Log Collector Installation - Linux Manual

Log Collector Installation in CyTech - Aquila

This guide outlines the step-by-step process for deploying the **Elastic Agent** as a log collector within the **CyTech - Aquila** environment. Following these instructions will establish a secure and automated mechanism for log collection and management, enabling centralized visibility and analysis critical to cybersecurity operations.

Pre-requisites

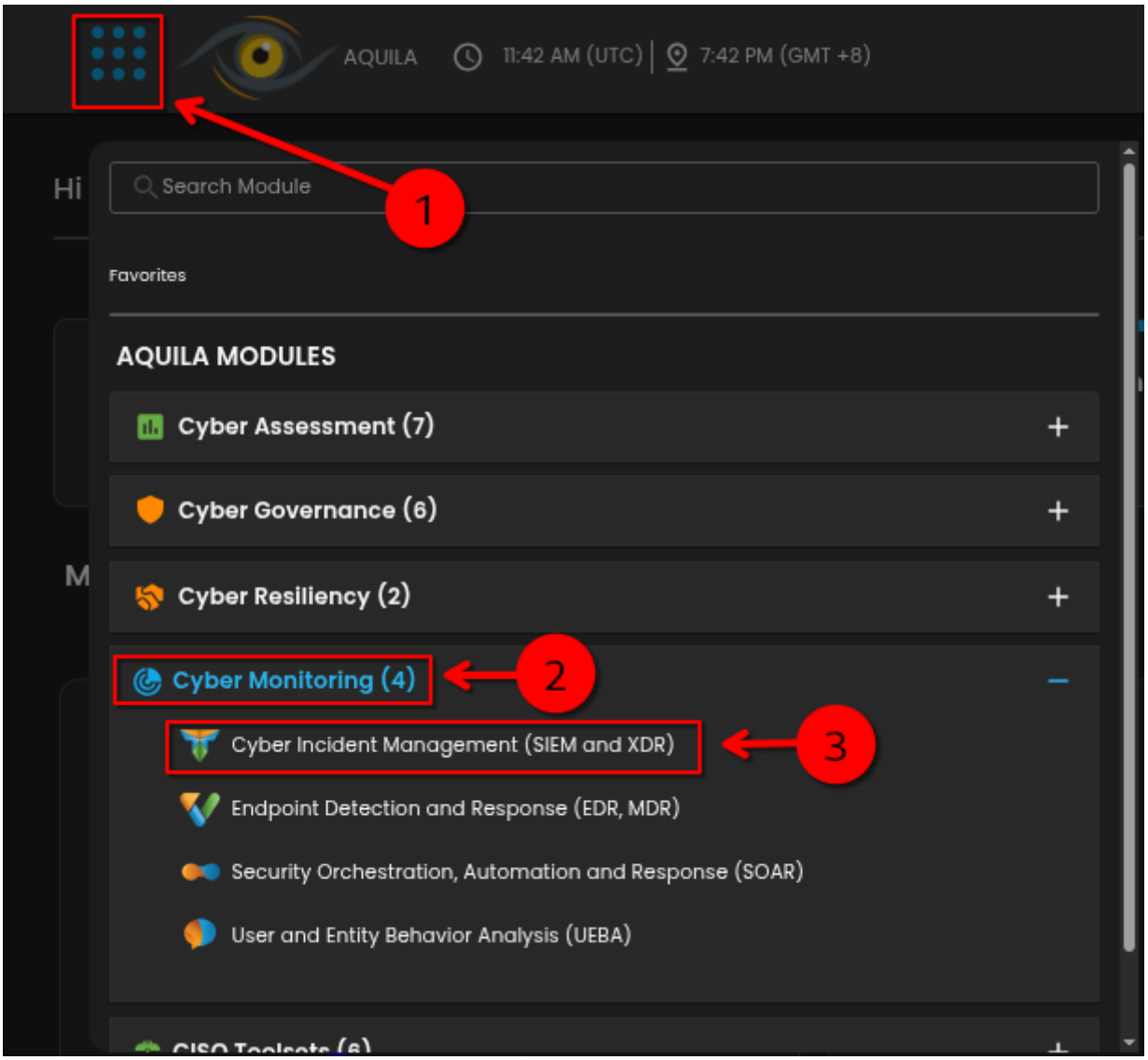
1. **Access to CyTech - Aquila**
   - Only users assigned the **"Owner"** or **"Admin"** role can access the Log Collector installation resources within the platform.
2. **Dedicated Virtual Machine for Log Collector Deployment**
   - **Dedicated Unit**: It is recommended to use a separate, dedicated VM exclusively for the Log Collector to prevent resource contention and ensure stable performance.
   - **Virtual Machine (VM) Preferred**: Deploying the Log Collector on a VM offers greater flexibility, scalability, and easier maintenance compared to physical hardware.
   - **Always Online**: The virtual machine must remain continuously online to ensure uninterrupted log collection from all integrated sources.

