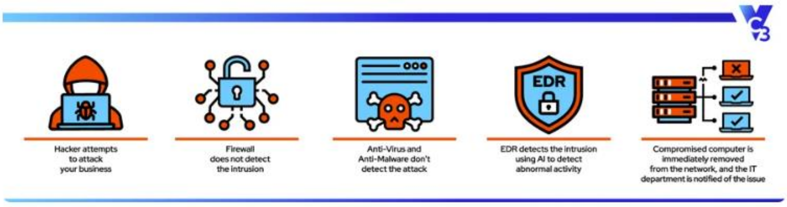
Endpoint Security Monitoring with Xcitium EDR on Linux

In today's cybersecurity landscape, endpoints such as laptops, servers, and virtual machines are frequent targets of malware, ransomware, and unauthorized access attempts. Traditional antivirus solutions are often insufficient to detect advanced persistent threats (APTs), fileless malware, and sophisticated attack techniques. To address this challenge, Endpoint Detection and Response (EDR) solutions are deployed to provide continuous monitoring, threat detection, and incident response capabilities on endpoints.


Hacker attempts to attack your business
Firewall does not detect the intrusion
Anti-Virus and Anti-Malware don't detect the attack
EDR
EDR detects the intrusion using AI to detect abnormal activity
Compromised computer is immediately removed from the network, and the IT department is notified of the issue

This project focuses on the installation, configuration, and testing of Xcitium OpenEDR, a free and open-source endpoint security platform. The tool is deployed on a Linux virtual machine, and its detection capabilities are validated using safe malware test files (EICAR).

What is EDR?

Endpoint Detection and Response (EDR) is a security technology designed to:

- Continuously monitor endpoint activities (processes, file access, network connections).
- Detect malicious behaviors and threats in real-time.
- Provide security teams with alerts, forensic data, and automated response actions such as isolating a device, quarantining files, or blocking malicious processes.
- Assist in incident investigation and remediation.

Unlike traditional antivirus software, EDR tools focus not only on prevention but also on detection and response, making them a crucial part of modern defense-in-depth strategies.

What is Xcitium (OpenEDR)?

Xcitium (formerly Comodo) OpenEDR is an endpoint protection and EDR platform that:

- Provides Next-Gen Antivirus (NGAV) and EDR capabilities in a single lightweight agent.
- Works across Windows, Linux, and macOS systems.
- Offers real-time monitoring, malware detection, forensic analysis, and automated response actions.

- Supports central management through the Xcitium ITSM/Endpoint Manager portal.
- Provides a Zero Trust Architecture: unrecognized files are executed in a secure container until verified safe.

Why it is used?

- To secure endpoints against malware, ransomware, and advanced threats.
- To provide visibility into endpoint activity and telemetry for incident response.
- To support compliance and audit requirements.
- To improve SOC (Security Operations Center) efficiency by automating detection and response.

Project Objective

The main objectives of this project are:

1. To install and configure Xcitium OpenEDR agent on a Linux endpoint.
2. To enroll the device into the Xcitium ITSM (cloud management console).
3. To generate safe test threats (using EICAR test files) on the endpoint.
4. To monitor how the EDR detects, quarantines, and responds to the simulated threats.
5. To analyze alerts and logs for better understanding of endpoint behavior.
6. To document the end-to-end process of endpoint protection using Xcitium OpenEDR.

