Enhance
Amplify
Revolutionize

CyberCyte EAR

Safeguarding the future today.

Many organizations are overwhelmed with problems like alert fatigue, difficulty prioritizing risks, and discovering complex attacks. CyberCyte EAR (Enhance, Amplify, Revolutionize) is a Blue Team and Automated Security Control Assessment (ASCA) platform utilizing Digital Forensic Analysis, Threat Hunting, and Asset Management through a new visibility layer with easy customization no other product can offer.

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 identification of 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 and unparalleled visibility.

The platform accurately prioritizes threats and risks by analyzing forensic artifacts using a robust classification system. The solution immediately identifies security gaps and creates a consolidated analysis framework for cyber assets, threats, and vulnerabilities against security controls. 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. This way of analysis enables the identification of additional risks not identified by the AV/EDR/XDR solutions as these systems analyze real-time activity. The solution also performs a complete analysis of the endpoints to assess how effective security applications are working and how security controls are applied. Remediation actions can be executed through the platform to minimize the dependency on other operations teams.

Main Features

- Provide a single classification and risk-scoring framework to reduce the noise from excessive security alerts.
- Enable immediate identification of security gaps.
- Create a consolidated visibility for assets, threats, and vulnerabilities for accurate prioritization.
- Offer a centralized remediation and response infrastructure.
- Discover and remediate configuration gaps based on CIS, DoD, BSI, and MSFT security baselines.
- Automate scenario execution based on YARA and SIGMA rules to detect the passive threats inside the IT infrastructure.
- Enable the discovery of unknown forensic artifacts to identify malicious and uncompliant activity.

Business Benefits

- Increased Resiliency to Cyber Threats
  - Complete Visibility to Forensic Artifacts and Assets
  - Discover the Unknown
- Lower Operational Costs
  - Simplify and Automate Remediation
  - Eliminate Security Gaps

Davidson House, Kings Road Reading RG1 3EU
+44 118 214 2400
www.cybercyte.com

Enhance
Amplify
Revolutionize

- Increased Productivity
    - Simplify Classification to Identify Risks Faster and Easier
    - Holistic View of Security Infrastructure

Use Cases

Leading International Energy Distribution Company

A leading energy distribution company with over ten million customers required a platform that automatically identifies and improves security gaps to strengthen the cyber security framework. CyberCyte platform provided a new layer of visibility to identify the improvements that can be performed within the existing cyber security solutions.

Leading Global Manufacturer

A global manufacturer producing motor pistons was looking for a solution to manage their cyber assets and assess if hardening in their infrastructure is performed effectively. Cybercyte was chosen as a managed service offering to monitor the health state of their cyber assets and improve the hardening settings in their endpoints.

A Hotel Group

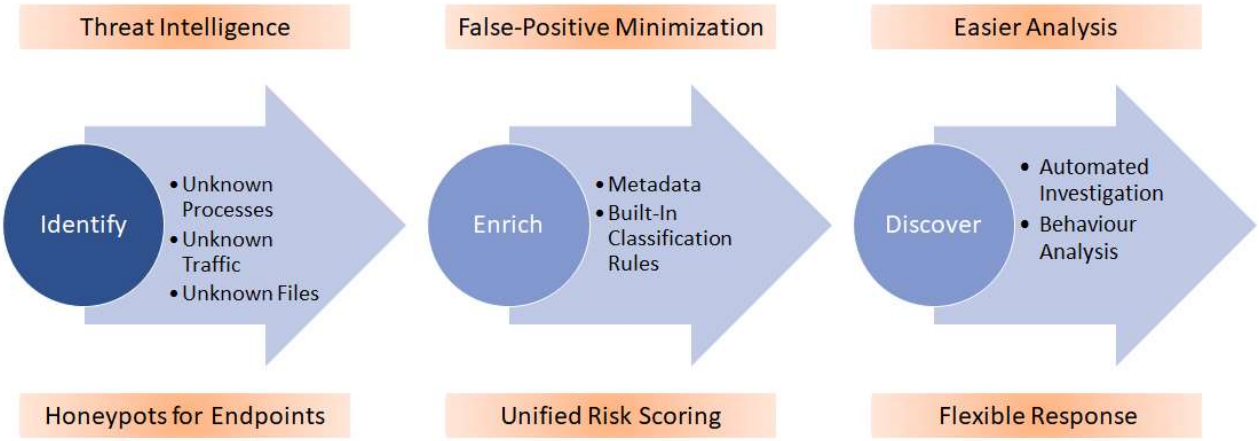
A hotel group with more than 15 hotels in Turkey, Europe, and the US preferred CyberCyte to improve their cyber security posture. They wanted to collect and manage digital forensics artifacts to identify uncompliant activity. Their EASM and vulnerability tools were also integrated into the platform to create a single visibility within the infrastructure.