> For the full Log Collector Hardware Requirements Guide, please refer to this link: Log Collector Hardware Requirements Guide

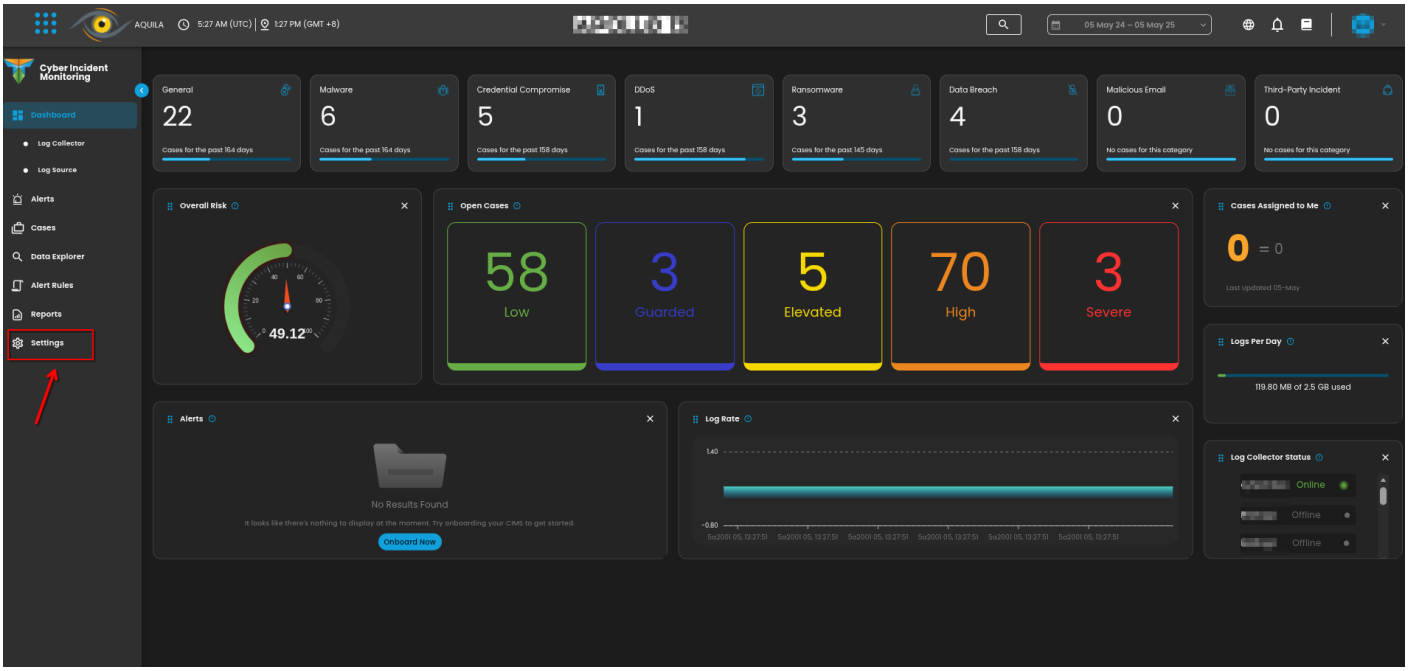
Steps to Add Log Collector

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

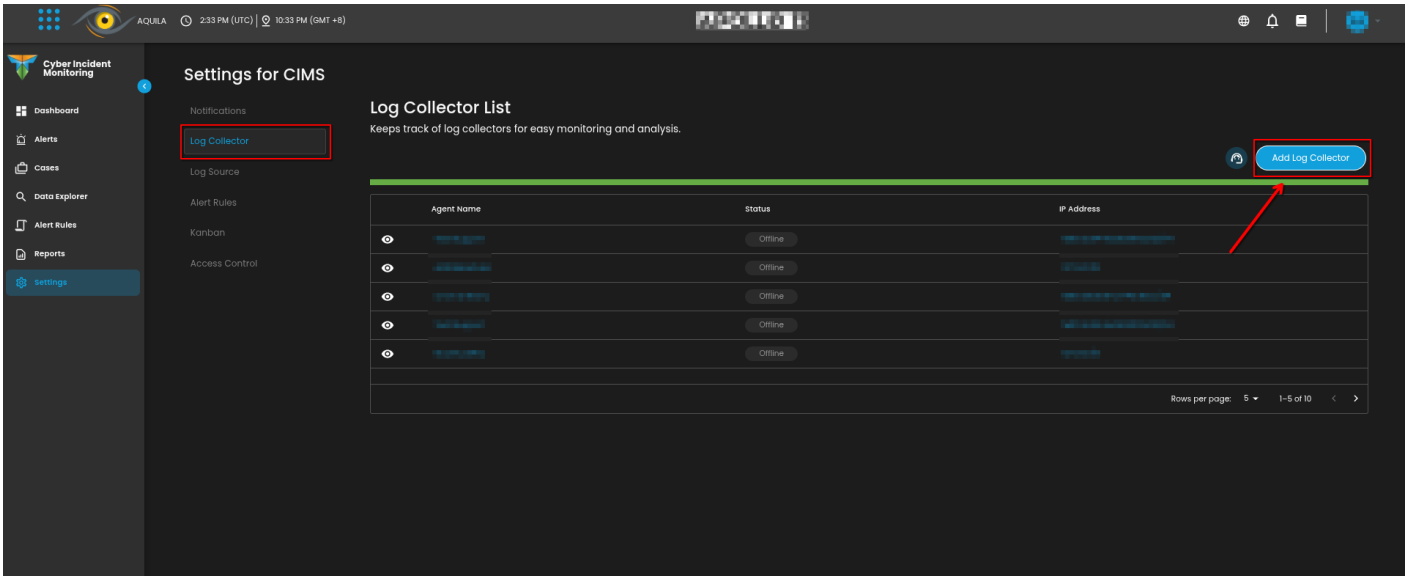
1. Log in to **CyTech - Aquila**. Click here: **cytechint.io** .
   - Go to the **Aquila Modules>Cyber Monitoring>Cyber Incident Management (SIEM and XDR)**.