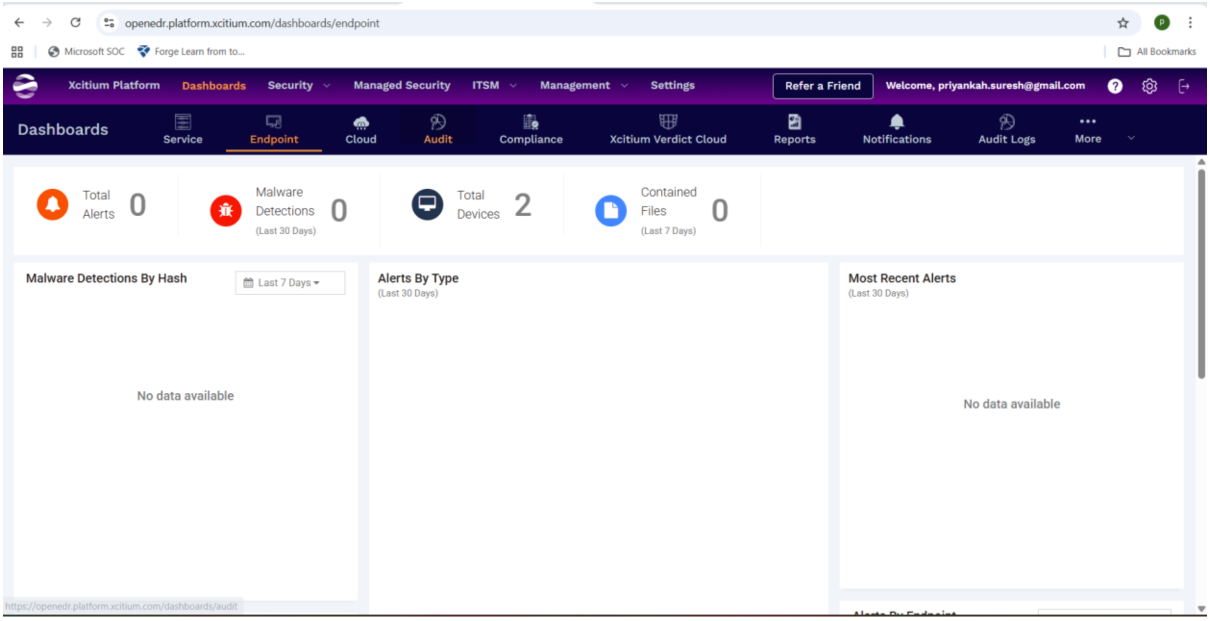
Tools Used

- Xcitium Endpoint Agent
    - Installed on the Linux machine to provide endpoint monitoring and protection.
    - Installed via terminal commands:
        1. sudo chmod 777 itsm
        2. sudo ./itsm
- Xcitium ITSM / Endpoint Manager
    - Centralized cloud portal for enrolling endpoints and managing alerts.
    - Provides features like blocked threats view, quarantined threats view, and policy management.
- Linux Command Line Utilities
    - chmod, wget, curl, zip, unzip → for installation and test file preparation.
- EICAR Test Files

    - Safe test files to simulate malware.
    - Used to validate that the EDR detects, blocks, and quarantines threats.

Lab Setup

- Host Machine (Lab PC)
    - Windows/Linux system with VirtualBox/VMware for virtualization.
- Virtual Machine (Target Endpoint)
    - OS: Linux (Ubuntu 20.04 / CentOS).
    - Role: Endpoint device with Xcitium EDR agent installed.
- Xcitium ITSM (Endpoint Manager Console)
    - Cloud-based console used for device enrollment, monitoring, and managing security incidents.
- Test Files
    - EICAR Standard Test File (safe malware simulation).
    - Packaged in .zip format to generate detection events.



Step by Step Procedure:

Step 1: Download the Xcitium EDR installer

- Sign in to the Xcitium Console with your account.
- Go to Devices → Enrollment / Installers.
- Select Linux as the target operating system.

- Copy the unique enrollment link:
- https://priyankahsureshgmailcom.itsm-us1.comodo.com:443/enroll/device/by/token/3ec9a200bb14f1f0fd92d555e43b9231
- Download the installer script (itsm) to your system.

Step 2: Install the agent on Ubuntu machine

- Move the downloaded installer to the Ubuntu VM.
- Run the following commands:
- sudo chmod +x itsm
- sudo ./itsm
- The script connects to the Xcitium servers using the enrollment link and automatically registers the endpoint.

Step 3: Verify enrollment in console

- Open the Xcitium console.
- Go to Devices.
- Your Ubuntu machine appears as Online / Enrolled.

