

# 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

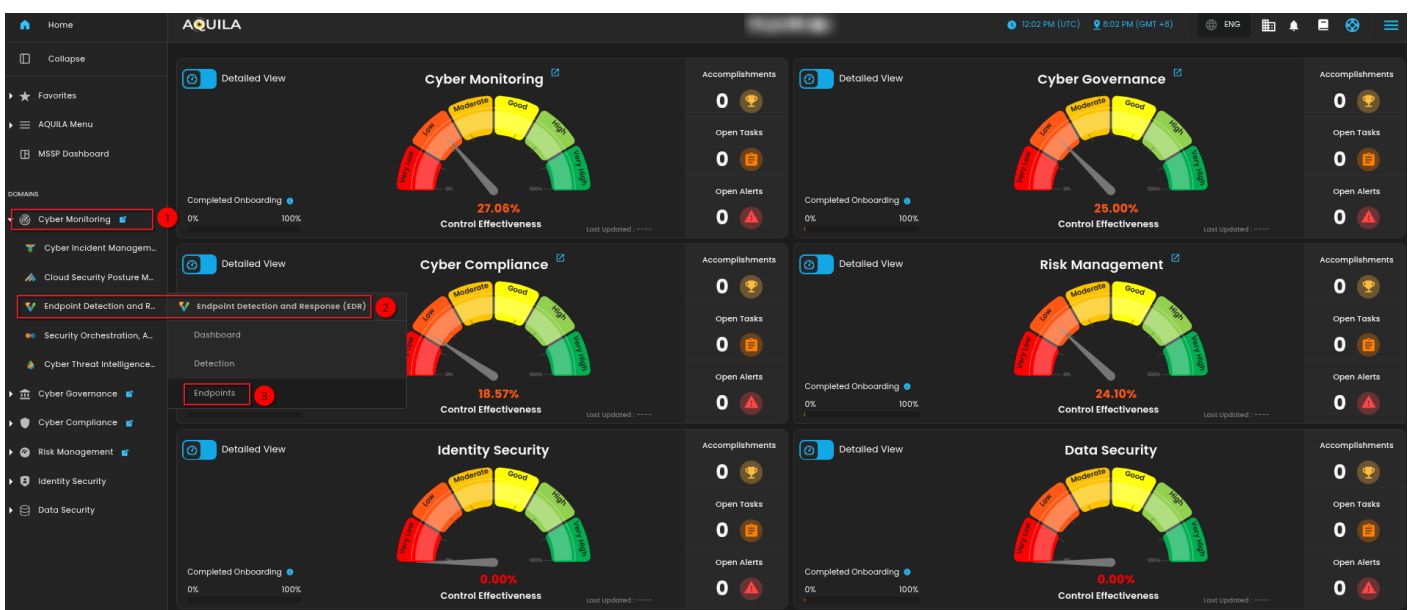
- Only users assigned the "**Owner**" or "**Admin**" role can access the Log Collector installation resources within the platform.

## 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](https://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.

The screenshot shows the 'Endpoints' dashboard with three main sections: 'Endpoint Security State', 'Endpoint Health', and 'Endpoint OS Type'. The 'Security State' section shows 0 Secured, 3 Infected, and 0 Isolated endpoints. The 'Health' section shows 3 endpoints, with a legend for Online (green), Unhealthy (orange), and Offline (grey). The 'OS Type' section lists various operating systems like Windows, Ubuntu, CentOS, etc. Below these is a search bar and a table of endpoints. A red arrow points to a blue '+ Install Endpoint' button in the top right corner.

Endpoint	Security Status	IP Address	Mac Address	Version	Health	Last Seen	Date Installed	
	Infected			8.18.2	Offline	56 Minutes Ago	July 22, 2025	👁
	Infected			8.18.2	Offline	5 Days Ago	July 17, 2025	👁
	Infected			8.18.2	Inactive	Jun 18, 2025	June 18, 2025	👁

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

The screenshot shows a 'Requirements' dialog box for Windows. It includes a title bar with a close button, a subtitle 'Make sure you have these things ready to have a smooth installation process of log collector.', and tabs for 'Windows', 'Linux', and 'Mac'. The 'Ready To Install?' section contains a note about folder navigation and a list of requirements: 'You have a stable Internet Connection.', 'Admin Privileges.', and 'Access to Command Prompt and PowerShell'. A red box highlights a small icon in the PowerShell requirement. At the bottom, there is a 'Back' button, a '1 / 4' indicator, and a 'Next' button, with a red arrow pointing to the 'Next' button.