2. In the Cyber Incident Monitoring (CIM) module, navigate to the '**Settings**' section.

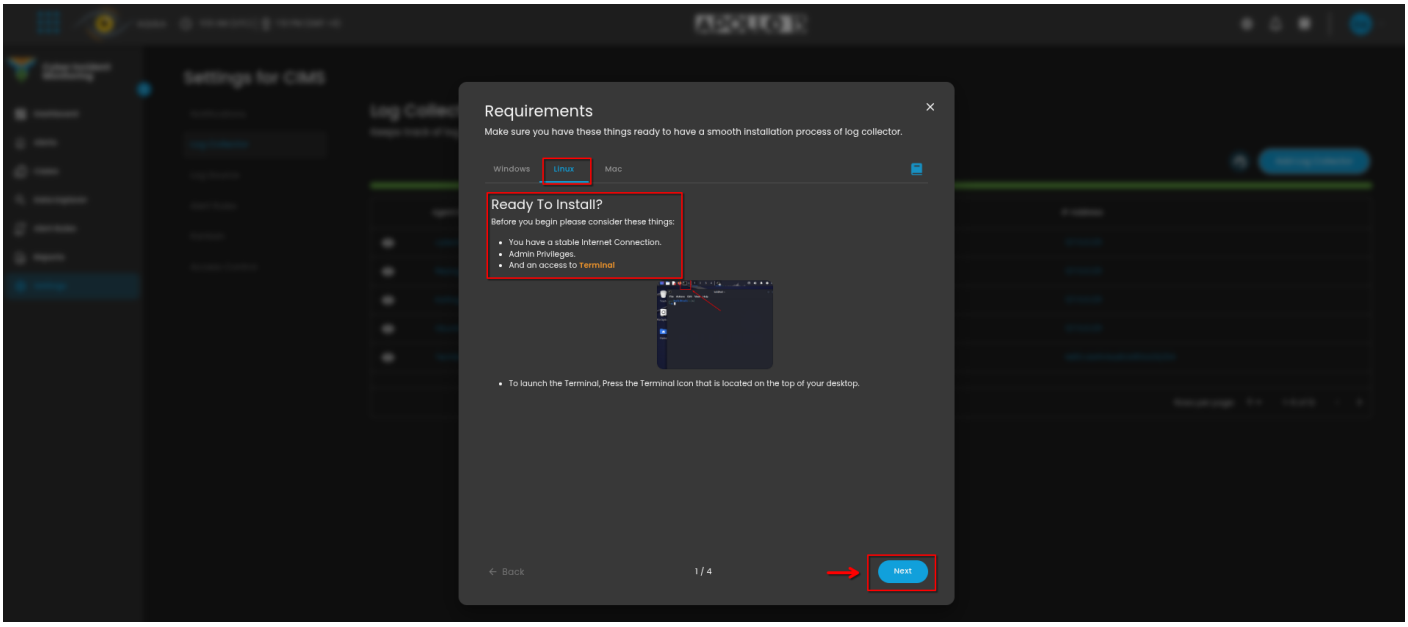


3. Navigate to the Log Collector section and click the 'Add Log Collector' button to launch the installation interface.

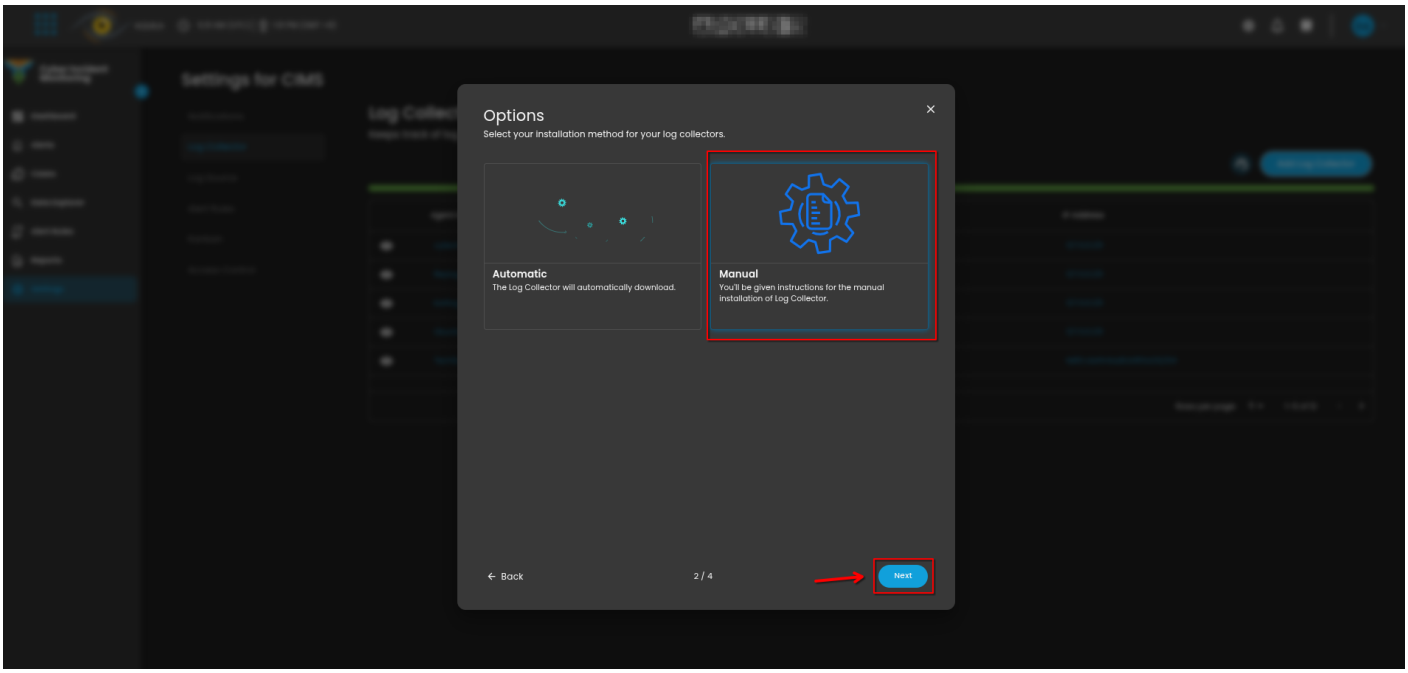


4. Once the installation window display is shown, thoroughly review the **System Requirements** specific