Lab #4 – End-Point Detection and Response (EDR) + Secure Information and Event Management (SIEM)

Outcomes

CIS Controls:
- CIS Control 5: Account Management
- CIS Control 7: Continuous Vulnerability Management
- CIS Control 8: Audit Log Management
- CIS Control 13: Network Monitoring and Defense
-

IT&C Learning Outcomes:
Secure Network Environments
Network Cyber Defense

Students will be able to:
- Gain experience using both an EDR and a SIEM tool to monitor end points
- Identify best practices in setup of EDR solutions
- Deploy an agent-based EDR and manipulate the environment to generate alerts
- Monitor a SIEM dashboard to identify potentially malicious activity

Background

Endpoint Detection and Response (EDR) is a cybersecurity technology focused on continuously monitoring and responding to threats on endpoint devices such as computers, mobile devices, and servers. EDR solutions collect and analyze data from these endpoints to detect suspicious activities, provide real-time threat detection, and enable rapid response to mitigate potential security incidents.

Security Information and Event Management (SIEM) tools, on the other hand, are designed to provide a centralized platform for collecting, aggregating, and analyzing security data from various sources across an organization's IT environment. SIEM solutions use advanced analytics and machine learning to detect anomalies and

potential security breaches, offering a comprehensive view of the organization's security posture.

It provides real-time monitoring, log management, and advanced analytics to detect and respond to potential security threats. A SIEM will centralize logs from firewalls, Intrusion Detection Systems (IDS), and other tools.

SIEMs play a crucial role in threat detection, incident response, and compliance enforcement. Security teams rely on SIEMs to detect and investigate security incidents quickly, minimizing potential damage from cyberattacks. EDR tools feed endpoint data into SIEM systems, enriching the SIEM's data pool with detailed endpoint activity logs. By combining the endpoint-specific insights from EDR with the broader network and application data in SIEM, organizations can achieve more accurate and comprehensive threat detection.

In this lab you will be using Wazuh, an open-source EDR and SIEM, to monitor a Windows and a Linux device, and explore some of the many features Wazuh has to offer. Wazuh agents act on the end devices to monitor them and it uses OpenSearch for log ingestion

Activity:
Install and configure Wazuh and use it to monitor the systems and files of a Windows 10 VM and a Kali Linux VM.

What You Will Need for This Lab:
- The Wazuh VM
- 2 Endpoint VMs
    - Kali Linux (or another distribution of Linux)
    - Windows 10 (or later)

1. Set Up Wazuh:

Wazuh provides a pre-built virtual machine image in OVA format. This VM only runs on 64-bit systems with x86_64/AMD64 architecture. If the OVA file does not work for you, please see the provided Docker Installation document with alternative instructions.

1. Visit https://documentation.wazuh.com/current/deployment-options/virtual-machine/virtual-machine.html
2. Download the `wazuh-4.10.X.ova` package
3. It is recommended that you install the VMs in NAT mode for their networking
4. The username and password are provided for you. NOTE: you may need to press ENTER for the sign-in prompt to appear.
   a. User: `wazuh-user`
   b. Pass: `wazuh`

5. Type `ip a` and take note of the IP Address.
6. On any local browser, access the Wazuh dashboard by using the following:
   a. URL: `https://<WazuhIpAddress>`
   b. User: `admin`
   c. Pass: `admin`

If you see "Wazuh dashboard server is not ready yet," refresh the page in a couple minutes and/or check your DNS settings.

2. Add Agents

Once you're logged in, you'll see the Wazuh dashboard. To effectively monitor a computer, Wazuh deploys "agents" on the end devices to enact policy and report back logs and alerts to the centralized dashboard (the SIEM). In this lab, you will deploy two agents to monitor. These are recommended to be Virtual Machines, and can include VMs used in previous labs. Alternatively, you may use your own device for the lab as an option.

2.1 Linux Agent

Boot up a Kali Linux VM and ensure it has network access. From the Wazuh dashboard, select "Deploy new agent." This can also be found by clicking the three bars in the top left and navigating to:

Agents Management > Summary
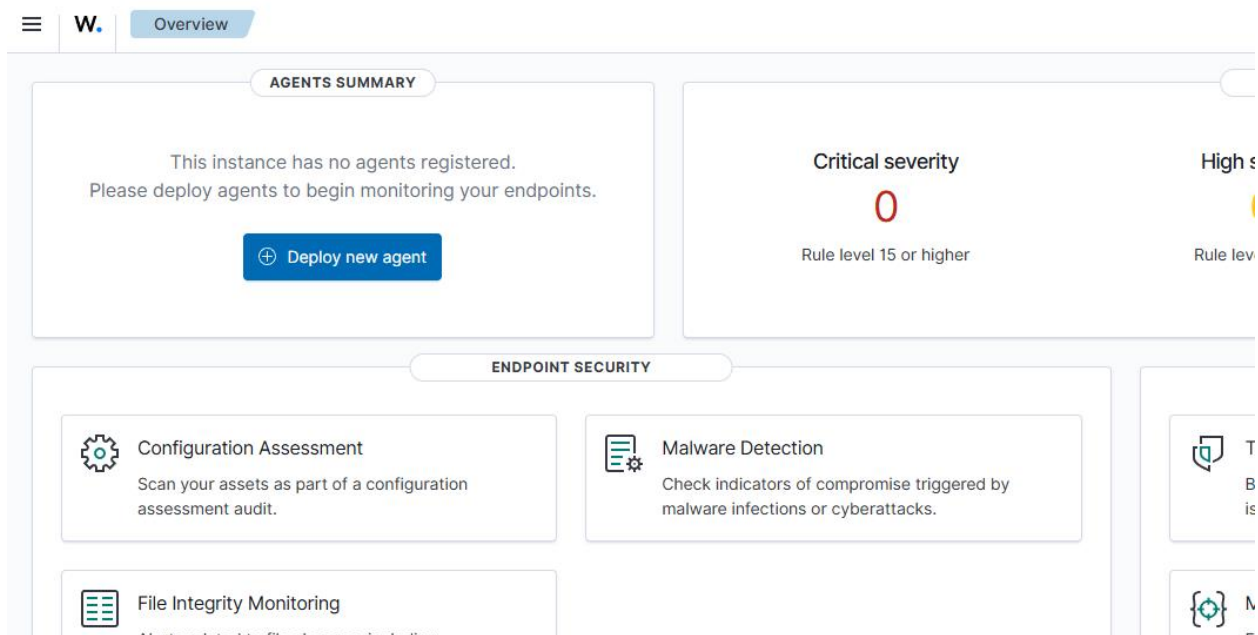
When you are presented with the package options select `Linux - DEB amd64`

