325) 515-4107

info@newevol.io



## COLLECT & DATA MODELING



## ML BASED CORRELATION



## VISUALIZATION

## How does it work?

NewEvol Analytics helps you overcome security challenges in four phases.

### — COLLECT

NewEvol Analytics first collect the normalized data from NewEvol collector. The collected data is then sent for the analysis.

### — DATA MODELING

Collected data will be analyzed by NewEvol Analytics to create data modeling. Here, NewEvol Analytics will understand the data and once sufficient data is available, data model will prepare for identifying unknown-unknown.

### — MACHINE LEARNING BASED CORRELATION

Once the NewEvol Analytics understands the network environment, It then runs Machine learning based algorithm to correlate the data and provide insightful output for detection of alerts.

### — VISUALIZATION

Lastly, the corelated data is presented in a more sophisticated manner through dashboards. Here analysts can have in depth visualization of the analytical data with respect to 2-D and 3-D visualization of alerts detected.

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.