to your operating system to ensure compatibility and avoid installation or runtime issues. Verifying these prerequisites is essential before proceeding with deployment. Then click "**Next**".

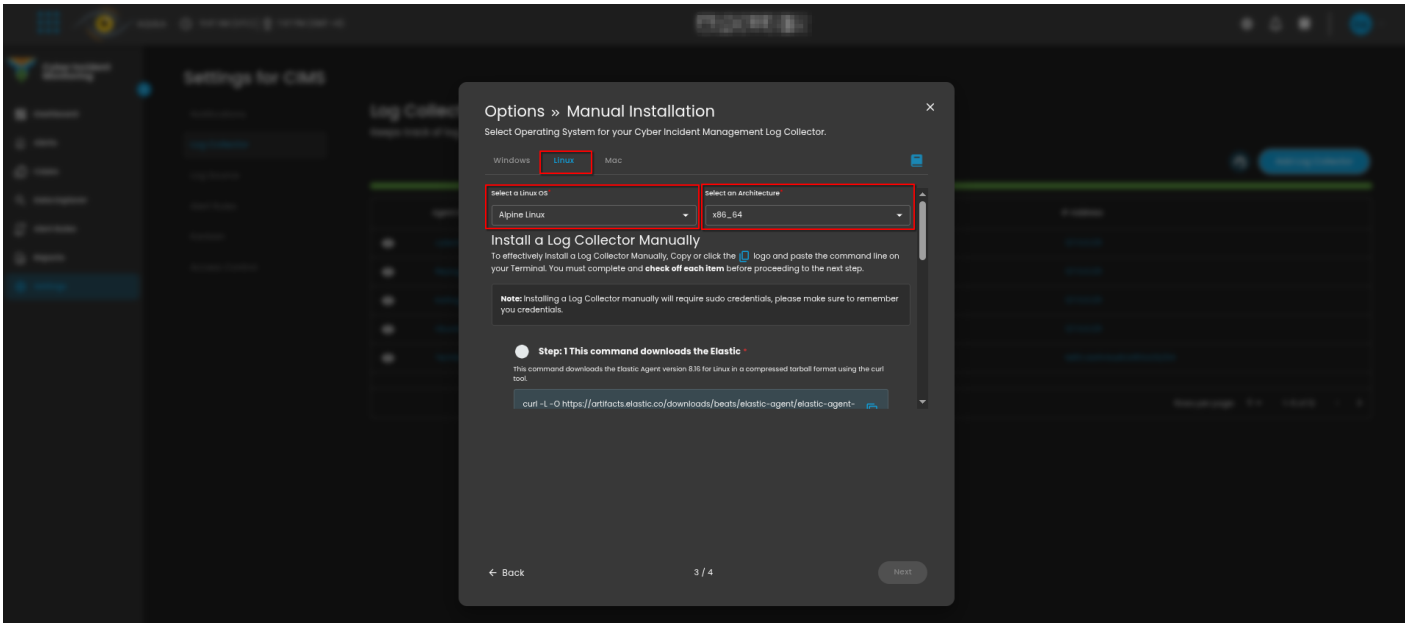
> You can also refer to our documentation manuals for Log Collector Installations Guidelines: https://docs.cytechint.io/books/log-collector-installations



