AQUILA - Endpoint Detection and Response (EDR) Manual Installation

Endpoint Detection and Response (EDR), is a cybersecurity technology that focuses on detecting, investigating, and responding to suspicious activities and threats on endpoints, such as workstations, laptops, and servers. EDR solutions provide visibility into endpoint activities and help security teams identify and mitigate potential threats before they can cause significant harm.

Pre-requisites

1. **Access to CyTech - AQUILA**
   - Only users assigned the **"Owner"** or **"Admin"** role can access the Log Collector installation resources within the platform.

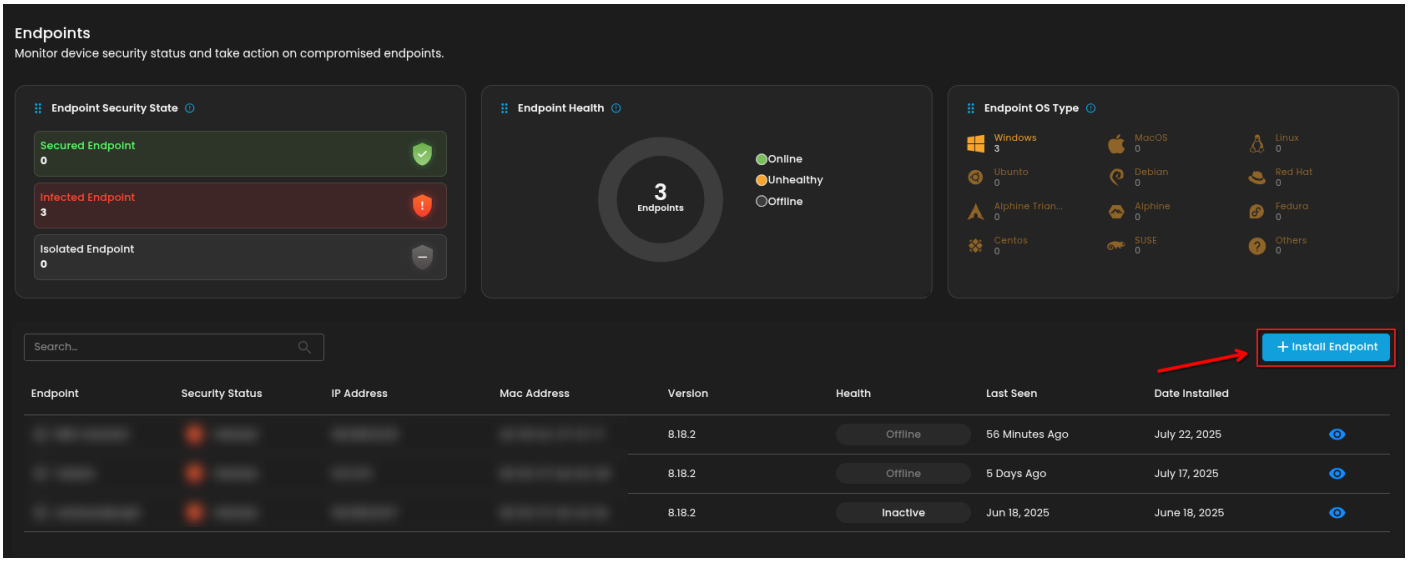
Steps to Add AQUILA EDR

Please follow the steps below to add a Log Collector using Windows Environment.

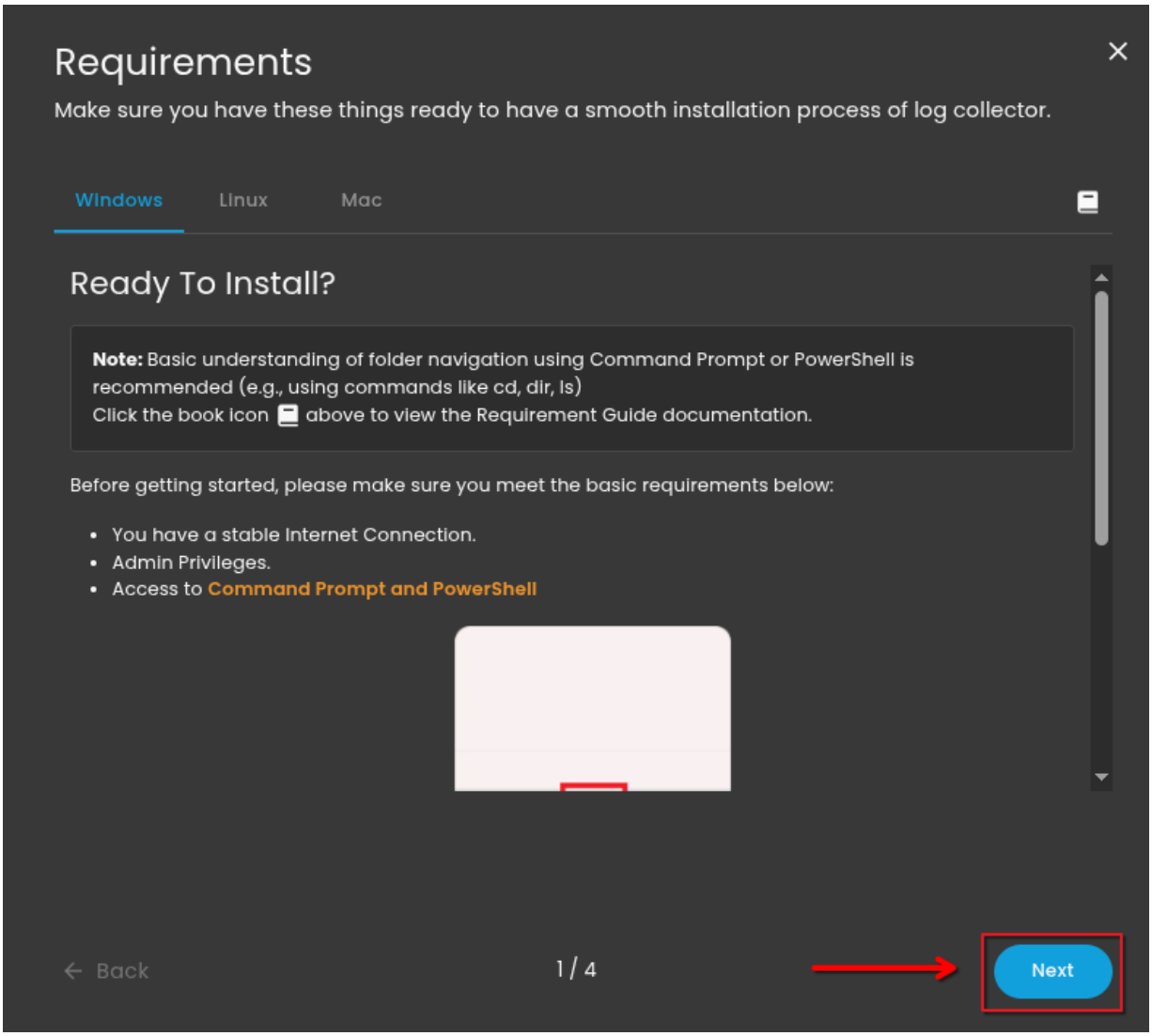
1. Log in to **CyTech - AQUILA**. Click here: **usdc.cytechint.io**

