Discover the Unknown

CyberCyte

CyberCyte offers an MDR platform for threat-hunting to identify cyber risks faster and easier through a zero-trust model. The system collects, classifies, and enriches assets, information, and forensic artifacts through a unified risk-scoring framework. Simplicity is achieved through analyzing artifacts instead of log data, as performed by most solutions in the market. Malicious traffic, uncompliant artifacts, and unknown activity not detected by the existing security controls are identified in hours through gap analysis. The system provides a unified risk-scoring framework for the asset, information, and forensics artifacts.

The platform can be deployed on-premise or on any cloud platform in minutes. All components are based on virtualized containers enabling scalability without requiring complex resource planning. The system offers two modules for threat hunting.

Forensic Analysis

The module performs the collection of forensic artifacts from endpoints, network and cloud applications. After collection, the system creates a neural map of how information flows within an organization. The neural map provides a library for forensic artifacts and communication patterns of how applications and devices communicate to discover malicious activity. The module also acts as an integration hub for existing security solutions.

Main Features

- Support SOC teams by providing a single classification and risk-scoring framework to reduce the noise from excessive security alerts.
- Enable the discovery of unknown forensic artifacts and gap analysis to identify malicious and uncompliant activity.
- Enable forensic analysis, investigations, and automated remediation without requiring agents on endpoints, networks, and e-mail/Microsoft Teams activity.
- Create a map of how information flows within an organization enabling drill-down analysis of applications running in endpoints and servers.
- Provide a library of communication patterns of how applications and devices communicate, enabling the detection of any abnormal activity.
- Act as an integration hub for existing security solutions to enable threat investigation and block malicious communication.
- Enable zero-trust access control by blocking any uncategorized traffic or network access of a device.

E-Mail and Communication Security

The module is a GDPR-compliant e-mail phishing detection and inbox security solution. The system enables organizations to identify and delete malicious e-mails and Microsoft Teams communication bypassing the security controls.

The users can report e-mails that they suspect are suspicious. The platform provides unmatched visibility for malicious e-mails reaching the end-users. Once an e-mail is identified as malicious, the system can trigger an investigation. The investigation process enables the discovery of risky e-mails without requiring mailbox access. Once an e-mail is identified as malicious, the e-mail can be deleted from all user mailboxes.

Main Features

- Identification of targeted phishing attacks bypassing the existing security controls.
- Enable automated actions for malicious e-mails.
- GDPR compliance by performing analysis based on the metadata collected from the e-mails
- Increased user awareness.
- File and content search within e-mail and Microsoft Teams activity.

Platform Support

→ Granular identification of traffic created by applications with or without agents:

- Agent/Agentless Collection for Windows
  - Autoruns & Processes
  - Sysmon & Event Log
  - Asset Inventory
  - Active Directory Objects
- Agentless for Linux/Unix
  - Autoruns & Processes
  - Command Execution
  - Users & Groups
  - Auth & System Logs

→ Support for different data collection methods:

- DNS Span and Relay (Microsoft DNS, Bind)
- Netflow / Sflow
- Port Span
- Perimeter Security Devices
- Network Devices

→ Support for different methods for blocking malicious communication:

- DNS Relay
- Perimeter Security Devices
- Network Devices
- Agent

Features for MSSPs

✔ **White-labeling support for all components to enable better MSSP brand visibility.**

✔ **Deployment on any Kubernetes-supporting cloud platform, including Amazon WS, Microsoft Azure, and Google.**

✔ **Ability to enroll and initiate customers in minutes.**

✔ **Full support for self-management and customer tracking.**

✔ **Enable self-deployment and zero maintenance overhead.**

E-Mail Security Platform Support

→ Agentless e-mail add-in for Microsoft Outlook (Windows, MAC OS, IOS, and Android) and Teams
- Microsoft Exchange Server 2016 +
- Microsoft Office 365

→ Agent-based add-in for Microsoft Outlook for Windows 2016 +

→ Microsoft 365

UK
Davidson House, Kings Road Reading
RG1 3EU
+44 118 214 2400

USA
1201 N. Orange Street Suite 7160
Wilmington, DE 19801
+1 302 425 9966

www.cybercyte.com