5. From the options, select the "**Manual**" installation option. Then click "**Next**".

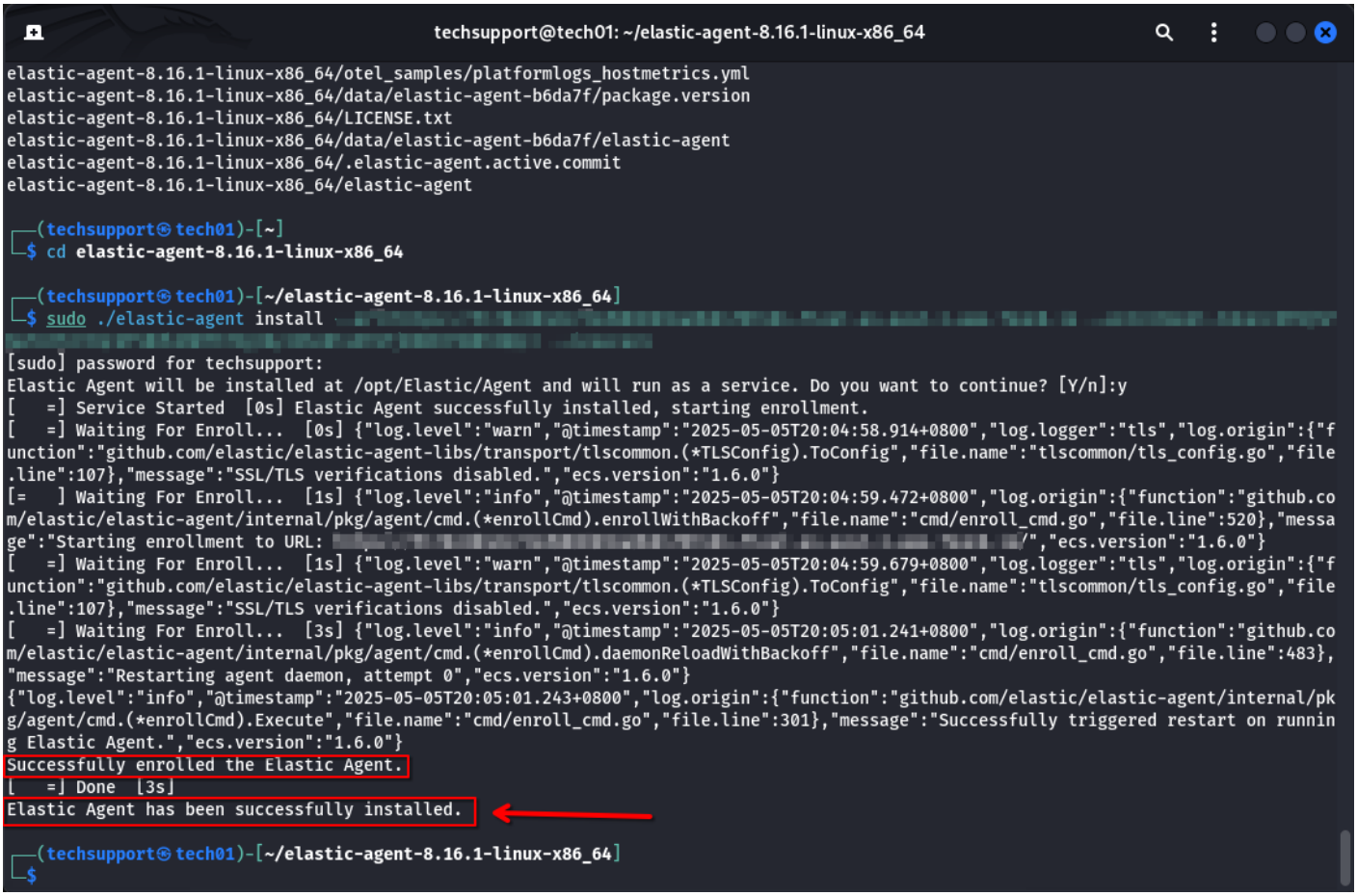


6. Carefully follow the instructions for the Manual Installation.
   - **Linux Distributions** - choose versions of the Linux operating system.
   - **Choose CPU Architecture**
     - x86_64 Architecture: Intel and AMD, x86_64 is an extension of the x86 architecture, providing 64-bit computing capabilities.
     - aarch64 Architecture: ARM architecture, specifically Apple's custom-designed ARM-based processors known as Apple Silicon (M1, M1 Pro, M1 Max, M1 Ultra, and M2 chips).
   - **Copy the commands** provided on the installation page and execute them sequentially to ensure successful execution. These commands are required to complete the log collector installation in the subsequent steps.