- Click **Collapse** to view side panel. Then navigate through **Domains>Cyber Monitoring>Endpoint Detection and Response>Endpoints**.

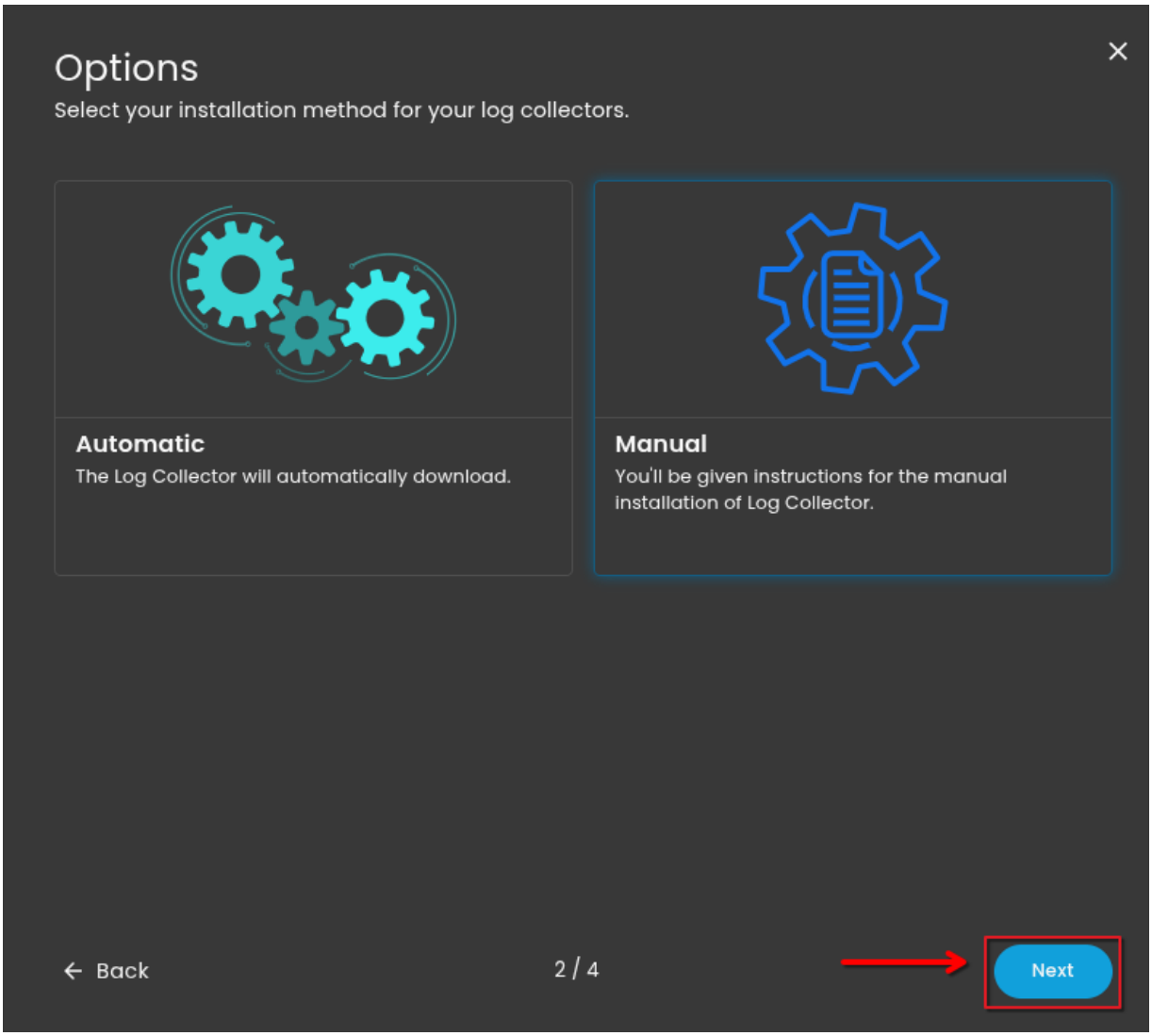
2. Click "**Install Endpoint**" to start installation window.



