Infrastructure Security

Infrastructure security involves protecting critical systems and assets, such as networks, data centers, and power grids, from cyber threats and physical attacks. It ensures the integrity, confidentiality, and availability of essential services and information.

- Endpoint Detection and Response

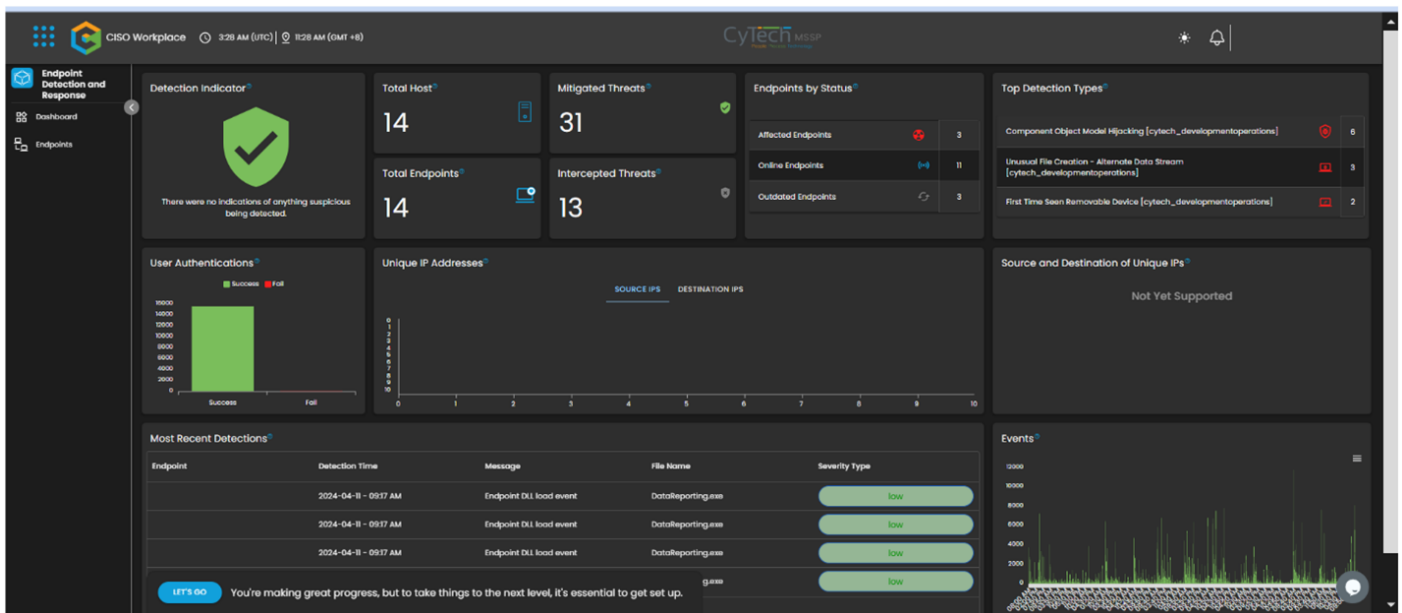# Endpoint Detection and Response

Overview

Endpoint Detection and Response (**EDR**) is a critical cybersecurity solution designed to detect, investigate, and respond to security incidents on endpoints within a network. This manual serves as a comprehensive guide to understanding and effectively utilizing our EDR system.

Key Features:

1. **Alert Monitoring**: The **EDR** system offers real-time alert monitoring to identify potential threats and protect against cyberattacks.
2. **Endpoint Protection:** It detects and safeguards endpoints from various threats, enhancing overall security posture.
3. **Behavioral Analysis:** Utilizes advanced behavioral analysis techniques to identify suspicious activities and potential indicators of compromise.
4. **Automated Response:** Offers automated response capabilities to promptly contain and remediate security incidents, reducing response times and minimizing potential damage.
5. **Forensic Investigation:** Enables in-depth forensic investigation of security incidents, providing detailed insights into the scope and impact of threats.
6. **User Activity Monitoring:** Monitors user activities on endpoints to detect insider threats and unauthorized access attempts.

