CITIC TELECOM CPC

"Facial Recognition" for Malware

AI Visual Security

重塑「眼見為實」的信息安全模式

迅速「看見」惡意軟件，快速「攔截」惡意軟件家族

AI Visual Security

Innovation Values:

Lightning-Fast Malware Detection:
Identify and classify malware threats 10-100x faster than traditional sandbox methods,drastically reducing response times.

Proactive Threat Prevention:
Leverages analysis of past threat behaviors to anticipate and neutralize evolving malware families, including mutations.

Efficient Resource Utilization:
Leverages GPU processing power with compact visual data representations, freeing up critical CPU resources.

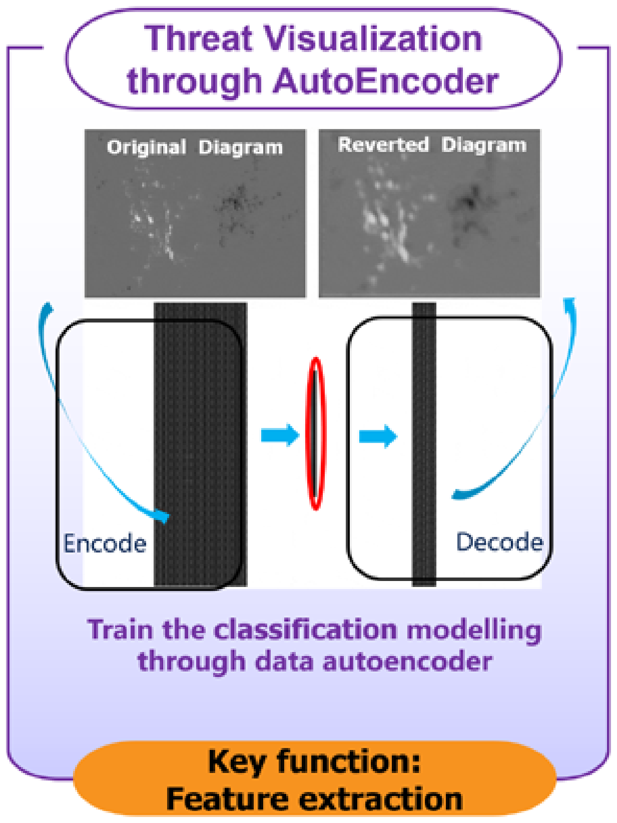
Scan to learn more about AI Visual Security:

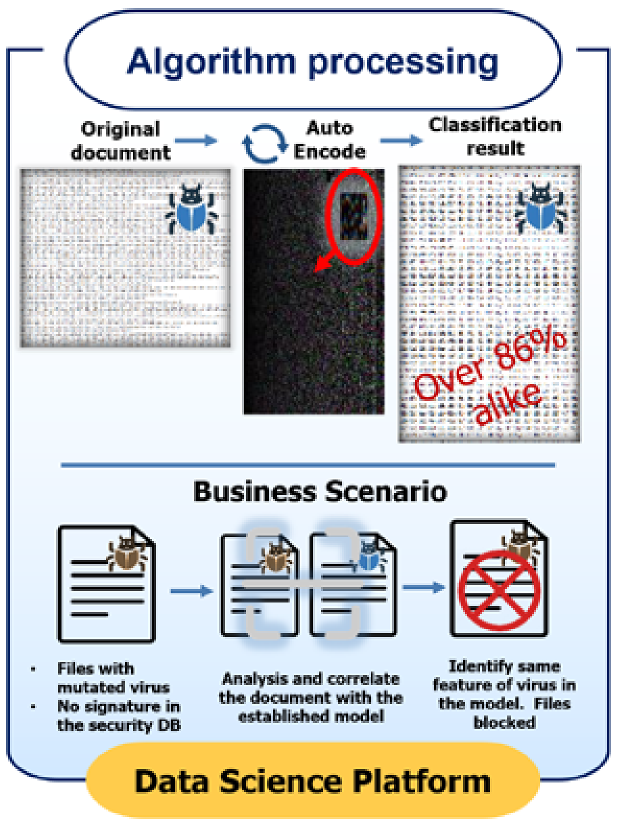
Features:

Data to Image Algorithm:
Transforms raw malware data into manageable 2D images, enabling "mix and match" malware classification.

AI-Enhanced Computer Vision:
Like facial recognition, detects and classifies even the most disguised malware within these visual representations.

Weakly Supervised Regularization Algorithm:
Leverages a specialized "Autoencoder" to automatically extract hidden malware features, accelerating and improving detection accuracy.


Threat Visualization through AutoEncoder
Original Diagram
Reverted Diagram
Encode
Decode
Train the classification modelling through data autoencoder
Key function: Feature extraction


Algorithm processing
Original document
Auto Encode
Classification result
Over 86% alike
Business Scenario
Files with mutated virus
No signature in the security DB
Analysis and correlate the document with the established model
Identify same feature of virus in the model. Files blocked
Data Science Platform

☎ (852) 2170 7401 ✉ info@citictel-cpc.com