



Day 3

ZROC102

Module 2: Case Management











LETSDEFEND Platform

The screenshot displays the LETSDEFEND Platform interface. On the left is a dark sidebar with navigation links: Homepage, Tutorial, Training (marked 'new'), Monitoring, Log Management, and Case Management (highlighted with a red box). The main area is titled 'Case List' and features a search bar labeled 'Search Here...'. Below the search bar is a table of cases. The first two rows are highlighted with a red box. The first row shows 'EventID: 94 - [SOC147 - SSH Scan Activity]' with a timestamp of 'Dec. 13, 2021, 10:57 a.m.' and a yellow warning icon. The second row shows 'EventID: 90 - [SOC143 - Password Stealer Detected]' with a timestamp of 'Dec. 1, 2021, 2:24 p.m.' and a yellow warning icon. To the left of the table, there are filter buttons: 'All' (highlighted in teal with a count of 2), 'Open' (with a count of 2), and 'Closed'.

Case List	
EventID: 94 - [SOC147 - SSH Scan Activity]	Dec. 13, 2021, 10:57 a.m.
EventID: 90 - [SOC143 - Password Stealer Detected]	Dec. 1, 2021, 2:24 p.m.

Case Management

This is the Case Mgt. Section that displays all cases that you created due to how suspicious the alert details were. Each case has their Event ID's.

<div> Case List</div> <div><div> All 2</div><div> Open 2</div><div> Closed</div></div>	Search Here...	
		EventID: 94 - [SOC147 - SSH Scan Activity] Dec. 13, 2021, 10:57 a.m. 
		EventID: 90 - [SOC143 - Password Stealer Detected] Dec. 1, 2021, 2:24 p.m. 

Case Management

This is the Case Mgt. Section that displays all cases that you created due to how suspicious the alert details were. Each case has their Event ID's. You can start playbook.

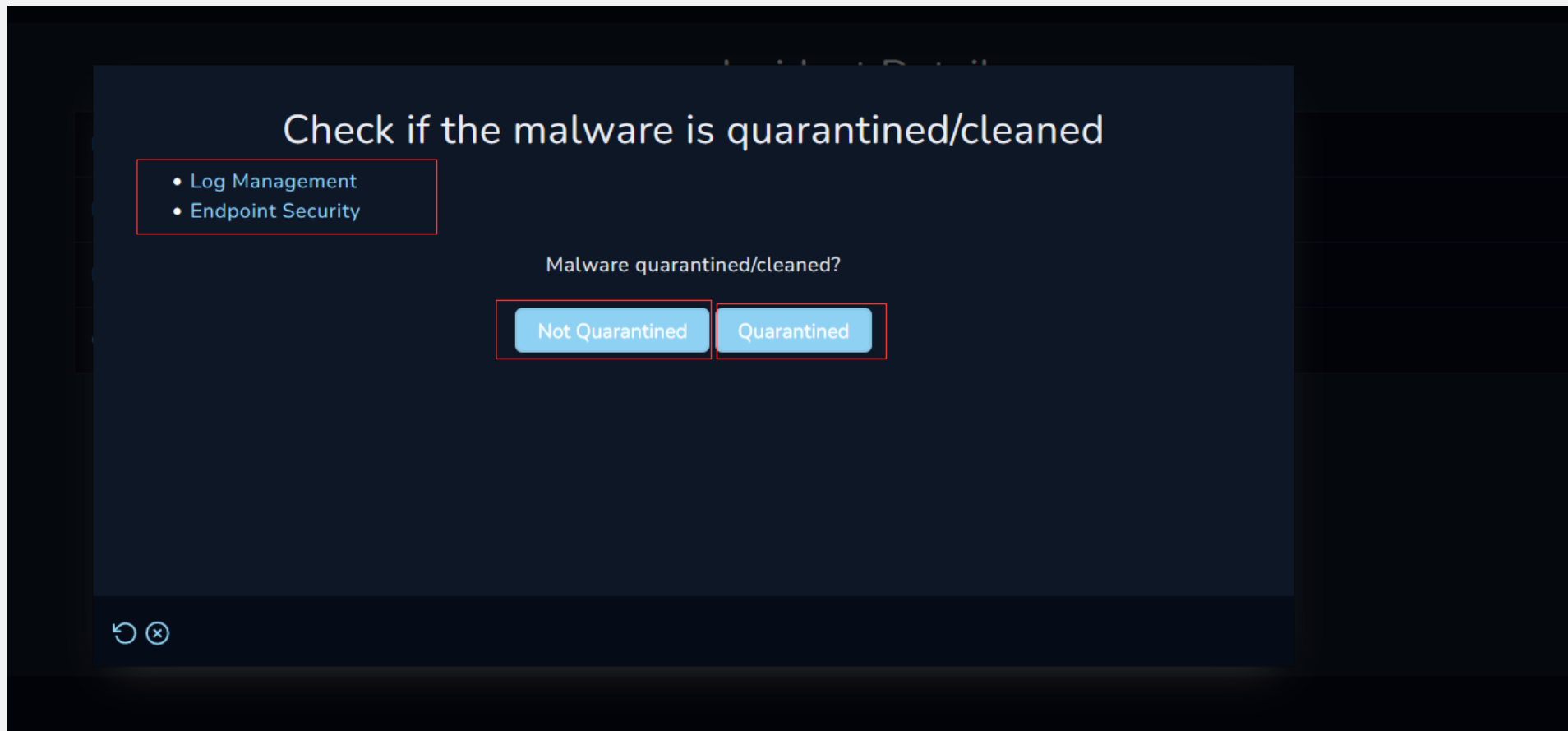
Incident Details

Incident Name:	EventID: 94 - [SOC147 - SSH Scan Activity]
Description:	AlertID: 94 + User: tigr3ss
Incident Type:	Malware
Created Date:	Dec. 13, 2021, 10:57 a.m.

Start Playbook!

Case Management

Letsdefend provides a playbook to help you understand which actions should be taken in the correct order. If fields in the playbook are not filled, the case will not be closed.



The screenshot shows a dark-themed interface for a playbook step. The title 'Check if the malware is quarantined/cleaned' is centered at the top. Below the title, on the left, is a list of prerequisites: 'Log Management' and 'Endpoint Security', each preceded by a blue dot. To the right of this list is a text label 'Malware quarantined/cleaned?'. Below this label are two light blue buttons: 'Not Quarantined' and 'Quarantined'. At the bottom left of the interface, there are two small circular icons: a refresh symbol and a close symbol (an 'x' inside a circle).

Check if the malware is quarantined/cleaned

- Log Management
- Endpoint Security

Malware quarantined/cleaned?

Not Quarantined Quarantined

Case Management

When the playbook is completed. The case will be indicated as “**closed**” in the Case list tab.

Results can be viewed in the “**Closed Alerts**” tab, via the Monitoring menu page.

Source

- <https://app.letsdefend.io/casemanagement/case/>
- <https://app.letsdefend.io/tutorial/videos/>