CyberCyte EAR

Manage the Unmanageable

Identify the unknown threats and risks through a unified threat, vulnerability, and hardening visibility layer with unparalleled accuracy powered by CyberCyte AI.

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 EAR (Enhance, Amplify, Revolutionize) is a Managed Blue Team and Automated Security Control Assessment (ASCA) platform that correlates existing system risk data, enriches it, and presents a new visibility layer utilizing Digital Forensic Analysis, Threat Hunting, and Asset Management to enable risk prioritization and faster remediation.

UNIFIED CLASSIFICATION, ENRICHMENT, AND RESPONSE

CyberCyte EAR creates a cyber defense framework to identify and respond to what is more important. It unifies threat, vulnerability, and hardening to enable accurate and fast risk discovery. 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 and audit data.

The platform accurately prioritizes threats and risks by analyzing forensic artifacts 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, and vulnerabilities against security controls.

A unique visibility layer is created for accurate risk prioritization and threat hunting by integrating forensic artifacts and audit data, enabling security teams to identify complex threat patterns easily. Cybersecurity professionals can minimize the risks faster and easier through a simplified remediation and response framework. Forensic artifact enrichment enables the discovery of risks that occurred in the past before security assessments were performed. Finding the needle in the haystack is easier with CyberCyte EAR.

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

The platform enables continuous security GAP analysis by executing specific scenarios. EDR and DLP assessments performed as part of gap analysis covering all endpoints and servers enable organizations to measure their readiness for ransomware attacks and data leakages.

Internal compliance is monitored by tracking activities like admin share logins (c$, d$..), network access to user documents, hardware changes, and USB disk activity.

The CyberCyte AI enables security teams to analyze unknown activity more accurately using multiple AI models and threat intelligence feeds.

www.cybercyte.com

CyberCyte

PLATFORM BENEFITS

- Enable immediate identification of security gaps.
- Measure ransomware infection and information leakage risk.
- Validate the effectiveness of the existing security controls.
- Create a centralized remediation and response framework.
- Track the impact of zero-day and exploited vulnerabilities.
- Consolidate threat hunting and forensic analysis processes.
- Create a unique visibility layer by unifying forensic artifacts and audit data.
- Automate classification, whitelisting, and risk-scoring through CyberCyte AI Robot.

100+ UNIQUE ARTIFACTS

are collected, classified, and enriched.

SINGLE-CLICK MAINTENANCE

for applications like Sysmon and osquery.

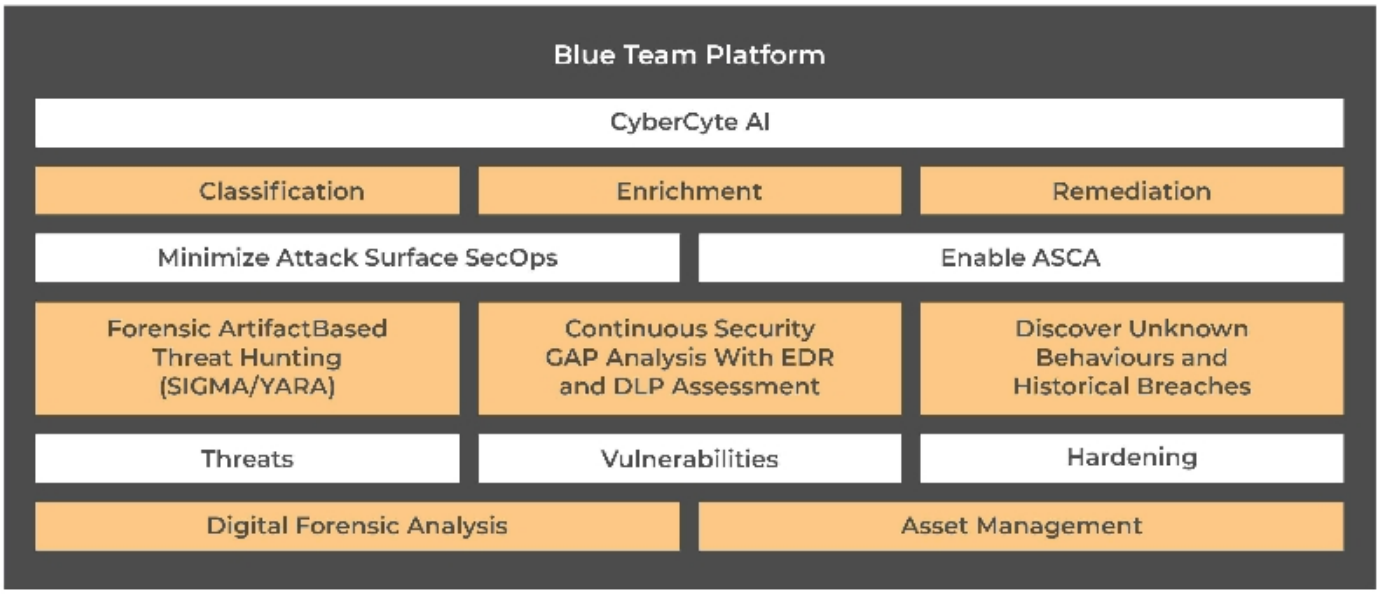
HOLISTIC VISIBILITY

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

UNIFIED REMEDIATION & RESPONSE

for Windows/MAC/Linux platforms.

SOLUTION COMPONENTS



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 through the GRC dashboard.
- Automate threat hunting and scenario execution based on YARA and SIGMA rules to detect passive threats inside the IT infrastructure.
- Unify threat hunting, investigation, and forensic analysis processes in a single solution that can be offered as an MDR service.
- Create a unique visibility layer by integrating forensic artifacts and audit data to enable security teams to identify complex threat patterns easily.
- Automate classification and risk-scoring to reduce the noise from excessive security alerts based on digital forensic analysis.
- Track internal compliance by monitoring activities like admin share usage (c$, d$..), network access to user documents, hardware changes and USB disk activity.
- Monitor the exact login and logoff times for the end users to their devices.

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

Davidson House, Forbury Square, King's Rd, Reading RG1 3EU United Kingdom
Tel: +44 118 214 2400
e-mail: info@cybercyte.com