User Manual

Dashboard:

- **Total Hosts:** This indicates the total number of active hosts or devices connected to the network being monitored by the EDR system, providing an overview of the network's size and scope.
- **Total Endpoints:** Similar to "Total Hosts," this represents the total number of endpoints, such as computers and servers, being monitored by the EDR system, offering insight into the number of protected devices.
- **Mitigate Threats:** This section displays information about ongoing or recent security threats detected by the EDR system, including threat type, affected endpoints, and recommended actions to mitigate the threat.
- **User Authentication:** Provides information about user authentication events, such as successful logins and failed login attempts, enabling administrators to monitor user activity and identify suspicious login behavior.
- **Unique IP Addresses (Destination & Source):** Displays unique IP addresses involved in network communications as source and destination, aiding in identifying potential malicious connections or unusual traffic patterns.
- **Most Recent Detections:** Lists the most recent security incidents or detections made by the EDR system, providing visibility into the latest threats or suspicious activities detected on the network.
- **Events:** Shows a log of security events and activities captured by the EDR system, including endpoint activities, network events, and system events, providing relevant security-related data.
- **Top Detections:** Highlights the top or most significant security detections or incidents based on severity, impact, or frequency, helping prioritize response efforts and focus on critical security issues.

Endpoints

"EDR endpoints" refers to devices or endpoints monitored and protected by an Endpoint Detection and Response (EDR) system.
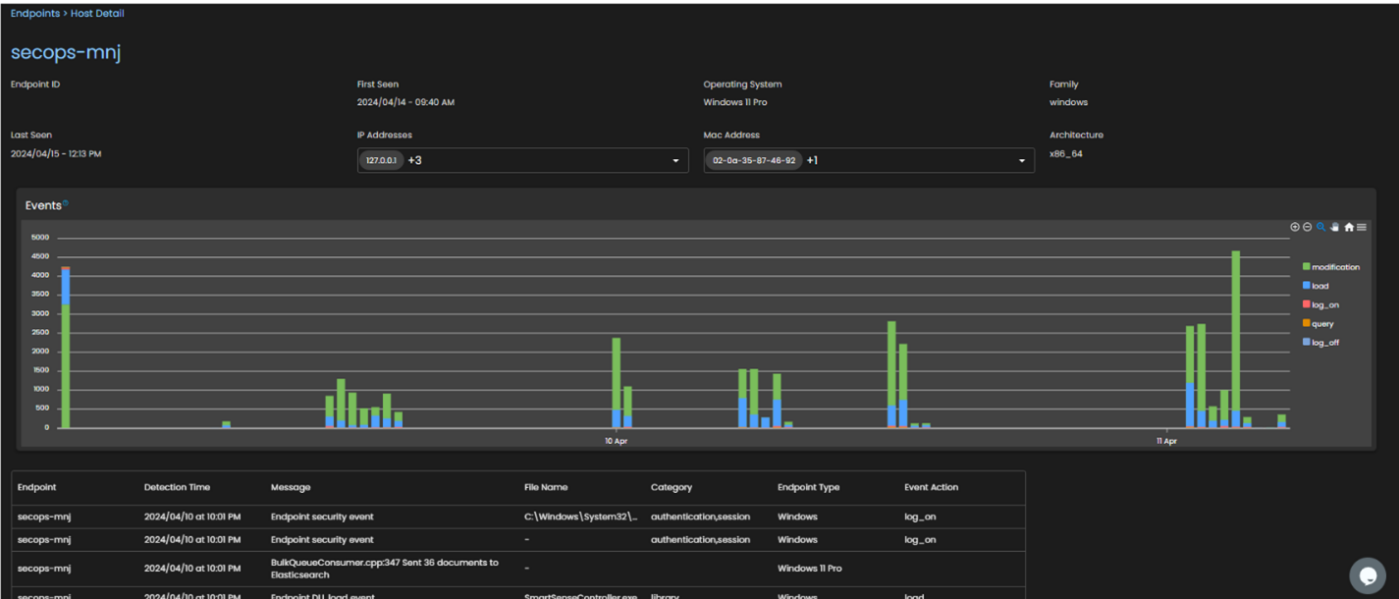
Endpoint Profile