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

## Options

Select your installation method for your log collectors.



### Automatic

The Log Collector will automatically download.



### Manual

You'll be given instructions for the manual installation of Log Collector.

← Back

2 / 4



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.**

## Options » Manual Installation


Select Operating System for your Endpoint, Detection and Response Log Collector.

Windows

Linux

Mac

### Install an Endpoint Log Collector Manually

To effectively Install an Endpoint Log Collector Manually, Copy or click the  logo and paste the command line on your Microsoft PowerShell. You must complete and **Complete each item on the checklist below in order. Click the checkbox for each item once completed** before proceeding to the next step.

**Note:** If you're going to install an Endpoint Log Collector Manually in your device, make sure to run the PowerShell 'as administrator'

#### Step: 1 Sets the PowerShell variable \*

Sets the PowerShell variable \$ProgressPreference to 'SilentlyContinue' suppressing progress output during script execution.

```
Set-PSDebug -Continue; $ProgressPreference = 'SilentlyContinue'
```

← Back

3 / 4

Next

**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.**

```
(tech01@tech-support)-[~ -8.18.1-linux-x86_64] Before you can proceed to the final installation set-up Found
will be installed at /opt/ and will run as a service. Do you want to continue?
[Y/n]:y
[= ] Service Started [2s] successfully installed, starting enrollment.
[= ] Waiting For Enroll... [2s] {"log.level":"warn","@timestamp":"2025-07-22T20:24:33.062+0800","log.l
ogger":"tls","log.origin":{"function":"github.com/ /transport/tlscommon.(*TLSCon
fig).ToConfig","file.name":"tlscommon/tls_config.go","file.line":107},"message":"SSL/TLS verifications di
sabled.","ecs.version":"1.6.0"}
[= ] Waiting For Enroll... [3s] {"log.level":"info","@timestamp":"2025-07-22T20:24:33.806+0800","log.o
rigin":{"function":"github.com/ /internal/pkg/agent/cmd.(*enrollCmd).enrollWithBackof
f","file.name":"cmd/enroll_cmd.go","file.line":532},"message":"Starting enrollment to URL: https://517dc8
848c734d909691ba9bd4f6feb4.fleet.us-east-1.aws.found.io:443/","ecs.version":"1.6.0"}
[ ] Waiting For Enroll... [3s] {"log.level":"warn","@timestamp":"2025-07-22T20:24:34.024+0800","log.l
ogger":"tls","log.origin":{"function":"github. -libs/transport/tlscommon.(*TLSCon
fig).ToConfig","file.name":"tlscommon/tls_config.go","file.line":107},"message":"SSL/TLS verifications di
sabled.","ecs.version":"1.6.0"}
[ =] Waiting For Enroll... [4s] {"log.level":"info","@timestamp":"2025-07-22T20:24:35.700+0800","log.o
rigin":{"function":"github.com/ /internal/pkg/agent/cmd.(*enrollCmd).daemonReloadWith
Backoff","file.name":"cmd/enroll_cmd.go","file.line":495},"message":"Restarting agent daemon, attempt 0",
"ecs.version":"1.6.0"}
{"log.level":"info","@timestamp":"2025-07-22T20:24:35.701+0800","log.origin":{"function":"github.com/
/internal/pkg/agent/cmd.(*enrollCmd).Execute","file.name":"cmd/enroll_cmd.go","file.line
":313},"message":"Successfully triggered restart on running .","ecs.version":"1.6.0"}
Successfully enrolled the
[ =] Done [4s]
has been successfully installed.
```

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

# Options » Manual Installation

Select Operating System for your Endpoint, Detection and Response Log Collector.