Main Differences

A New Visibility for Threat Hunting	A New Approach to Discovering the Unknown	Enable Zero-Trust
•SIEM/SOAR focused on audit data. •Collect and analyse forensic artifacts for all devices based on open standards.	•NDR/EDR/XDR monitors events and activities. •Automated scenario execution for detecting the hidden risks.	•SOAR and XDR solutions act for blocking threats. •Enable in-depth investigation to eliminate non-standard artifacts and configuration gaps.

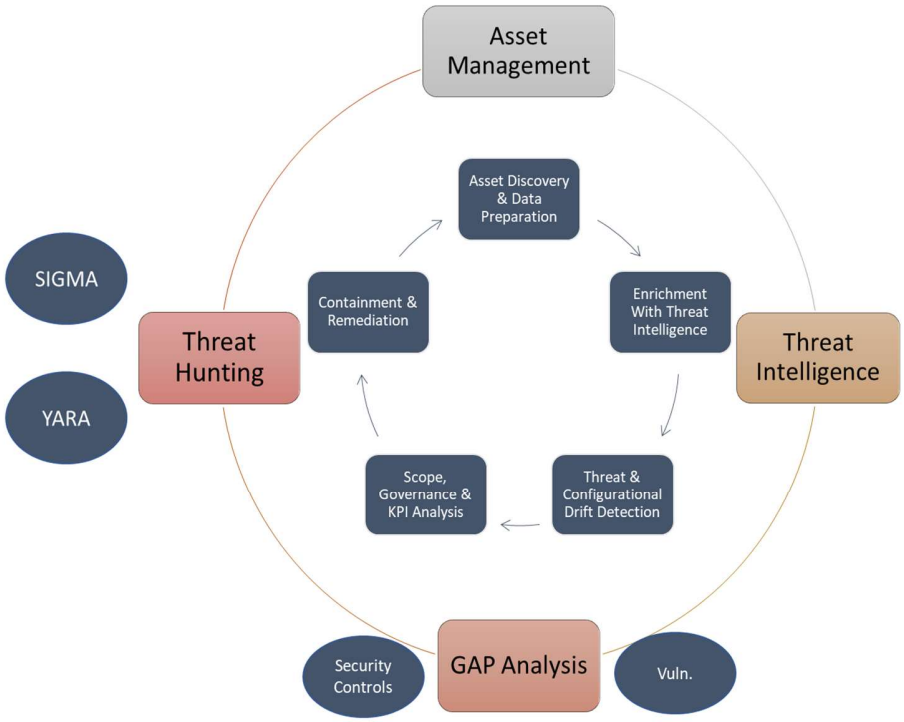
Enhance
Amplify
Revolutionize

A New Layer of Visibility



Without Performance Overhead, CyberCyte Creates a New Visibility Layer With Limitless Customization No Other Product Can Offer

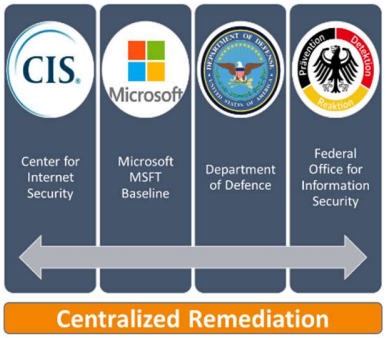
Solution Components



Davidson House, Kings Road Reading RG1 3EU
+44 118 214 2400
www.cybercyte.com

Enhance
Amplify
Revolutionize

Response & Remediation



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

Platform Support

- Granular artifact collection with or without agents.
    - Agent/Agentless Collection for Windows
        - Autoruns & Processes
        - Sysmon & Event Log
        - Asset Inventory
        - Active Directory Objects
        - Macro Files, Office MRU
        - AM, Shim, DNS, SMB Caches
        - Windows Prefetch
        - Network Adaptors and PnP Devices
        - Software Vulnerabilities
    - Agentless for Linux/Unix
        - Autoruns & Processes
        - Command Execution
        - Users & Groups
        - Auth & System Logs
- Support for different data collection methods.
    - Remote Connection With WMI/Win-RM/SSH
    - SNMP Discovery
    - NMAP Scanning
- Support for different methods for blocking malicious communication:
    - DNS Relay
    - Perimeter Security Devices
    - Network Devices
    - Agent

Davidson House, Kings Road Reading RG1 3EU
+44 118 214 2400
www.cybercyte.com