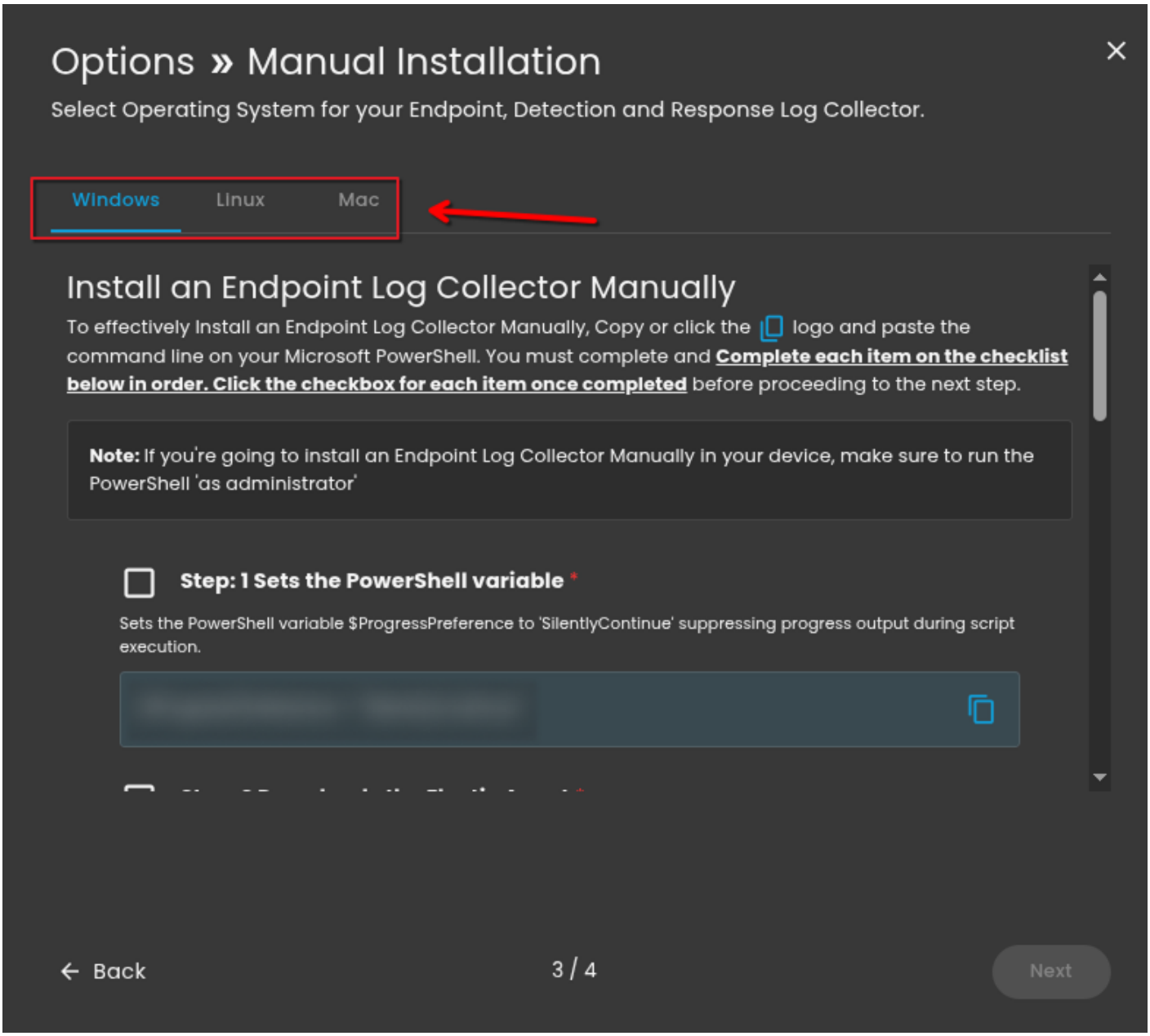
3. Review the needed requirements for each Operating Systems and click "Next".