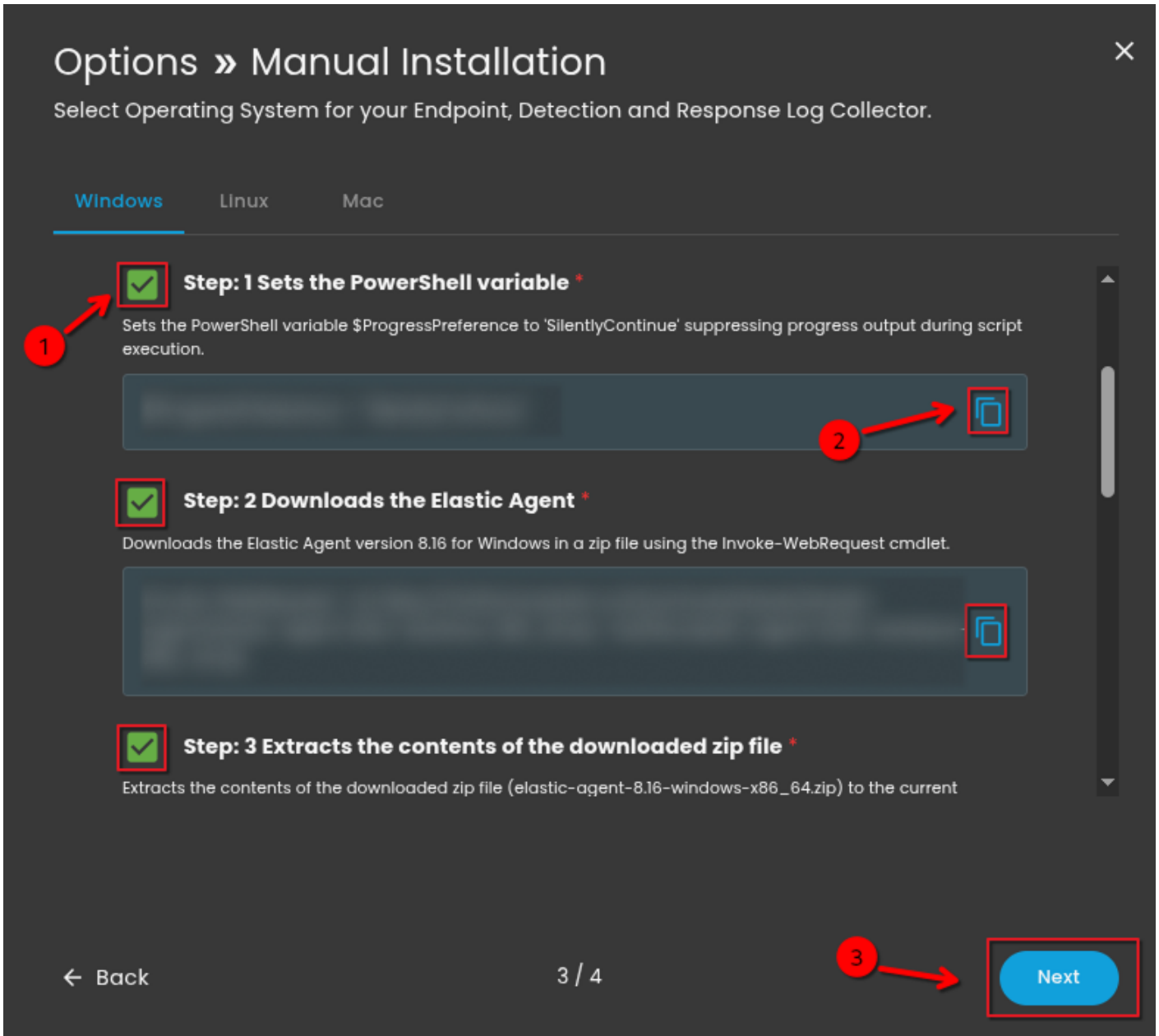
Windows Linux Mac

**Step 1 Sets the PowerShell variable \***  
Sets the PowerShell variable \$ProgressPreference to 'SilentlyContinue' suppressing progress output during script execution.

**Step 2 Downloads the Elastic Agent \***  
Downloads the Elastic Agent version 8.16 for Windows in a zip file using the Invoke-WebRequest cmdlet.

**Step 3 Extracts the contents of the downloaded zip file \***  
Extracts the contents of the downloaded zip file (elastic-agent-8.16-windows-x86\_64.zip) to the current

← Back 3 / 4 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.



## Setting up your service

Great start! Now, please wait 2–3 minutes while we get everything ready for you.



### Did you know?

In Aquila's CIM, you can create playbooks that guide you through effective case investigations.

← Back

4 / 4

Continue

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

# Awesome! You're almost there.



By clicking "Continue" you will be redirected to the Settings page to install your Log Sources.