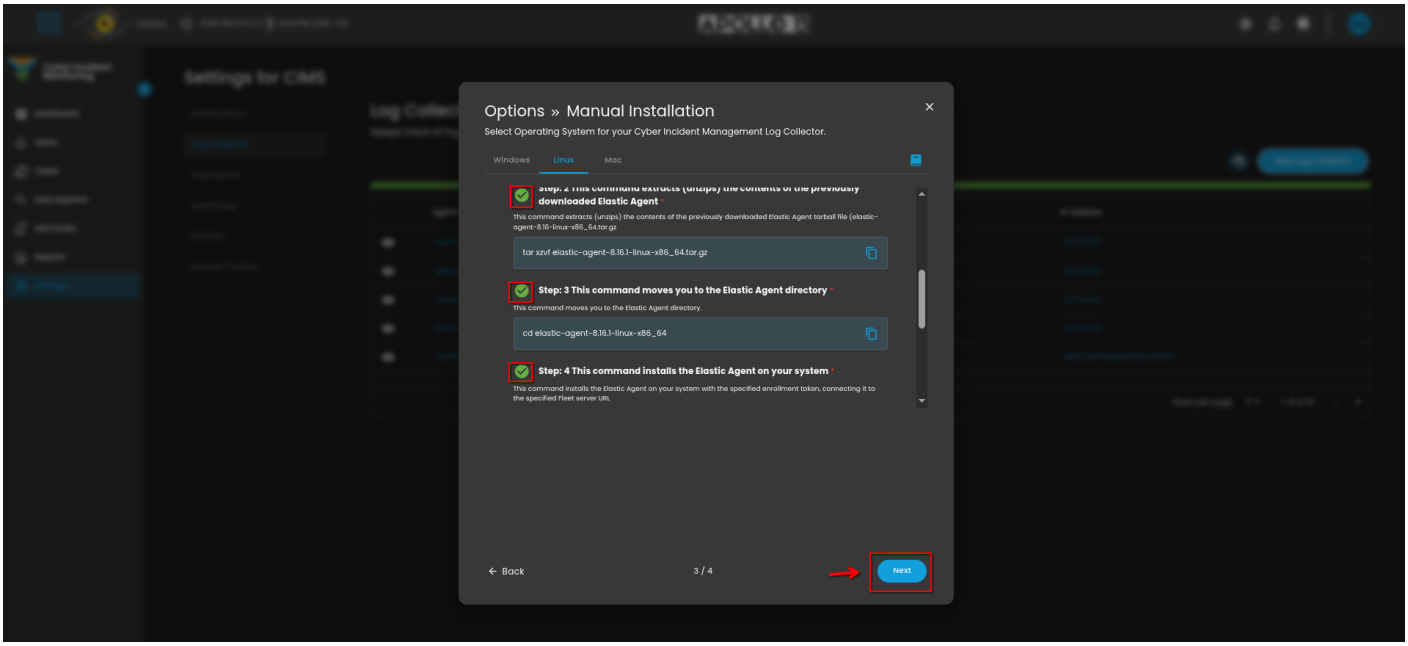


7. In your dedicated environment for your Log Collector, open the **Terminal** and provided you have **root privilege.** Execute the commands displayed in Step 6 as shown in the installation manual.

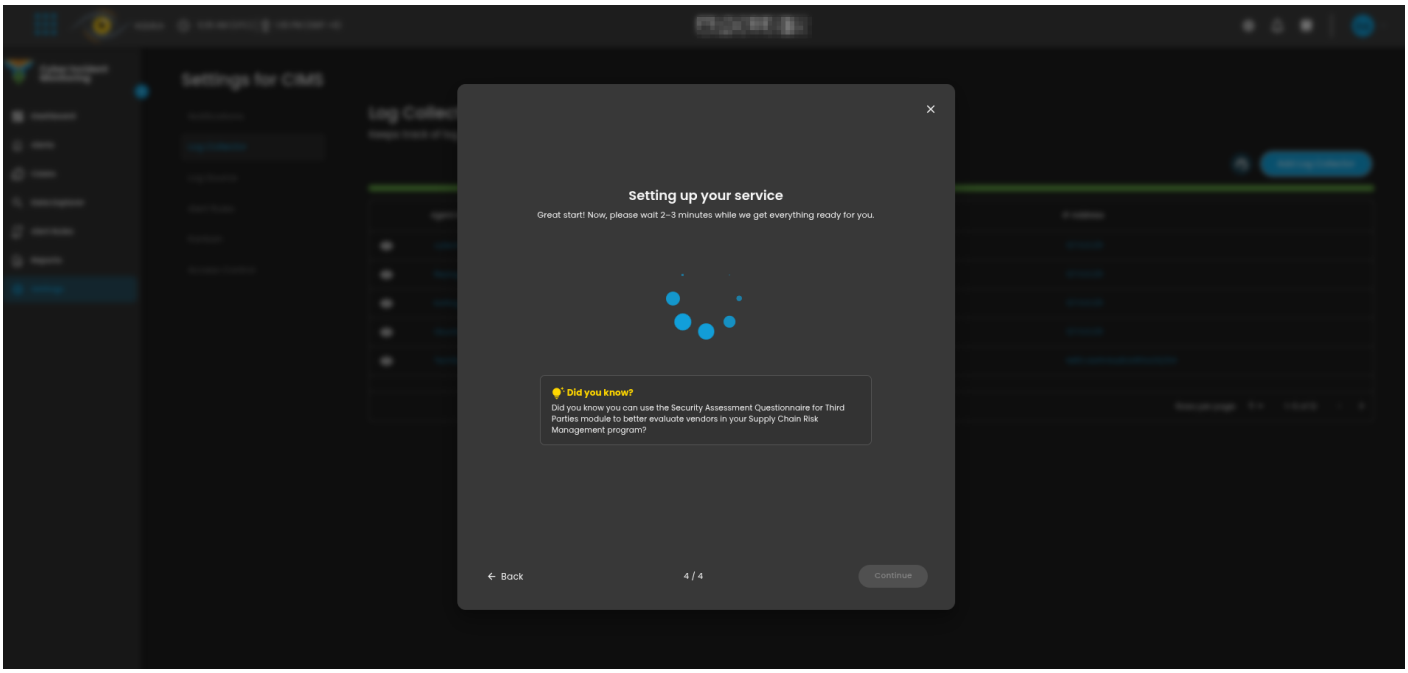
Once the commands are executed successfully, you should see an output similar to the example shown in the image below. Go back to **Cytech - Aquila** to finish manual installation.