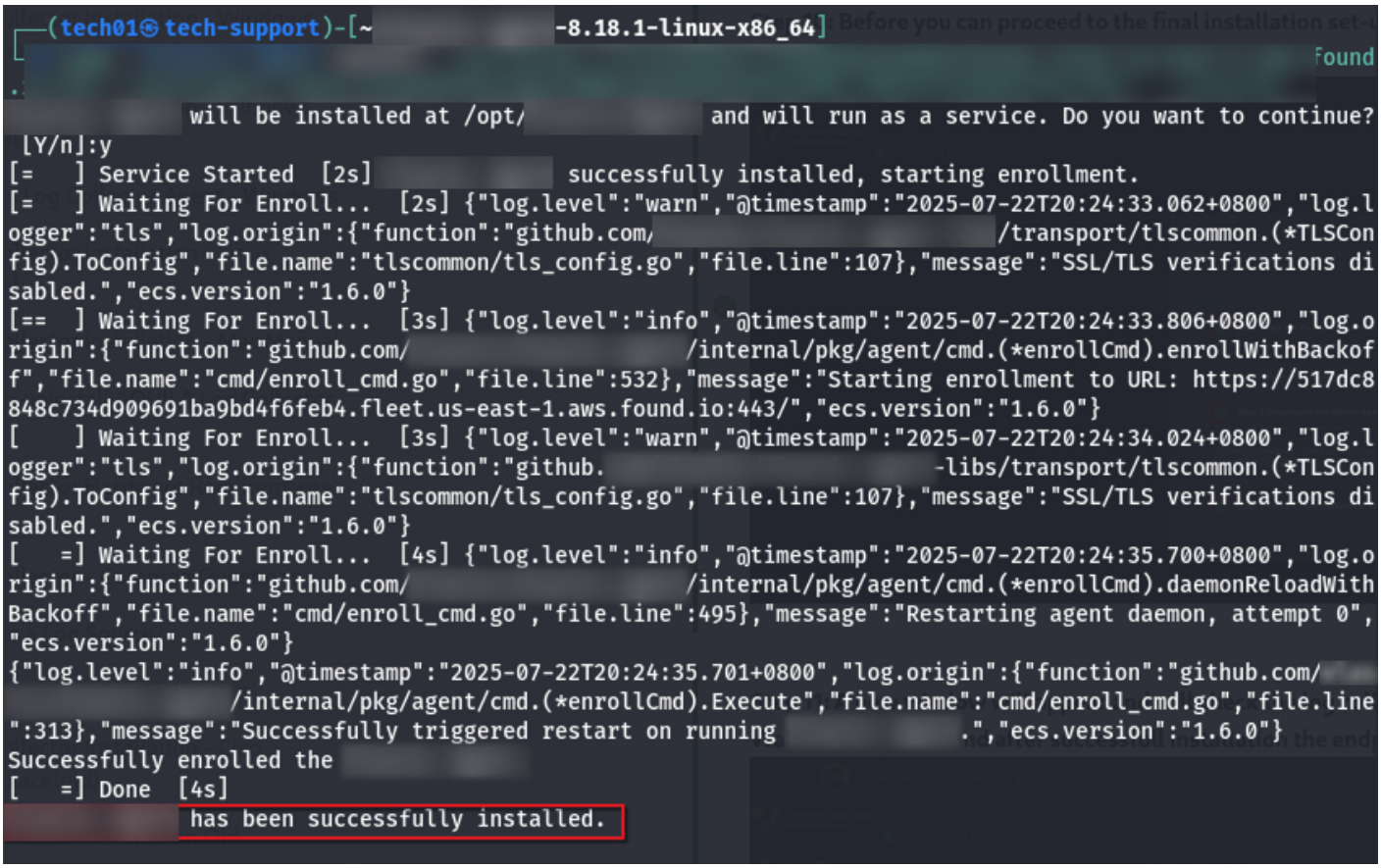
4. Choose "Manual" installation and click "Next".



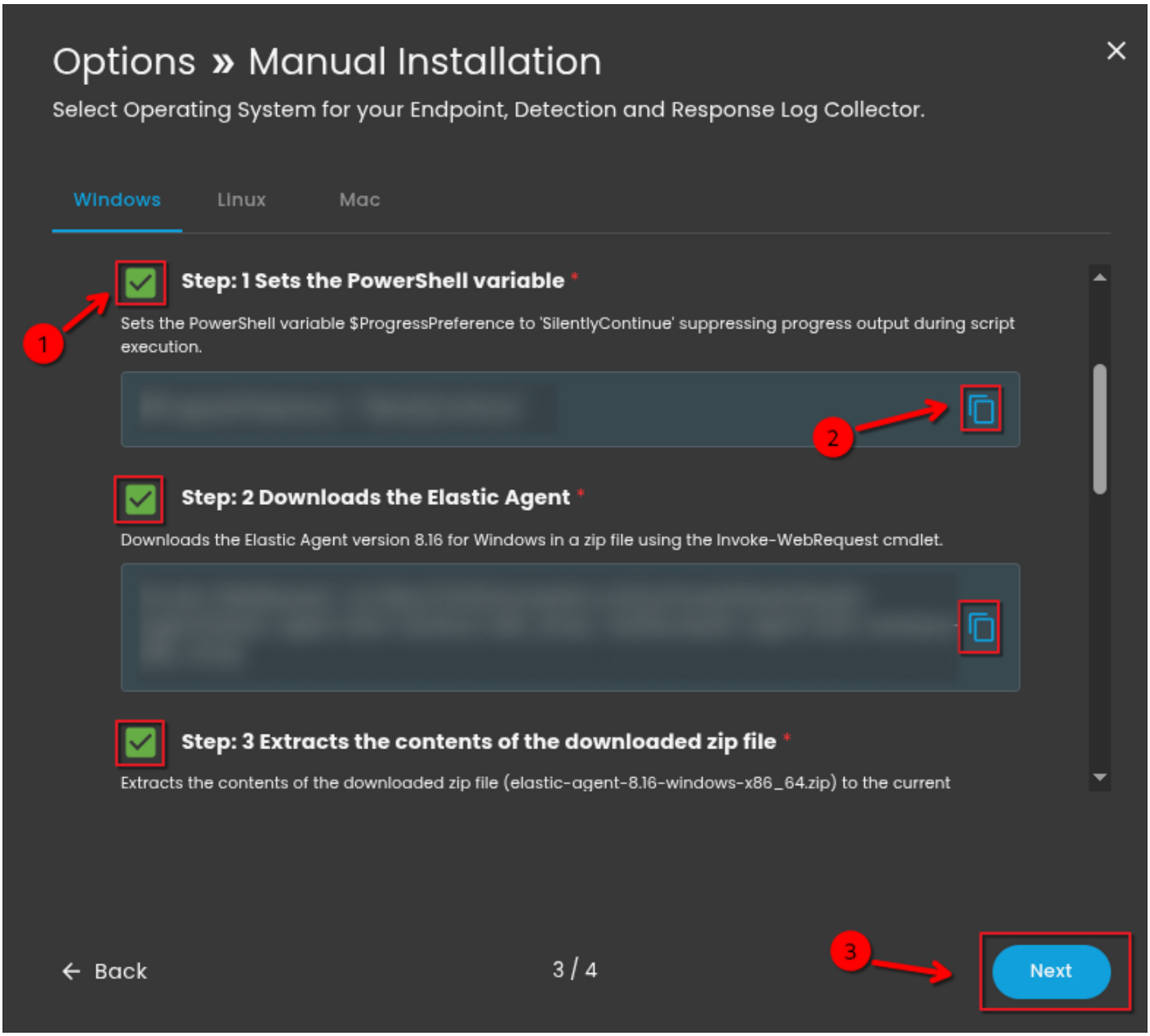
5. Choose the correct Operating System for your endpoint. After choosing the type of your Operating System, the commands will display below needed for installing the EDR agent.