Log Collector Setup Complete

## Details

☰ Log Collector

tech-support

⚠ Enable

Enabled

👤 Setup by

📘 "Tip: Add your log Sources"

Press **Continue** to start collecting logs by adding your first log source integration. You can choose from our wide range of supported platforms and services.

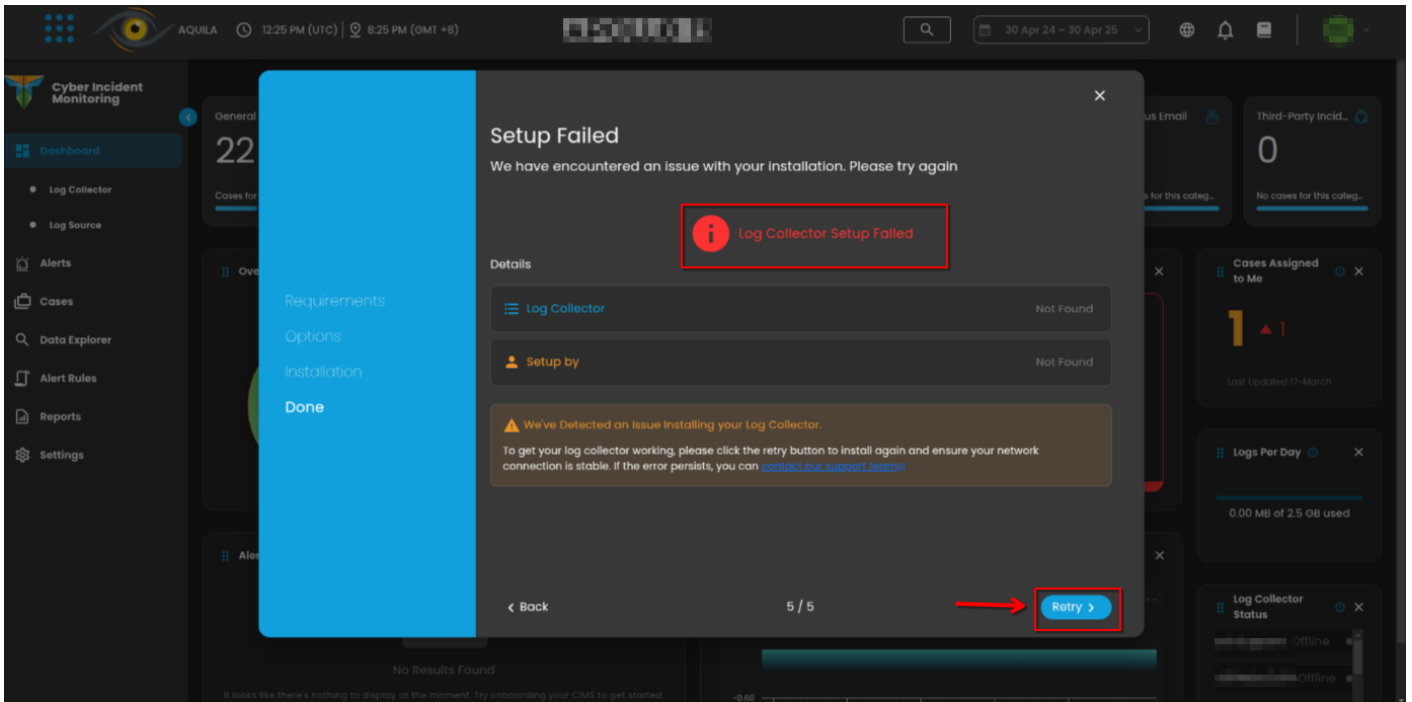
← Back

4 / 4

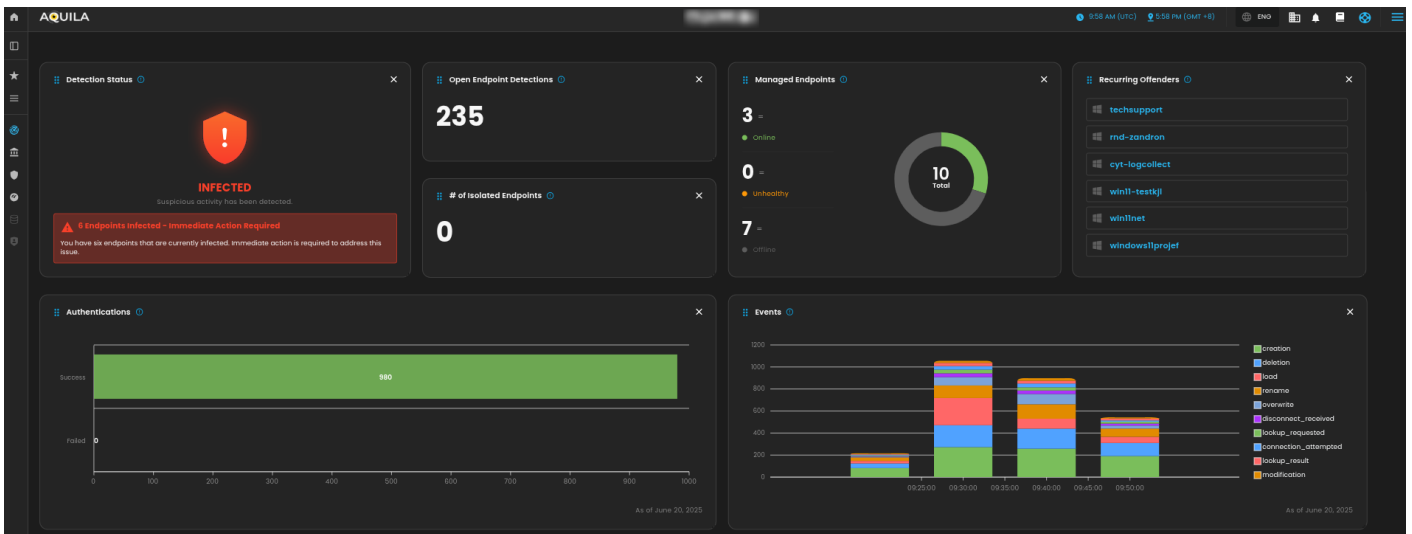


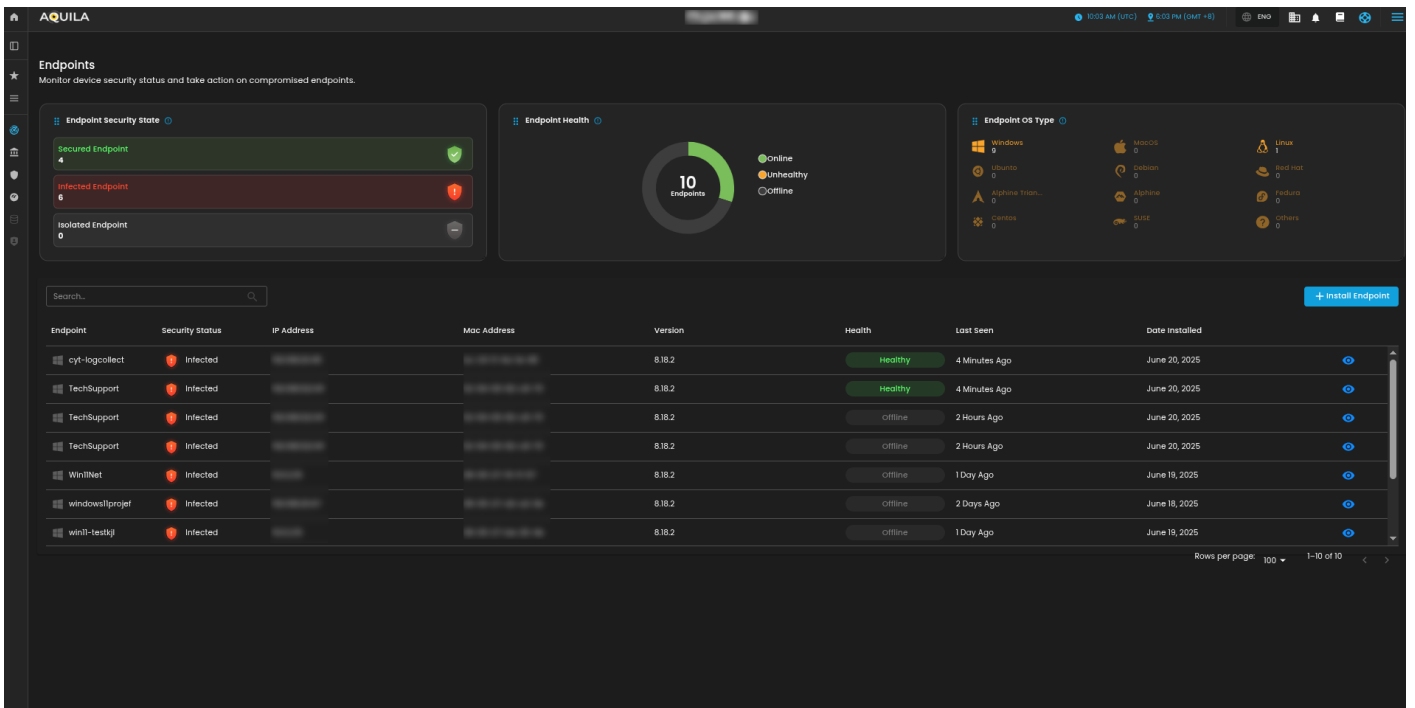