- **Endpoint Identification:** Each endpoint is identified by unique attributes such as hostname, IP address, MAC address, operating system version, and associated user.
- **Events:** Displays a log of security events and activities specific to the selected endpoint, including process executions, file modifications, network connections, logins, and other relevant activities.
- **Behavioral Activity:** Provides insights into the behavioral activity of the endpoint, highlighting patterns of normal behavior and deviations indicative of suspicious or malicious activity.
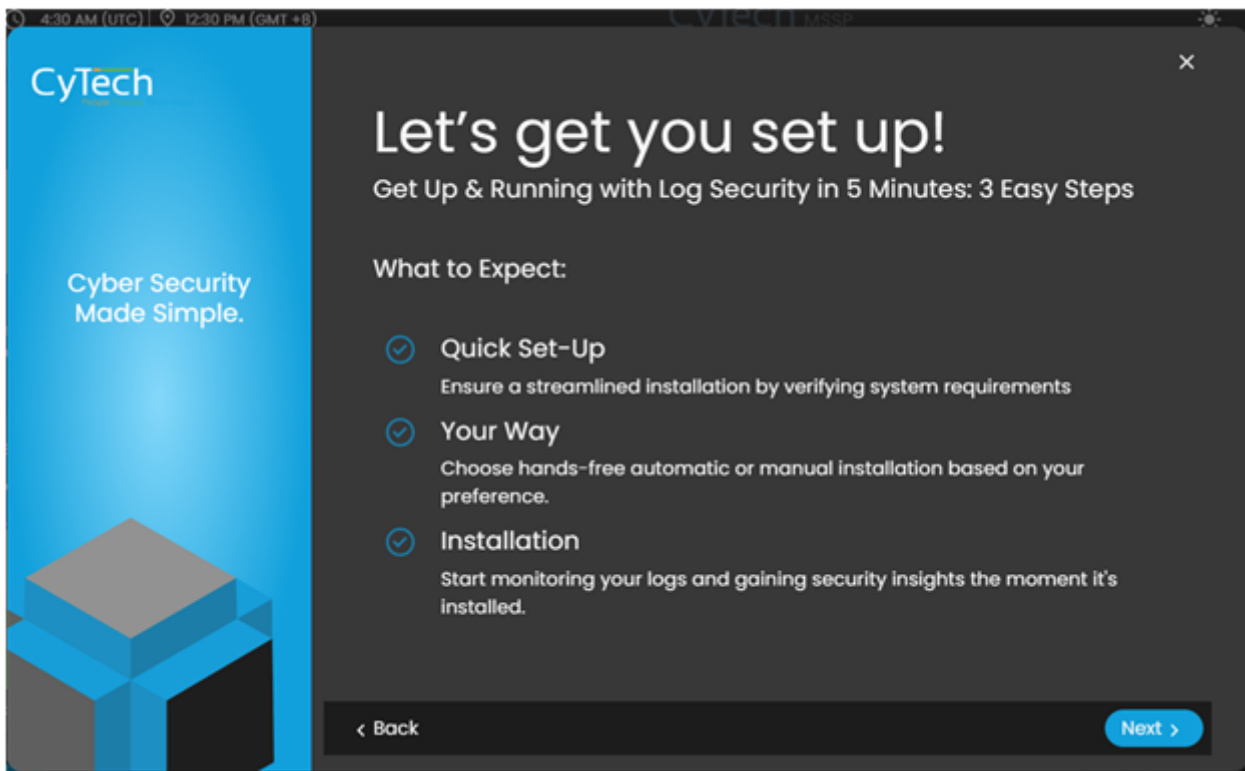
Installation Manual