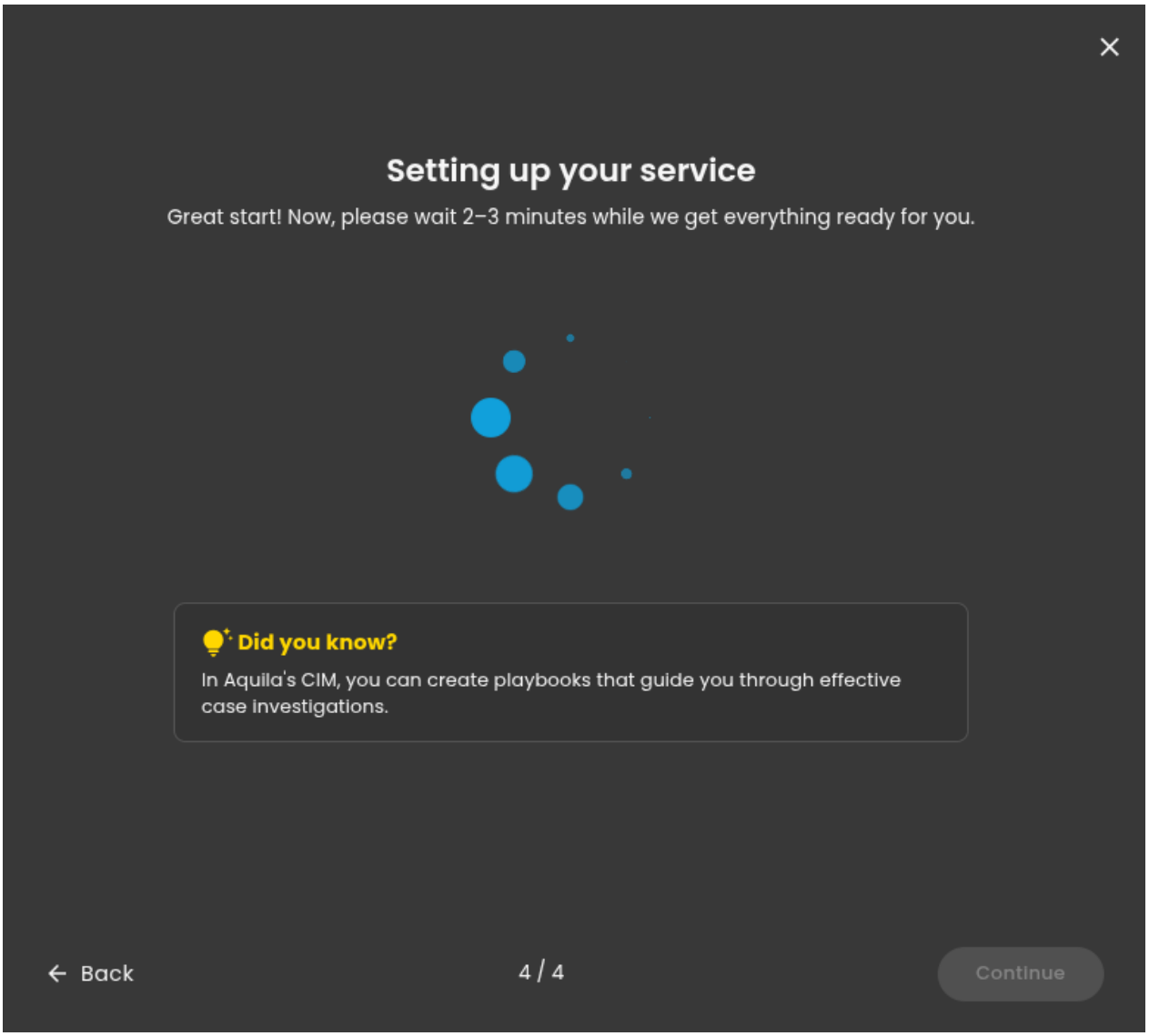
6. Execute the command in your Endpoint environment using PowerShell or terminal under admin privilege. Once the commands are executed successfully, you should see an output similar to the example shown in the image below. Go back to Cytech - Aquila to finish manual installation.



