CyberCyte x NATICA

AI-Driven Risk and Threat Exposure Management

Continuously identify, assess, and prioritize security risks through a unified platform for complete visibility and automated response to threats, vulnerabilities, and misconfigurations.

EXECUTIVE SUMMARY

Many organizations are overwhelmed with problems like alert fatigue, difficulty prioritizing risks, and discovering complex attacks. Critical risks are often unknown, and environments are not hardened due to a shortage of skilled cybersecurity experts.

CyberCyte is an Extended Threat Exposure Management (X-CTEM) platform, unifying Threat Detection Response (TDR), Automated Security Control Assessment (ASCA), and GRC Management. The system collects, classifies, and assesses forensic artifacts and threat indicators to transform the unknown activities performed by unknown artifacts(unknown/unknown) to the known/known.

The risk management framework creates a unified visibility layer, enabling accurate prioritization and validation. The system discovers previously unknown risks, reduces complexity, and minimizes operational costs. The platform improves the GRC processes through the automated management of the risk registry, minimizing the operational overhead in risk management.

UNIFIED CLASSIFICATION, ENRICHMENT, AND RESPONSE

CyberCyte offers a cyber defense framework to identify, classify and prioritize cyber risks. The platform enhances an organization's defense capabilities, amplifies threat visibility, and revolutionizes automated defense mechanisms. Once deployed, the system empowers organizations to proactively defend against evolving threats by providing advanced insights. A unique visibility layer is created for accurate risk prioritization by integrating forensic artifacts, threat indicators and audit data.

The platform accurately prioritizes threats and risks by using a robust classification system and the CyberCyte AI. The solution immediately identifies security gaps and creates a consolidated analysis framework for cyber assets, threats, vulnerabilities and misconfigurations against security controls.

The platform offers a proactive approach to cybersecurity that involves continuously monitoring the attack surface. This method ensures that potential vulnerabilities are identified and addressed in real-time, significantly reducing the risk of a breach. The effectiveness of security measures and hardening controls is assessed continuously. SIGMA, YARA, and scenario tests are used to perform the assessments. The scenario tests include automated penetration tests and real-life simulations to detect the effectiveness of the deployed security applications, including EDR and DLP software.

www.cybercyte.com

PLATFORM BENEFITS

- Create a unique visibility and response layer by unifying forensic artifacts, threat indicators, and audit data.
- Measure ransomware infection and information leakage risk.
- Enable immediate identification of security gaps.
- Validate the effectiveness of the existing security controls.
- Create a centralized remediation and response framework.
- Track the impact of zero-day and exploited vulnerabilities.
- Improve the GRC processes through the automated management of the risk registry.
- Automate classification, whitelisting, and risk-scoring through CyberCyte AI.
- Minimize operational overload and reduce costs by automating configuration management of the infrastructure.

100+ UNIQUE ARTIFACTS

are collected, classified, and enriched.

SINGLE-CLICK MAINTENANCE

for applications like Sysmon and osquery.

HOLISTIC VISIBILITY

by consolidating threat, vulnerability, hardening, and asset information.

UNIFIED REMEDIATION & RESPONSE

for Windows/MAC/Linux platforms.

Why Use CyberCyte When EDR, NDR, XDR, SIEM/SOAR... is Deployed?

CyberCyte is a market leading platform that unifies Cyber Threat Exposure Management (CTEM), Automated Security Control Assessment (ASCA), and GRC Management. This comprehensive integration ensures that all aspects of cyber security are covered, providing a holistic approach to risk management and compliance.

Internal compliance is monitored by tracking activities like admin share logins (c$, d$..), network access to user documents, hardware changes, and USB disk activity. A new visibility layer is created to detect malware and insider threats. The platform analyzes every process and its activities within the operating system, enables in-depth analysis of access to user documents and monitors access to user documents through browsers.

The GRC Management module minimizes the operational overhead arising from compliance requirements by automating the management of the risk registry.

IMMEDIATE VISIBILITY

by deploying in minutes and achieving results in a few hours after the deployment.

SIMPLIFIED GRC

Bridge the communication gap between the security and compliance teams.

MAIN FEATURES

- Enable immediate identification of security gaps.
- Measure ransomware infection and information leakage risk by executing EDR and DLP effectiveness assessments covering all endpoints and servers.
- Validate the effectiveness of the existing security infrastructure and the security controls.
- Identify and remediate configuration gaps based on CIS, DoD, BSI, and MSFT security baselines.
- Create a centralized remediation and response infrastructure.
- Analyze unknown forensic artifacts to identify hidden threats and uncompliant activity.
- Track zero-day and exploited vulnerabilities.
- Map the impact of the discovered risks against standards like NIST, ISO 27001, and CIS.
- Automate threat hunting and scenario execution based on YARA, SIGMA, and simulation rules to detect passive threats inside the IT infrastructure.
- Integrate forensic artifacts, threat indicators, and audit data to create a unique visibility layer, enabling security teams to identify complex threat patterns easily.
- Automate classification and risk-scoring to reduce the noise from excessive security alerts based on forensic analysis.
- Monitor internal compliance activities such as admin share usage (c$, d$...), network access to user documents, hardware changes, and USB disk activity.
- Monitor user login, logoff, and computer lock activities.

PLATFORM SUPPORT

- Granular artifact collection with or without agents.
  - Agent/Agentless Collection for Windows
  - Agent/Cron Based for Linux/MAC/Unix
- Support for different data collection methods.
  - Remote Connection With WMI/Win-RM/SSH
  - SNMP Discovery
  - NMAP Scanning

RESPONSE & REMEDIATION

- Uninstall Application
- Remediate Security Controls
- Kill Process
- Manage File/Registry/Service
- Execute PowerShell Command & Script
- Install/Upgrade Application

Pasific Plaza A Blok Sevinçli Sok. N:3 K:8 Küçükbakkalköy Ataşehir 34750 İstanbul
Tel: +90 (212) 296 61 90
Email: infoNatica@natica.com.tr
www.natica.com.tr