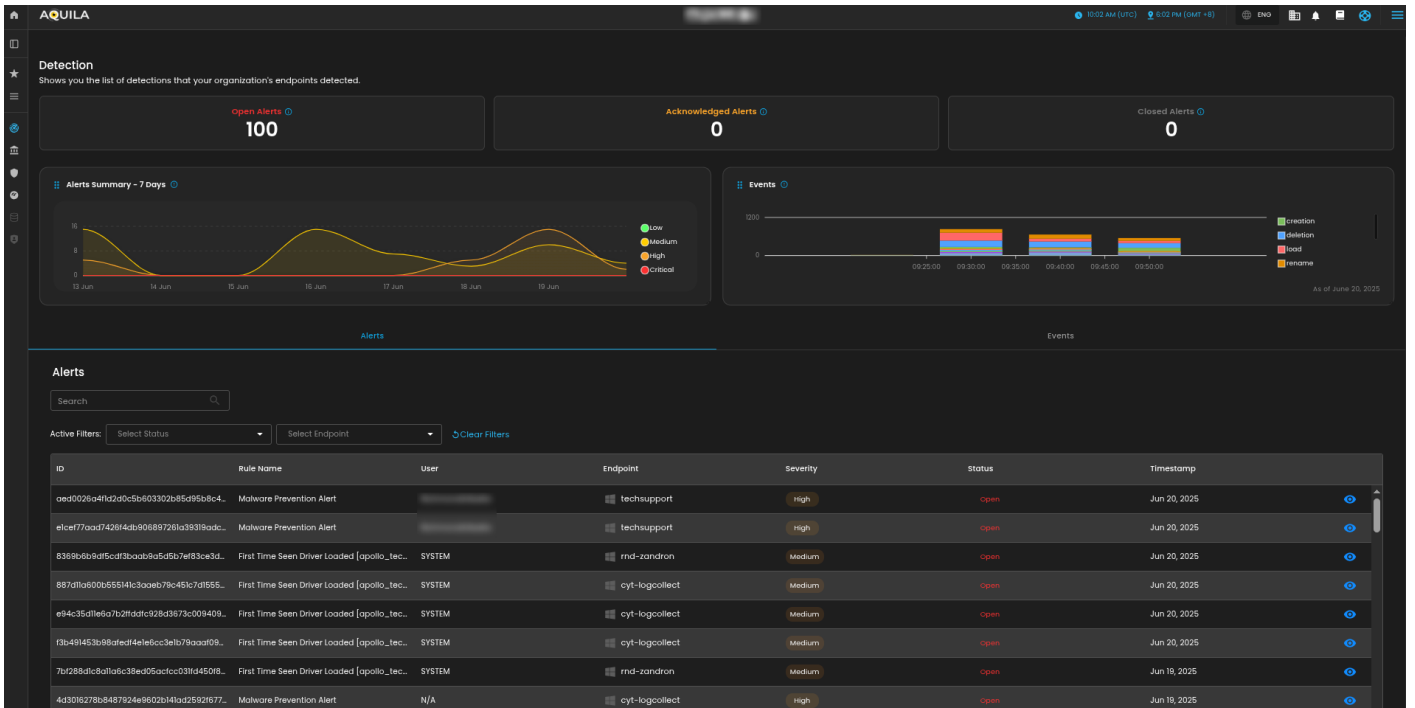
Continue

\*\*\*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](mailto: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](mailto: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