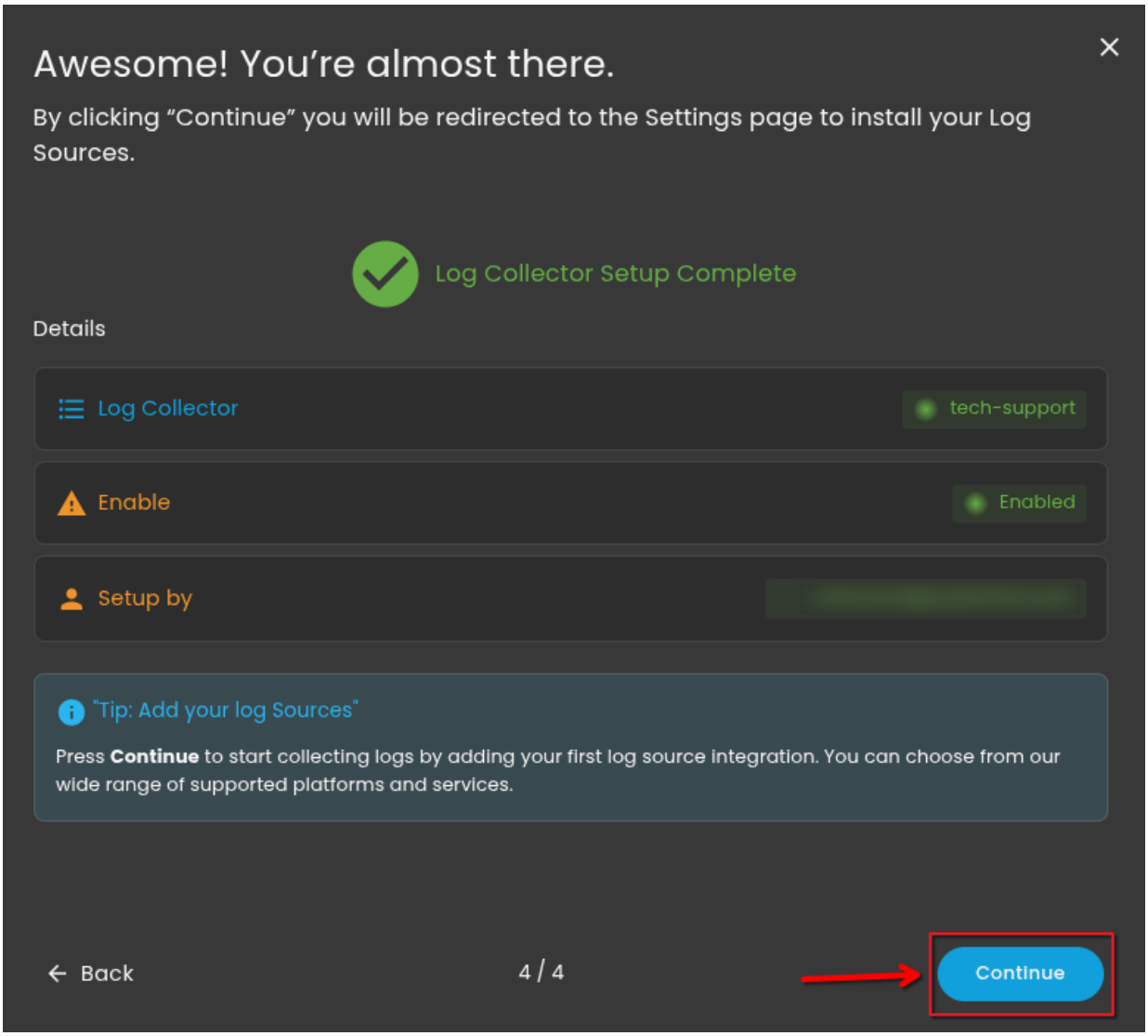
7. **Before you can proceed to the final installation set-up make sure you check off each steps required. Then you can click "Next".**



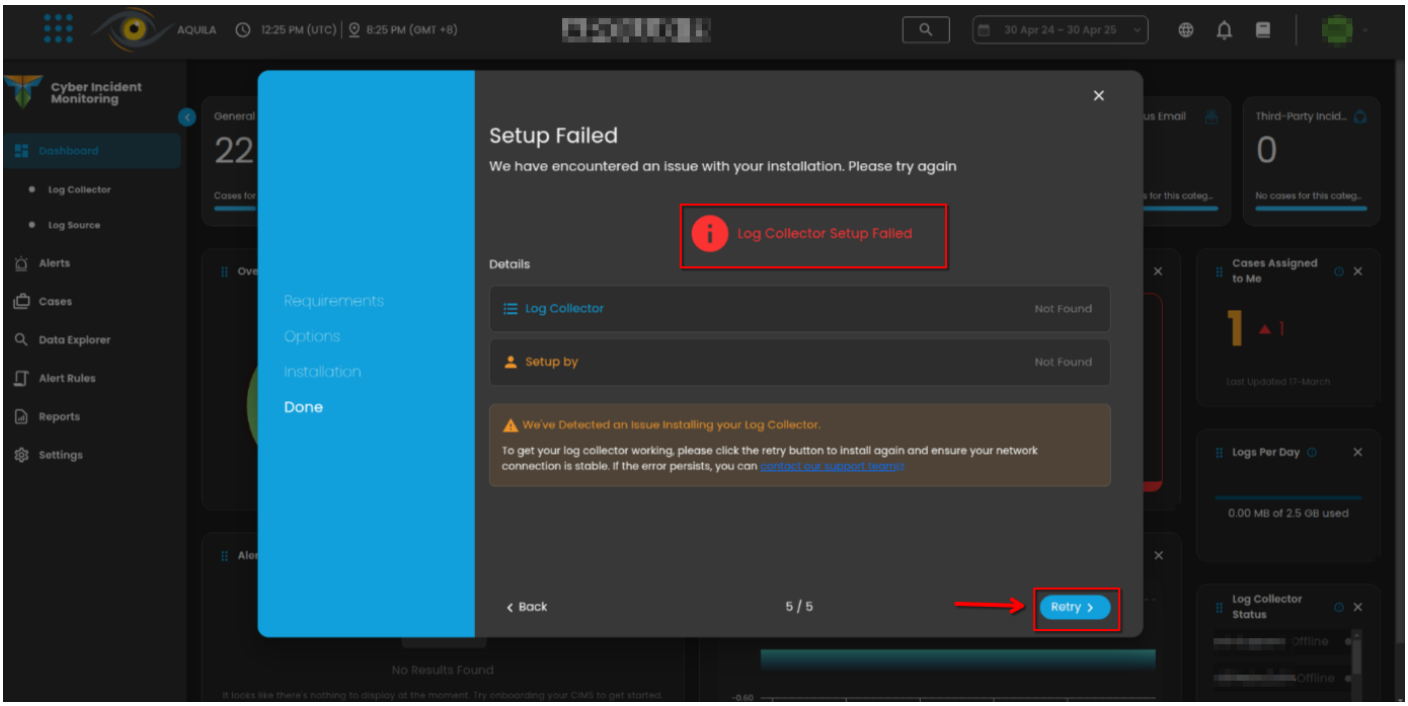
8. **A new window will appear and will check the log collector status and update the latest installation of EDR agent. Wait for it to finish and after successful installation the endpoint will displayed in the dashboard.**



