Use Case: Handle Malware Infection

Primary Actor

- **Security Analyst** – Member of the Incident Response Team responsible for handling the infection.

Supporting System Actor

- **MIRS Platform** – Provides detection, analysis, automation, and incident tracking capabilities.

1. Preconditions

1. The Security Analyst is successfully authenticated and authorized to access the MIRS platform.
2. A malware alert or suspicious activity has already been detected by automated monitoring tools.
3. The MIRS platform is fully operational, including:
    - Log collection services,
    - Threat detection modules,
    - Network isolation and containment features,
    - Incident management interface.

2. Main Success Scenario

1. Security Analyst receives malware infection alert.

The MIRS platform generates a real-time alert based on threat indicators. The analyst is notified via dashboard, integrated SIEM alerts, or email.

2. Analyst reviews the incident details.

The analyst examines:

- Alert severity and category,
- Indicators of compromise (IoCs),
- List of affected hosts,
- Event logs,
- Previous similar incidents.

3. Analyst initiates investigation.

On selecting *Start Investigation*, the system assigns the case to the analyst and updates the incident state to **In-Progress**.

4. System retrieves relevant logs and evidence.

The MIRS platform automatically collects:

- Endpoint security logs,
- Network traffic data,
- File system activity,
- Memory snapshots,
- Registry and process data.
  All retrieved evidence is correlated and presented to the analyst.

5. Analyst isolates affected system.

The analyst issues a containment command such as *Isolate Host* or *Block Network Access*.
The MIRS platform coordinates with EDR, firewall, or network segmentation tools to prevent malware propagation.

6. Analyst performs containment and removal actions.

Available remediation actions include:

- Deleting malicious files,
- Terminating suspicious processes,
- Removing persistence mechanisms,
- Executing automated malware removal scripts.
  The system executes selected actions and logs outcomes.

7. Analyst verifies successful threat removal.

After remediation, the analyst runs additional scans.
If no malicious behavior is detected, the threat is validated as eliminated.

8. System updates the incident status to *Resolved*.

Upon confirmation, the MIRS platform marks the incident as **Resolved**, updating timelines, logs, and case metadata.

9. Analyst closes the incident report.

The analyst documents final notes, lessons learned, and remediation summaries.
The incident is archived for forensic and audit purposes.

3. Postconditions

1. Malware is fully contained or removed from the affected systems.
2. All investigation steps, actions, timestamps, and system responses are securely logged.
3. Affected machines are restored to normal operation with network access re-enabled.
4. The finalized incident report is stored in the incident history archive.
5. Threat intelligence data may be updated based on discovered indicators.

4. Special Requirements

Performance Requirements

- Alerts must be generated within seconds of detection.
- Log and evidence retrieval should occur with minimal delay.

Security Requirements

- All logs and evidence must be deposited into tamper-proof storage.
- Isolation and remediation actions require role-based authorization.

Functional Requirements

- Must support integration with SIEM, firewall, and EDR systems.
- Automation workflows must allow scripted response and containment actions.

Usability Requirements

- The user interface must clearly show incident severity, status, and progress.
- Analysts must be able to quickly access affected system details and actions.

5. Alternative Flows

3a. False Positive Detection

Trigger: Occurs during **Step 2** (Analyst reviews the incident details).

1. The Analyst examines the Indicators of Compromise (IoCs) and event logs.
2. The Analyst identifies the activity as a legitimate business process or authorized administrative action (e.g., IT department using a remote maintenance tool).
3. The Analyst flags the incident as **"False Positive"** within the MIRS platform.
4. The Analyst adds an exclusion or tuning note to the detection rule to prevent future alerts.
5. The System closes the incident; no isolation or removal actions are taken. **Postcondition:** System continues normal operation; the incident is archived as a False Positive.

5a. Isolation Failure

Trigger: Occurs during **Step 5** (Analyst isolates affected system).

1. The Analyst issues the "Isolate Host" command.
2. The MIRS platform fails to communicate with the endpoint agent or firewall (e.g., due to network outage or malware disabling the agent).
3. The System returns an **"Isolation Failed"** error message.
4. The Analyst initiates out-of-band communication (phone/ticket) to the Network Engineering team or on-site IT support for manual intervention.
5. *Alternative:* The Analyst attempts a more aggressive network block via the MIRS platform, such as a **Switch Port Shutdown**.
6. Once isolation is confirmed, the flow resumes at **Step 6**.

6a. Critical Asset Exception (Business Continuity)

Trigger: Occurs before or during **Step 5**.

1. The Analyst identifies the affected system as a **Critical Asset** (e.g., Production Database, Live Patient Support Unit).
2. Determining that full isolation would cause unacceptable business disruption, the Analyst **holds** the isolation command.
3. The Analyst initiates the Business Continuity Plan (BCP) or seeks Manager Approval for partial containment.
4. The System is used to only terminate specific malicious processes rather than blocking full network access.
5. **Step 6** (Containment/Removal) is executed with heightened caution.

7a. Remediation Failed / Persistence Detected

Trigger: Occurs during **Step 7** (Analyst verifies successful threat removal).

1. Upon rescanning after remediation, the MIRS platform detects continued malicious activity or "beaconing" (signaling to a command-and-control server).
2. The Analyst determines that standard remediation scripts are insufficient or the malware has rootkit-level persistence.
3. The Analyst escalates the incident severity to **High/Critical**.
4. The decision is made to physically remove the device from the network for **Re-imaging** or **Forensic Analysis**.
5. The flow branches to the "Device Replacement / Re-imaging Procedure."

2b. Automated Remediation (Zero-Touch)

Trigger: Occurs after **Step 1**, before Analyst intervention.

1. The MIRS platform identifies the threat with **High Confidence** and classifies it as "Automatically Remediable."
2. The System executes isolation and removal playbooks immediately without waiting for Analyst approval.
3. The Analyst receives the notification, but the incident state is already marked as **"Resolved - Pending Verification."**
4. The Analyst reviews the automated action logs to confirm success.
5. The flow resumes at **Step 8**.