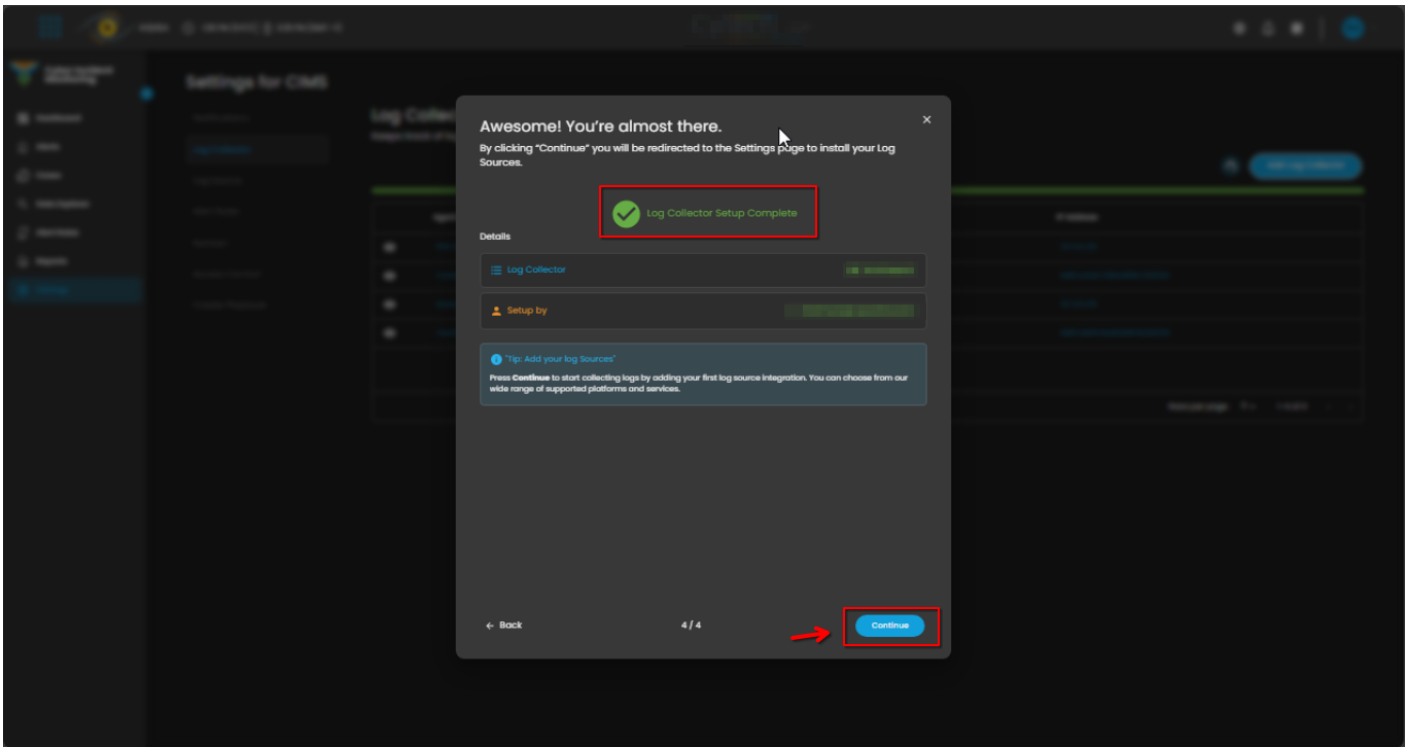
9. Before you can proceed to the final installation set-up make sure you check off each steps required. Then you can click "**Next**".



10. Allow 3–5 minutes for the Log Collector Agent to complete registration and report its "**Online**" status to the fleet server, indicating a successful installation.