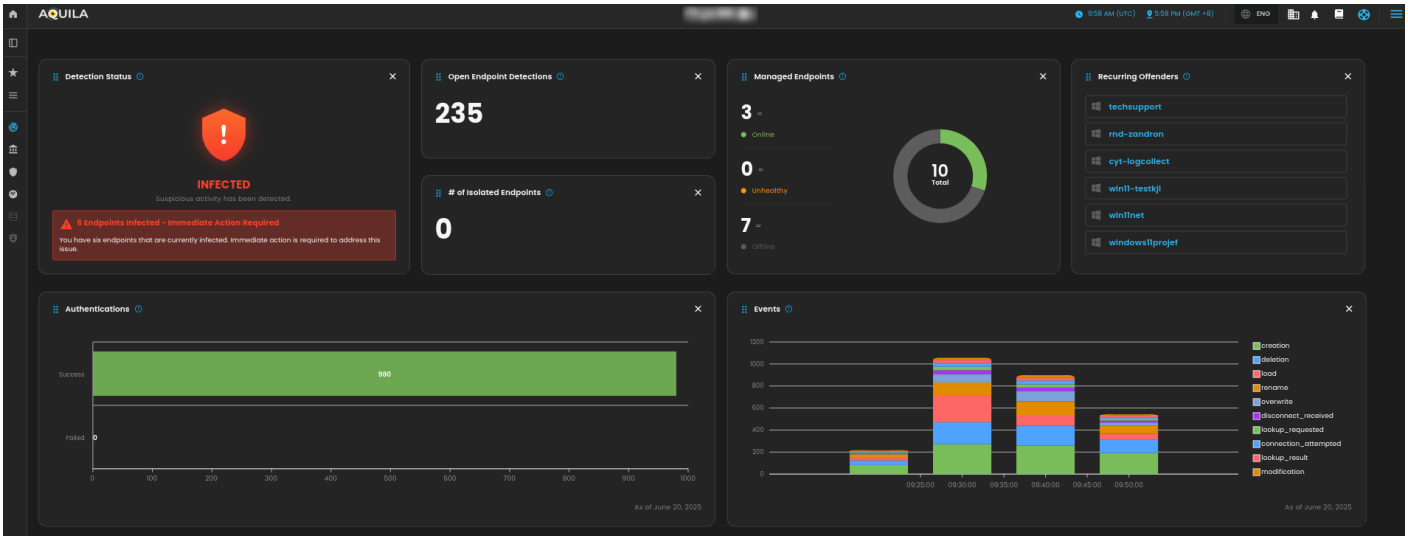
9. This step confirms the successful installation and enrollment of the EDR Agent with the fleet server.

