



AI Driven
Fully Automated Offensive
Security Simulation Platform



ANALYZER

AI Driven

Fully Automated Offensive
Security Simulation Platform

CYBRAL STORM™ ANALYZER is a cutting-edge CTEM (Continuous Threat Exposure Management) platform powered by artificial intelligence that continuously identifies different assets, scans for vulnerabilities and weaknesses, and helps act proactively against potential threats, allowing organizations to stay ahead of evolving cyber threats.

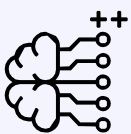
It uses Symbolic AI and Reinforcement Learning, combined with proprietary, patent-pending algorithms, to help organizations identify potential threats by analyzing all possible attack scenarios and generating a practical, prioritized defense strategy. An advanced LLM is then utilized to facilitate the communication of the remediation steps.

CYBRAL STORM™ Differentiators



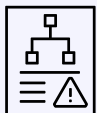
360° View of Attack Paths

Offers a complete view of all possible attack paths and potential vulnerabilities and identifies all attack paths the organization is exposed to without requiring actual exploitation of weaknesses.



Critical Attack Path Identification & Prioritization Using Reinforcement Learning

Leverages reinforcement learning to provide optimized and prioritized critical attack paths, generating actionable insights that drive focused and effective security measures.



Defense Strategy Generation

Uses generative AI to generate remediation strategies in an intuitive, user-friendly manner, providing clear, actionable steps that make proactive security management approachable and effective

Capabilities



Comprehensive Scanning

It offers complete visibility into external and internal assets and potential vulnerabilities without requiring actual exploitation of weaknesses.



AI-Driven Analysis

Our product uses advanced AI algorithms to analyze scanned data and identify potential threats and attack scenarios.



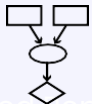
Continuous Monitoring

It continuously monitors network activity to detect emerging threats, enabling teams to respond proactively



Detailed Reporting

It provides detailed reports and visualizations, including attack graphs and critical path analyses, to support risk understanding.



Attack Scenarios Representation

CYBRAL STORM™ ANALYZER uses advanced AI technologies to generate detailed attack scenarios. This feature provides a clear and comprehensive visualization of potential attack paths and methods that could be used against your network. By simulating these scenarios, users can better understand the nature of potential threats and take proactive measures to strengthen their network security..



Defense Planning

CYBRAL STORM™ ANALYZER and attacks. This feature helps security teams develop defense strategies, prioritifacilitates strategic defense planning by providing detailed insights into potential vulnerabilities ze remediation efforts, and implement targeted security measures.



Remediation Simulation

CYBRAL STORM™ ANALYZER includes a remediation simulation feature that allows users to model and test remediation actions before implementation.

Benefits



Proactive Threat Management

CYBRAL STORM™ ANALYZER Keeps organizations ahead of potential threats with advanced threat detection, enabling proactive security measures.



Enhanced Security Posture

CYBRAL STORM™ ANALYZER Identifies and addresses vulnerabilities before they can be exploited, strengthening the network's overall security.



Operational Efficiency

Automates security assessments with **CYBRAL STORM™ ANALYZER**, allowing teams to focus on strategic security initiatives. This automation reduces the need for extensive configuration and manual processes, saving time and effort while enabling quicker responses to emerging threats.



Comprehensive Insight

Gain a complete view of your network's security status and potential risks. It provides detailed insights into vulnerabilities, attack paths, and remediation strategies, ensuring a full understanding and management of network security.



Scalable Solutions

Our product supports organizations of all sizes, providing scalable solutions that can grow with their network and security needs.



Cost-Effective Security

By automating security processes and reducing the need for manual intervention, it offers a cost-effective solution for maintaining high network security.

How It Works

Scanning Process



Network Topology Scanning

Maps out the structure of the user's network infrastructure.

Analyzes connections between devices and systems.

Creates a detailed representation of the network topology for better resource management.



Vulnerability Scanning

Identifies weaknesses and security gaps within the network.

Uses advanced techniques to examine network devices, applications, and configurations.

Detects vulnerabilities and misconfiguration entry points for cyber threats.

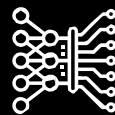
AI Analysis



Symbolic AI Engine

Processes output from the NLP Engine to generate an attack graph.

Provides a complete map of all possible attack paths that an attacker can exploit inside the organization



Reinforcement Learning

Analyzes the attack graph to rank critical paths based on their vulnerabilities and asset criticality.

Provides ranked and prioritized critical paths with a criticality score for each based on asset importance and vulnerabilities.



Gen AI

Generates attack scenarios and defense strategies based on critical paths and assets.

Offers a complete defense strategy that considers all possible attack scenarios



Conclusion

CYBRAL STORM™ ANALYZER is a comprehensive security solution that uses advanced AI technologies to provide visibility into network vulnerabilities and potential attack vectors.

By prioritizing critical paths and simulating remediation actions, it empowers organizations to enhance their security posture proactively and effectively.

AI Driven
Fully Automated Offensive
Security Simulation Platform