Step 4: Download EICAR test malware files

- On Ubuntu, download safe EICAR test files in .zip format:
- wget https://secure.eicar.org/eicar_com.zip -O eicar_com.zip
- wget https://secure.eicar.org/eicarcom2.zip -O eicarcom2.zip
- These are harmless test files used only for security product validation.

Step 5: Scan with Comodo Scan (local scan)

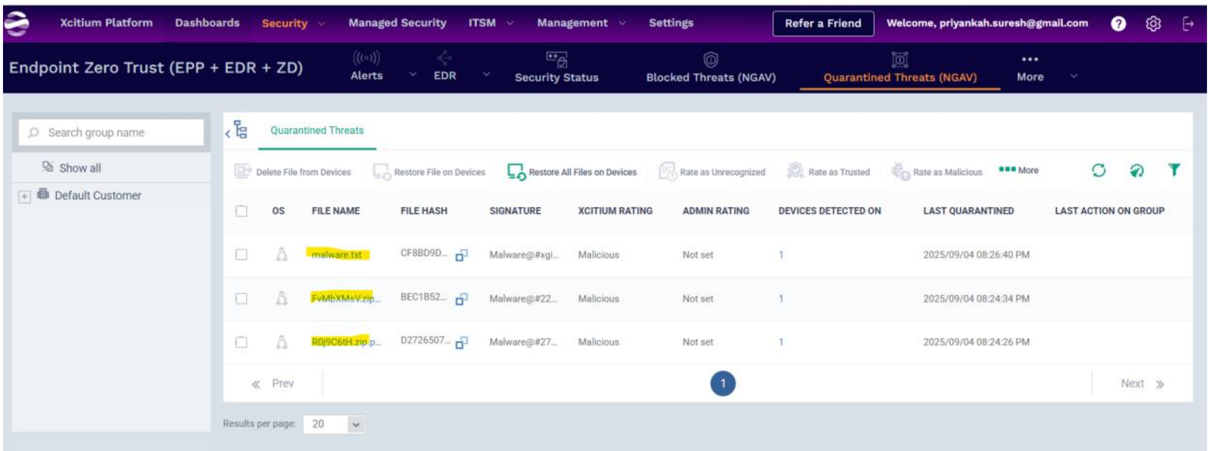
- Run the Comodo/Xcitium scanner on Ubuntu.
- The scan identifies the EICAR .zip files as malicious.

Step 6: Monitor detection in OpenEDR

- In the Xcitium console, go to Security → Blocked Threats (NGAV).
- Details shown:
  - File name (e.g., eicar.zip)
  - Device name (Ubuntu VM)
  - Detection type (Malware / Test file)
  - Action (Blocked)

Step 7: Quarantine the threats

- From the Blocked Threats view, choose Quarantine File on Device.
- The files are moved to a secure quarantine location by OpenEDR.
- Now go to Security → Quarantined Threats (NGAV).
- Confirm that the EICAR test files appear there.
- Options available:
  - Delete permanently
  - Restore to device (not recommended, only for false positives)

