4. Malware Reports

Malware Reports track the output of antivirus or anti-malware scans on servers. Common tools include:

- **ClamAV** (open-source antivirus)
- **Rootkit** detection scripts

Use Cases

1. **Detecting Server Malware:** A CLAMAV scan detects malware in email attachments. Security isolates the files and marks the report as "In progress" for further analysis.
2. **Rootkit Detection:** A ROOTKIT scan finds hidden malicious processes. Engineers remove the infected files and mark the report as "Resolved".
3. **Scheduled Security Checks:** Weekly malware scans report no issues. Security logs the "Found = false" status and archives the report.
4. **Emergency Malware Response:** Malware is detected during a live incident. The security team performs an immediate investigation, quarantines infected files, and completes a system clean-up.

Table View

Total: (top-left) shows how many reports are in your system.

Filter launches a sidebar to narrow your list by:
Scan type (e.g. CLAMAV, ROOTKIT)
State (Not processed • In progress • Resolved)
Project
Search finds any term in server names or descriptions.
+ Add (top-right) opens the “Add malware report” form.

Columns

	Column Name ⇅	What It Shows
☑	(checkbox)	Select individual rows for bulk actions.
1	**Server name**	Hostname or IP address scanned.
2	**Project**	Link to the project/environment.
3	**Scan type ⇅**	Which tool ran (CLAMAV, ROOTKIT, etc.).
4	**Vulnerabilities ⇅**	“Detected” or “Not found” based on scan.

	Column Name ⇅	What It Shows
5	**Created at ⇅**	When the report was first logged.
6	**Updated at ⇅**	When any field was last changed.
7	**State ⇅**	Processing status (Not processed, etc.).
8	**Actions**	• ✏ Edit • ◫ Delete

> Security engineers then mark the report as “In progress” to investigate or “Resolved” if no further action is needed.

Adding a Malware Report

1. Click **+ Add**.

2. In the “Add malware report” form:
Server name: Enter the machine’s name or IP.
Scan type: Choose from your configured tools (ROOTKIT, CLAMAV, etc.).
Project: Link it to the correct project.
State: Select “Not processed,” “In progress,” or “Resolved.”
Malware found: Check this box if the scan flagged any threats (it’ll show “Detected” under Vulnerabilities).
Description: Summarize any details or remediation steps.

3. Click **Save**. The new row appears in the table.

Editing Reports

Edit: Click the ✏ icon in the Actions column to open the side-panel. You can change **Server name**, **Scan type**, **State**, **Malware found**, or update the **Description**. Then hit **Save**.

> If action is required, they set the State to “Processed” or “Not Processed.”

Filtering Malware Reports

To narrow down the list of malware reports, use the **Filter** panel available at the top of the Malware Reports table.
To open filters, click **Filter** in the upper-left corner of the table. A sidebar will appear with the following options:

State
Filter reports by their processing status:

1. Not processed

2. In progress
3. Resolved

This helps track which reports still require investigation versus those already handled.

Scan type
Limit results to reports generated by a specific malware detection tool, such as:

1. CLAMAV
2. ROOTKIT

Vulnerabilities
Use these checkboxes to control whether reports with or without detected threats are shown:

1. Show issues with detected vulnerabilities
2. Show issues without detected vulnerabilities

This is useful for quickly isolating confirmed incidents or reviewing clean scan results.

After selecting the required parameters, click **Save** to apply the filters.
To change the filter set, reopen the panel and adjust the selected values.

Revision #10
Created 27 February 2025 09:20:23
Updated 27 January 2026 12:04:06