GRC103 Lab: Practical Risk Monitoring with Wazuh

Course: GRC103 - Risk Assessment and Management Techniques
Module: Practical Risk Assessment Workshop

Table of Contents

1. Lab Overview & GRC Learning Objectives

Welcome, GRC Analysts! This hands-on workshop bridges the gap between risk theory and practice. You will deploy a technical control (Wazuh) to actively monitor an IT asset for a specific risk, unauthorized file changes, demonstrating how technical tools feed into the risk management lifecycle.

By the end of this lab, you will be able to:

- **Operationalize** a risk treatment by deploying a **detective control**.
- **Identify** a specific IT risk (unauthorized file modification) and configure a tool to monitor for it.
- **Analyze** and **evaluate** security events based on risk severity and potential business impact.
- **Demonstrate** the process of risk monitoring and control effectiveness reporting using a central dashboard.
- **Articulate** the value of centralized monitoring for governance and compliance reporting.

2. Scenario: A Governance and Risk Mandate

You are a GRC analyst. A recent risk assessment identified the **unauthorized modification or deletion of sensitive financial forecast documents** as a medium-to-high risk to the organization. The Risk Treatment Plan approved the implementation of a **detective control** to monitor for this activity.

Your task is to implement a solution that can:

1. Continuously monitor a designated folder (C:\Users\<YourName>\SensitiveFiles) on a key user's workstation.
2. Detect and log any creation, modification, or deletion of files within that folder.
3. Provide a centralized audit trail and real-time alerting to demonstrate the control's operation for compliance and monitoring purposes.

You have selected the open-source Wazuh platform to fulfill this requirement.

3. Lab Architecture

Component	Host	GRC Role
Wazuh Manager	Ubuntu (VirtualBox)	The **Risk Monitoring Platform**. Aggregates and analyzes data for reporting.
Wazuh Agent	Windows (Host Machine)	The **Control Agent**. Installed on the asset (endpoint) being monitored.

Network Configuration:

- Set your Ubuntu VM's network adapter to **Bridged Adapter**. This places it on the same network as your host machine, allowing them to communicate.

4. Prerequisites

- VirtualBox installed.
- Ubuntu Server 20.04+ installed in VirtualBox (with bridged networking enabled).
- Internet access on the Ubuntu VM.
- Administrative access on your Windows host machine.

5. Part 1: Deploying the Wazuh Manager (Ubuntu)

Run the following steps on your Ubuntu VirtualBox server via a terminal window.

1. Add Wazuh GPG Key

bash

curl -s https://packages.wazuh.com/key/GPG-KEY-WAZUH | sudo gpg --dearmor -o /usr/share/keyrings/wazuh-archive-keyring.gpg

2. Download and Execute Installation Script

bash

curl -sO https://packages.wazuh.com/4.12/wazuh-install.sh && sudo bash ./wazuh-install.sh -a -i

- -a: Installs **all** components.
- -i: Runs in **interactive** mode (follow any on-screen prompts).

GRC Note: In a production environment, the separation of these components would be a key **compensating control** to mitigate the risk of a single point of failure.

Wazuh Management Commands

sudo systemctl restart wazuh-manager

sudo systemctl stop wazuh-manager

sudo systemctl start wazuh-manager

sudo systemctl status wazuh-manager

6. Part 2: Accessing the Wazuh Dashboard

1. Find your Ubuntu VM's IP address: ip addr show
2. Open a web browser and navigate to: https://<UBUNTU_VM_IP_ADDRESS>
3. **Accept the browser security warning.** (This is expected in a lab environment).
4. Log in using the credentials provided at the end of the installation script (default username is admin).

GRC Note: This dashboard serves as your **Risk & Control Monitoring Console**. It provides the evidence needed for compliance audits and ongoing risk assessments.