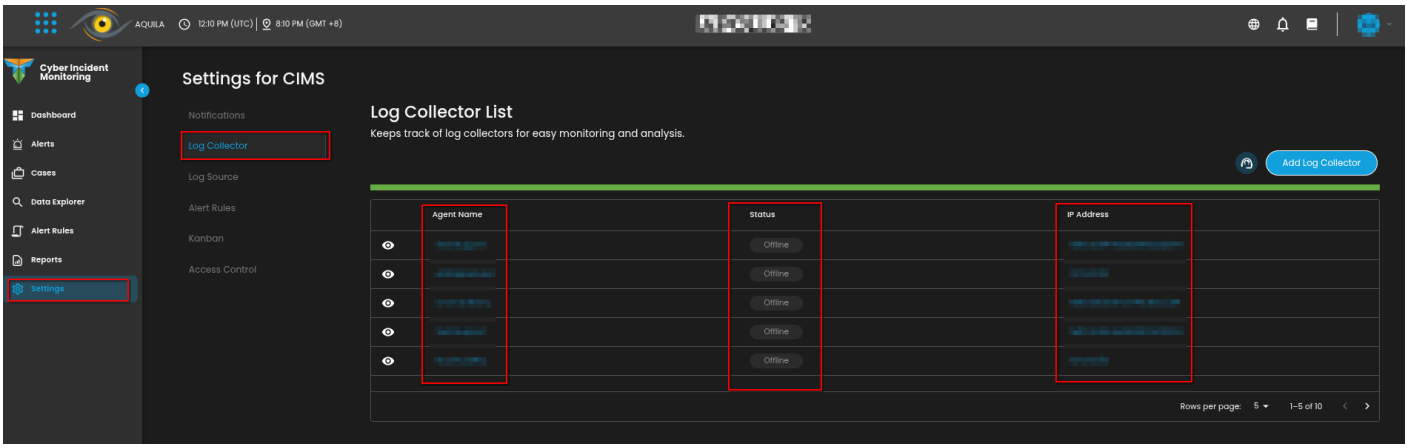


11. This step confirms the successful installation and enrollment of the Log Collector Agent with the fleet server. The interface will display the Log Collector host name and the user who performed the installation. Click "**Continue**" to complete the setup process.

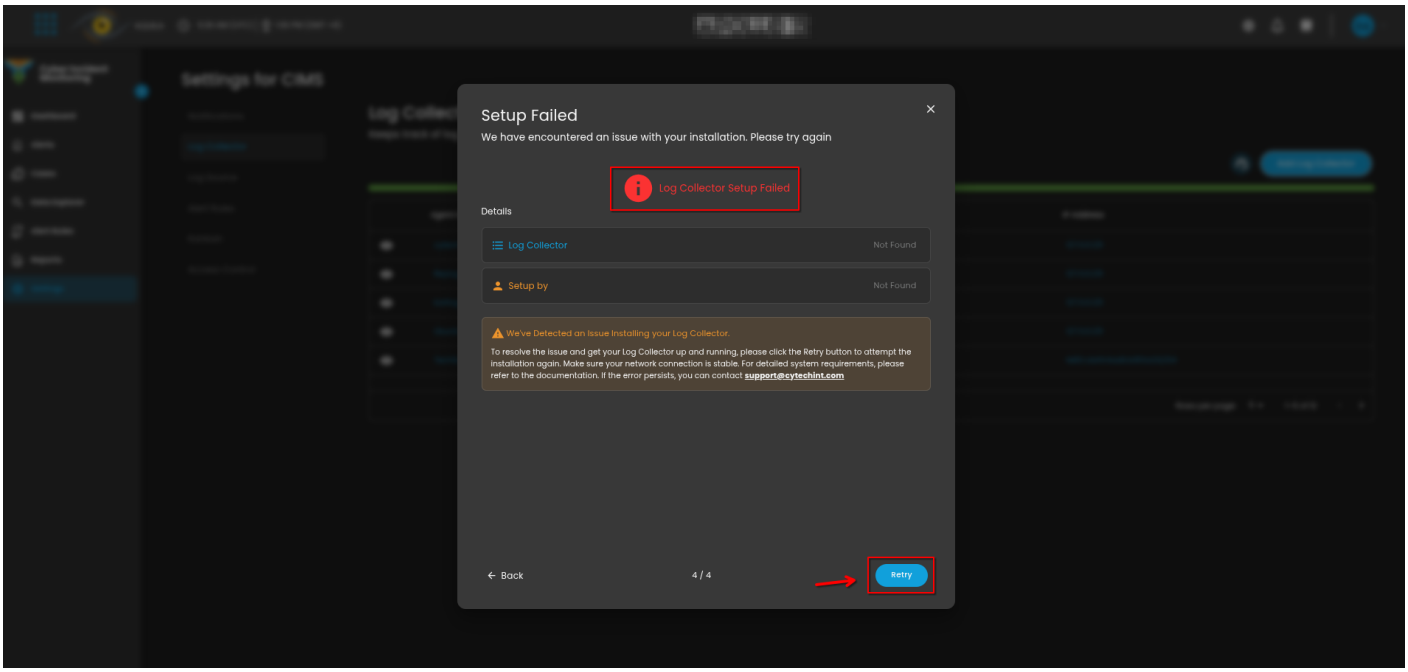


12. Also you can verify successful installation by going to **Cyber Incident Monitoring>Settings>Log Collector**.

- In the Log Collector List, you can see all the log collector installed. You can also view the Log Collector details such us: **Agent Name, Status and IP address**.



> ****If you encounter **Log Collector Setup Failed**. Please click "Retry" and carefully go gack to Steps 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.*



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

Revision #1
Created 30 April 2025 02:37:21 by Richmond Abella
Updated 5 May 2025 12:21:35 by Richmond Abella