- **Step 1:** Click the **"Let's Go"** button on the dashboard to initiate the installation process.
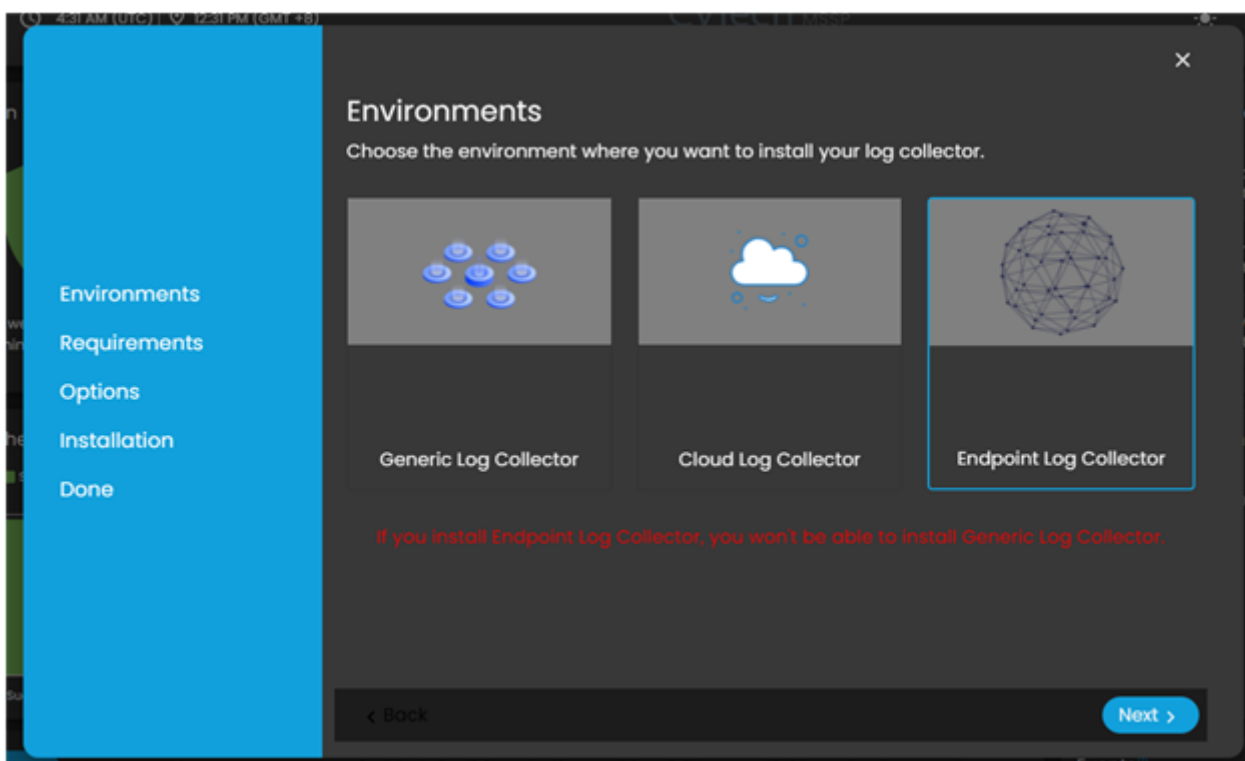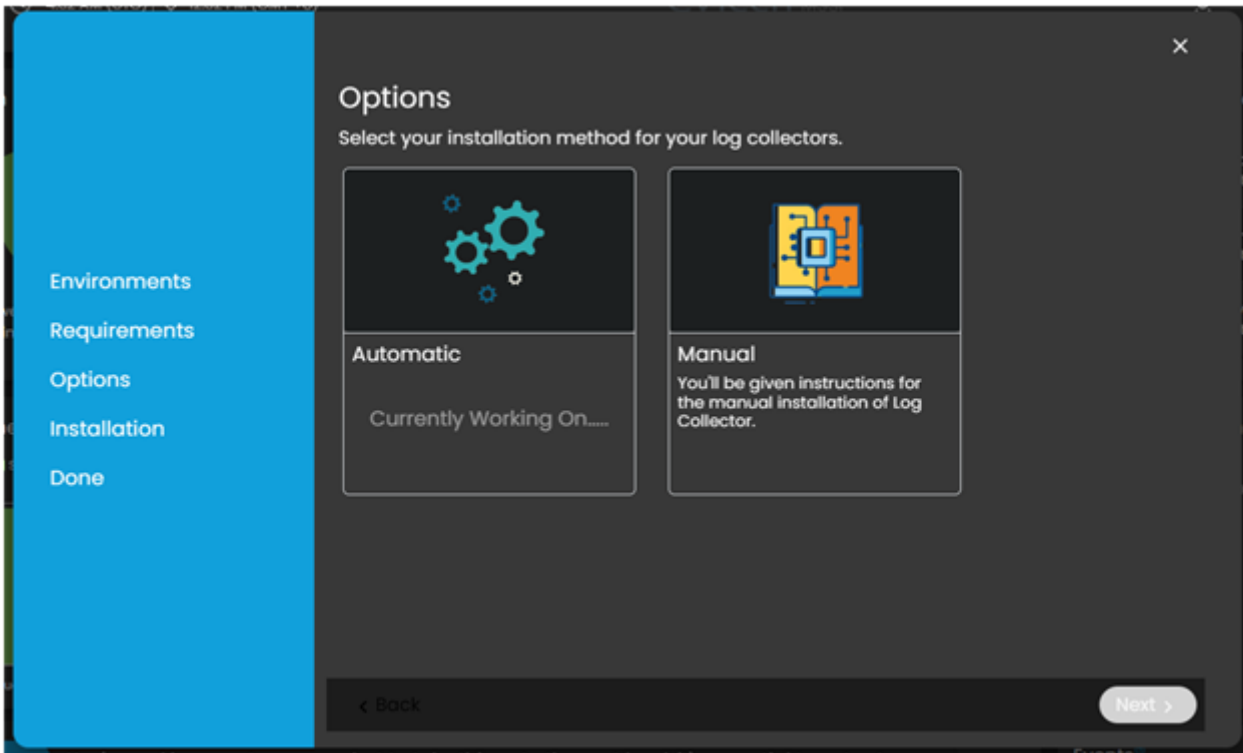
- **Step 2:** A pop-up modal will appear with instructions on proceeding with the setup.
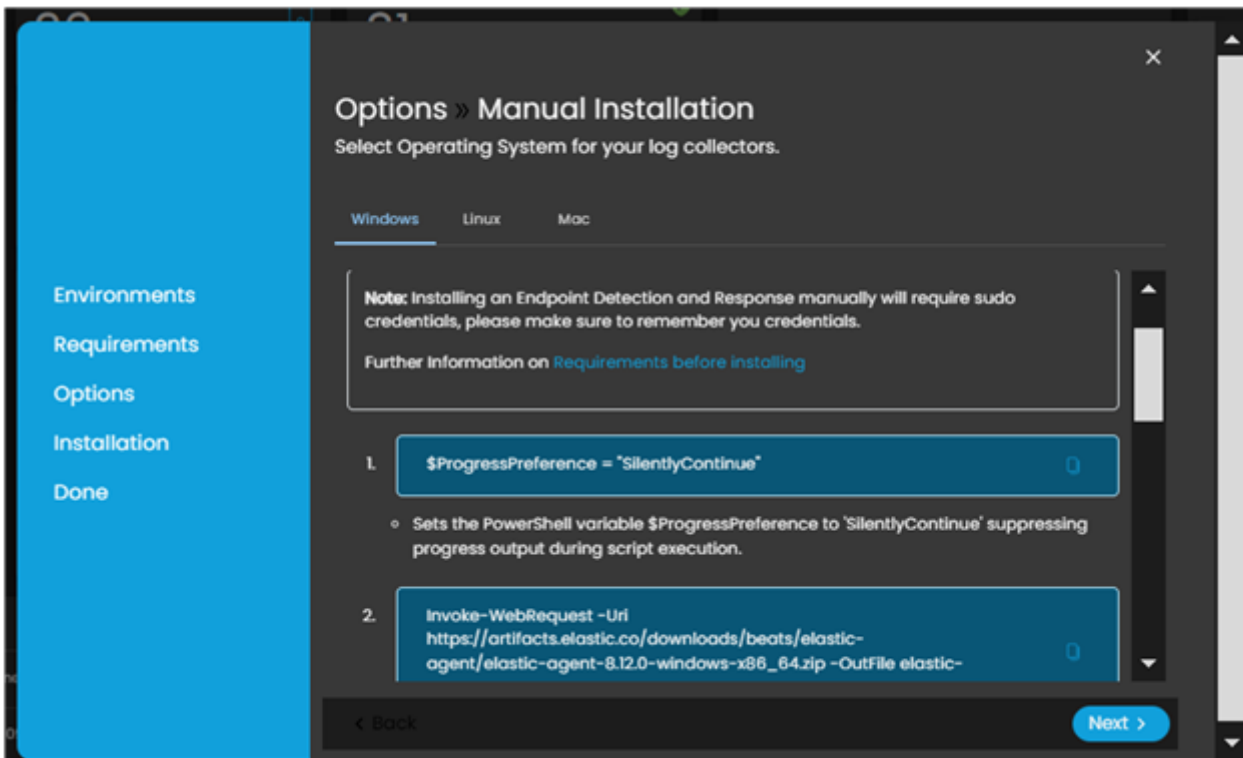

- **Step 3:** Select the **"Endpoint Log Collector"** option to specify the environment for installing the agent.

- **Step 4:** Choose between automatic or manual installation options.

- **Step 5 Manual:** If selecting Manual, follow the provided steps for installation.

If you need further assistance, kindly contact our support at info@cytechint.com for prompt assistance and guidance.