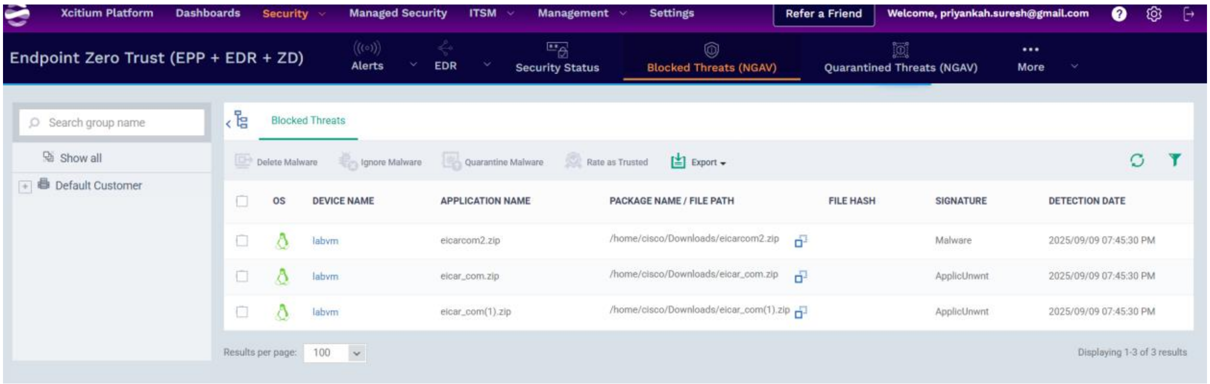


□	OS	FILE NAME	FILE HASH	SIGNATURE	XCITIUM RATING	ADMIN RATING	DEVICES DETECTED ON	LAST QUARANTINED	LAST ACTION ON GROUP
□		malware.txt	CF8BD9D...	Malware@#xgi...	Malicious	Not set	1	2025/09/04 08:26:40 PM	
□		FvMbXMsV.zip...	BEC1B52...	Malware@#22...	Malicious	Not set	1	2025/09/04 08:24:34 PM	
□		R0j9C6tH.zip p...	D2726507...	Malware@#27...	Malicious	Not set	1	2025/09/04 08:24:26 PM	

This section lists files that have not only been blocked but also moved to a quarantine location where they can no longer harm the system.

- File Name: The threats found (malware.txt, FakeMalware.zip, R0Y0SHS.zip).
- File Hash: Cryptographic hash of each file for unique identification.
- Signature: Shows the detection category, here marked as Malware@... → malicious files.
- Xcitium Rating: Marked as Malicious (automatic classification).
- Admin Rating: Not set (admins can override/confirm).
- Devices Detected On: Number of endpoints where the file was found.
- Last Quarantined: Date and time when the file was moved to quarantine.

Meaning: These files were not just blocked — they were isolated in a secure quarantine so they cannot interact with the system unless an admin restores or deletes them.



□	OS	DEVICE NAME	APPLICATION NAME	PACKAGE NAME / FILE PATH	FILE HASH	SIGNATURE	DETECTION DATE
□		labvm	eicarcom2.zip	/home/cisco/Downloads/eicarcom2.zip		Malware	2025/09/09 07:45:30 PM
□		labvm	eicar_com.zip	/home/cisco/Downloads/eicar_com.zip		ApplicUnwnt	2025/09/09 07:45:30 PM
□		labvm	eicar_com(1).zip	/home/cisco/Downloads/eicar_com(1).zip		ApplicUnwnt	2025/09/09 07:45:30 PM

Results per page: 100

Displaying 1-3 of 3 results

This section lists all threats that the EDR has detected and immediately blocked, preventing them from executing.

- Device Name (labvm): The endpoint (Ubuntu VM) where the files were detected.
- Application Name: The malicious/test files (eicarcom2.zip, eicar.com.zip, eicar_com(1).zip).
- File Path: Shows the exact location on the endpoint (/home/cisco/Downloads/...).
- File Hash: Unique identifier for the file to confirm its integrity.
- Signature: The type of detection – e.g.,
  - Malware → flagged as malicious
  - ApplicUnwant → application identified as unwanted/harmful.
- Detection Date: Timestamp when the detection occurred.

Meaning: The EDR successfully stopped these EICAR test files from running on your Linux VM and logged them here.

Step 8: Confirm final response

- The EICAR test files are blocked, quarantined, and logged.
- OpenEDR shows full details of detection, device, and action taken.

Project Summary

In this project, Xcitium OpenEDR was installed and deployed on an Ubuntu machine using the enrollment link provided by the Xcitium console. The endpoint was successfully registered and monitored through the management dashboard. To test detection capabilities, EICAR test malware files were downloaded on the Ubuntu machine. The EDR agent identified these files during scanning, blocked their execution, and moved them into quarantine for secure isolation.

This demonstrated the full functionality of Xcitium EDR — from agent deployment, threat detection, and blocking to quarantining malicious files — ensuring endpoint security and visibility through the centralized console.

Author Details

Name: Priyanka H S
Project Title: Endpoint Security Monitoring with Xcitium EDR on Linux