7. Part 3: Installing the Wazuh Agent (Windows)

1. On your **Windows host**, download the Wazuh Agent MSI installer: https://packages.wazuh.com/4.x/windows/wazuh-agent-4.12.0-1.msi
2. Run the MSI file and install it with the default settings.

8. Part 4: Agent-Manager Registration

1. Generate Agent Key on Manager
On your **Ubuntu VM terminal**, run:

bash

sudo /var/ossec/bin/manage_agents

- Press A to **Add an agent**.
- Enter a name (e.g., Finance-Dept-Workstation).
- For the IP address, you can leave it as any.
- Confirm and then press E to **Extract the key**.
- **Copy the generated key.**

2. Apply Key in the Windows Agent

1. On your **Windows host**, open the **Wazuh Agent Manager**.
2. Go to the **Management** tab.
3. Paste the key into the "Agent key" field.
4. In the "Manager address" field, enter the IP address of your **Ubuntu VM**.
5. Click **Apply** and then **Restart**.

Verification: Go to the Wazuh Dashboard > **Agents**. You should soon see your agent with a green **Active** status.

9. Part 5: Implementing a Detective Control (File Integrity Monitoring)

We will now configure the **detective control** to monitor for the identified risk.

1. Edit Agent Configuration

1. On your **Windows host**, navigate to C:\Program Files (x86)\ossec-agent\.
2. Open the ossec.conf file as Administrator.
3. Find the <syscheck> section.
4. Add the following line (replace abc with your Windows username):

xml

<directories realtime="yes">C:\Users\AMINU IDRIS\SensitiveFiles</directories>

2. Restart the Agent
Restart the Wazuh agent from the **Wazuh Agent Manager** GUI or via services.msc.

10. Part 6: Risk Monitoring & Control Verification

Now, you will verify that your control is operating effectively and generate risk-related events.

1. **Create the Monitored Folder:** Create C:\Users\abc\SensitiveFiles on your Windows machine.
2. **Simulate a Risk Event:** Perform these actions in the SensitiveFiles folder to simulate unauthorized activity:
   - ✓ Create a new file (Q4_Financial_Forecast.docx).
   - ✓ Modify the file by adding text.
   - ✓ Delete the file.
3. **Monitor Control Effectiveness in the Dashboard:**
   - ✓ Go to the Wazuh Dashboard.
   - ✓ Navigate to **Security Events**.

- ✓ Filter for rule.groups: "syscheck" to see only File Integrity Monitoring alerts.
- ✓ Click on alerts to see details: file path, action (added/modified/deleted), timestamp, and file checksums.

11. GRC Workshop & Analysis Questions

Answer the following questions in your lab report, connecting the technical exercise to GRC principles.

1. **Risk Identification & Analysis:** In the context of our scenario, the risk was "unauthorized modification of financial documents."
   - ✓ What is the potential **business impact** (e.g., financial, reputational, operational) if this risk were realized?
   - ✓ Based on the alerts you generated, how does this control help in **quantifying** the risk (e.g., frequency of events)?
2. **Control Evaluation & Treatment:** The implemented FIM is a **detective control**.
   - ✓ What would be a complementary **preventive control** for this same risk?
   - ✓ Explain a situation where the alert from this detective control would trigger a **corrective control** (a response action).
3. **Risk Monitoring & Reporting:**
   - ✓ If you had to report on the **operational effectiveness** of this FIM control to a manager, what three key metrics would you pull from the Wazuh dashboard?
   - ✓ How does centralizing this monitoring data, as opposed to checking logs on each individual computer, improve the **governance** and **auditability** of the risk management program?
4. **Compliance Mapping:** Many regulations (like SOX, PCI DSS, HIPAA) require monitoring critical files for changes.
   - ✓ How does a tool like Wazuh provide **evidence** for compliance audits?
   - ✓ Briefly describe how you would use the Wazuh dashboard to demonstrate to an auditor that a specific sensitive file has not been altered during a defined period (e.g., last quarter).