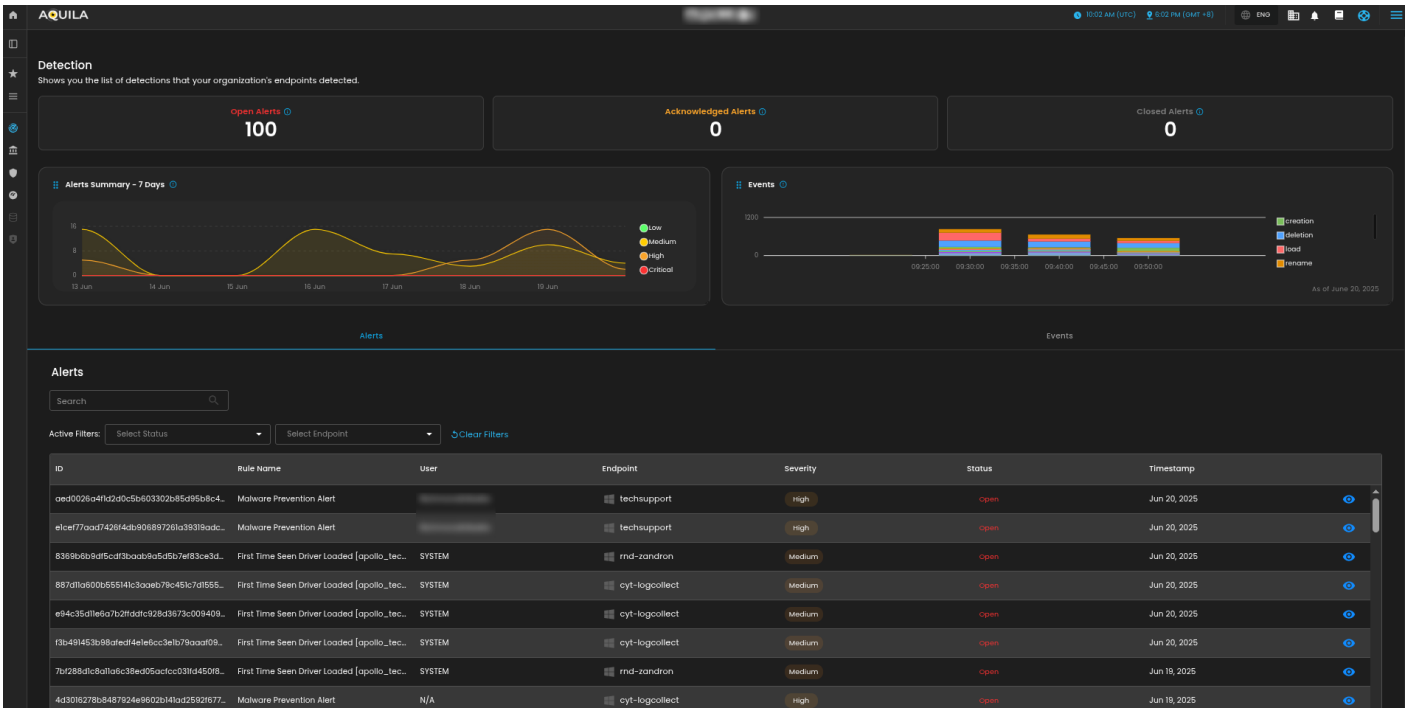


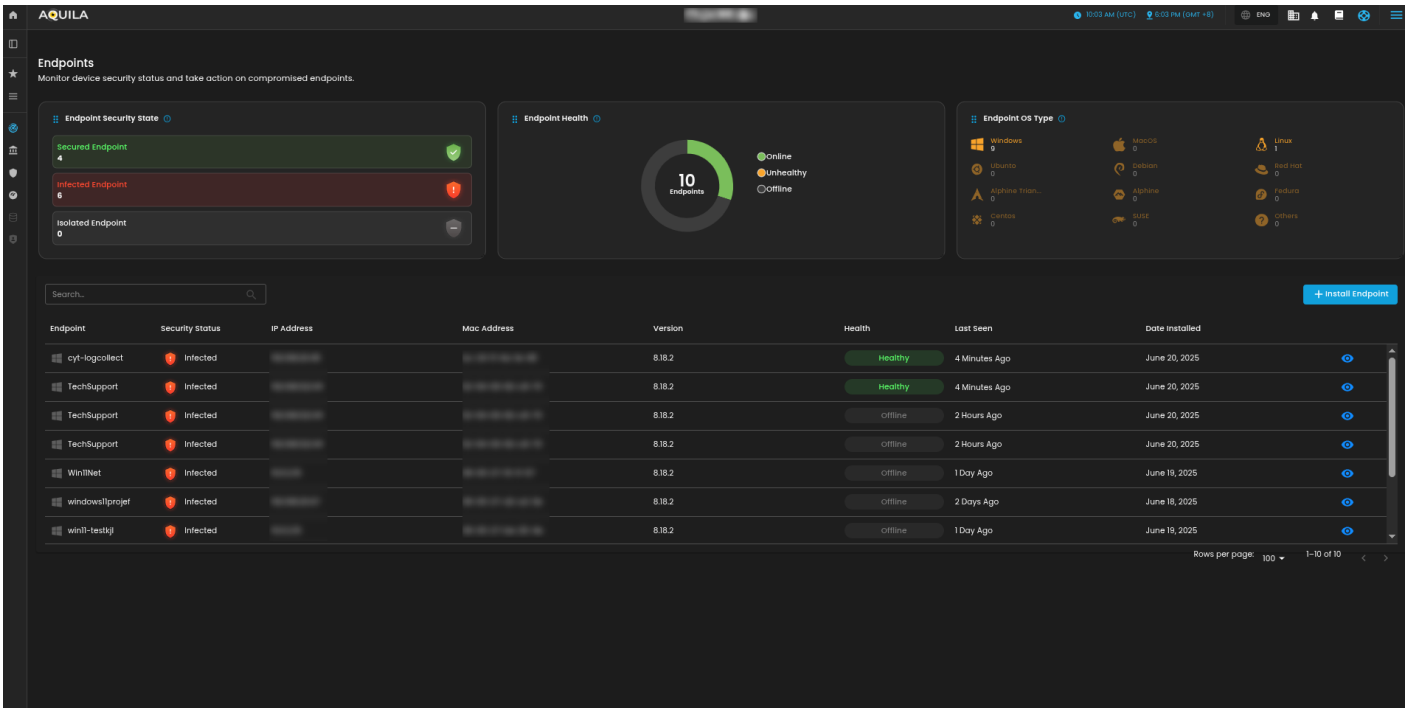
> ***If you encounter ***Log Collector Setup Failed***. Please click "Retry" and carefully go back to Step 5 or 6. You can also try "***Manual***" installation. If issues persist, please contact our technical support at ***support@cytechint.com*** for prompt assistance and guidance.*



For a more detailed report and in-depth analysis, navigate to **CyTech - AQUILA > Cyber Monitoring > Endpoint Detection and Response (EDR)**. This section provides comprehensive visibility into endpoint activity, detection timelines, threat classifications, and response actions to support advanced threat analysis and incident investigation.







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

Revision #8
Created 22 July 2025 12:12:27 by Richmond Abella
Updated 19 November 2025 16:49:09 by Richmond Abella