For the FQDN, use the Wazuh IP Address (the same one you used to access the dashboard).

Deploy new agent

✓ **Select the package to download and install on your system:**

🐧 LINUX	⊞ WINDOWS	🍎 macOS
○ RPM amd64 ○ RPM aarch64	○ MSI 32/64 bits	○ Intel
● DEB amd64 ○ DEB aarch64		○ Apple silicon

ⓘ For additional systems and architectures, please check our documentation ☑.

✓ **Server address:**

This is the address the agent uses to communicate with the server. Enter an IP address or a fully qualified domain name (FDQN).

Assign a server address: ⓘ

```
192.168.86.82
```

✓ **Optional settings:**

Name it something you'll remember.

Put it in the default group.

Copy the agent download and install command that is generated. On your Kali Linux VM, open the terminal, and paste it in there.

Copy the systemctl commands at the bottom of the page and paste them in the Kali machine.

Navigate to the Agent Management page. Here you'll find information about your operating system and the new agent you've created.

2.2 Windows Agent

Click Deploy new agent and follow the same instructions to install an agent on a Windows machine. Make sure the VM is running and connected to the internet.

Select Windows - MSI 32/64 bits

Copy the agent download and install command. Launch a Windows VM (you can use the Domain Controller you used in the previous lab), run PowerShell as administrator, and paste the commands.
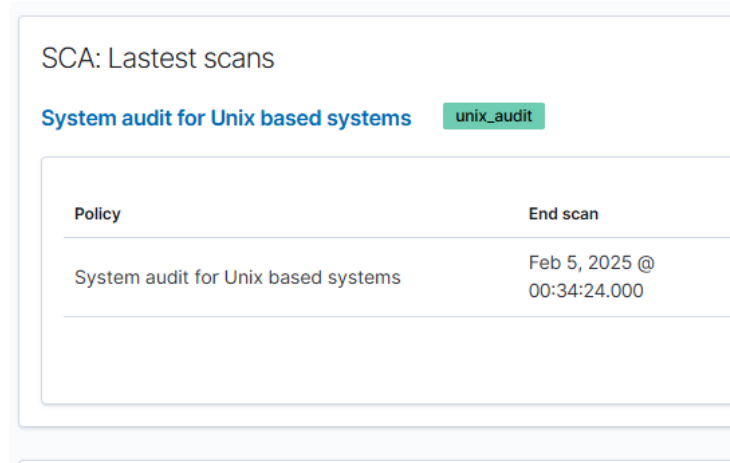
Return to the Agents Summary page and verify that both agents have been properly configured.

Now that you have installed Wazuh and agents on 2 clients, **go complete <u>Question 1</u>**, then proceed with the next section of the lab.

---

3. Security Operations

3.1 Security Control Assessment

Explore the dashboard of one of your agents. Of the useful widgets displayed, select the subcategory under "SCA: Latest Scans." For your Windows agent, this may be a CIS benchmark test. For Linux, this may be a System audit.

These are automatic checks Wazuh makes on the system to ensure the agent meets basic security requirements. It will give you a score for how many checks you Passed, Failed, and how many weren't applicable.

Go complete Question 2, then proceed with the next section of the lab.

3.2 Compliance

When you use the menu bars in the top left, Wazuh will automatically feed you data for the most recent agent you've selected for viewing. That means if you were just in the Kali agent dashboard and you navigate to Threat Intelligence > Vulnerability Detection, you will see at the top of the screen that Wazuh is displaying data for the Kali agent. You can change the agent by selecting the agent name (in the case of the screenshot below, that is "KaliVM") and then "Endpoints," which will appear where "Vulnerability De…" currently is. This will take you back to the Agent Summary screen.
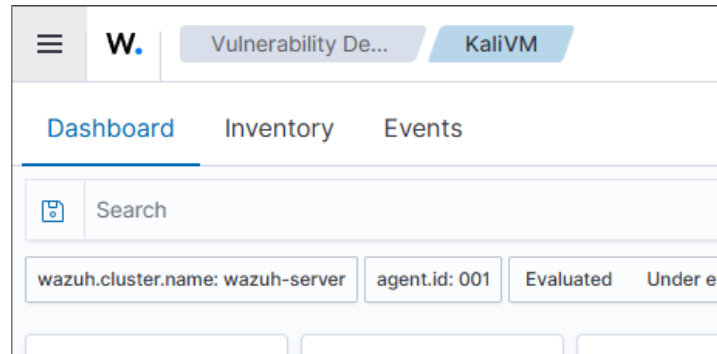
In the menu, expand "Security operations." There you will find 5 standards of compliance.

Go complete Question 3 and Question 4, then proceed with the next section of the lab.

---

4. Customize the Windows Agent

Navigate to the Windows 10 Agent dashboard > File Integrity Monitoring > Inventory
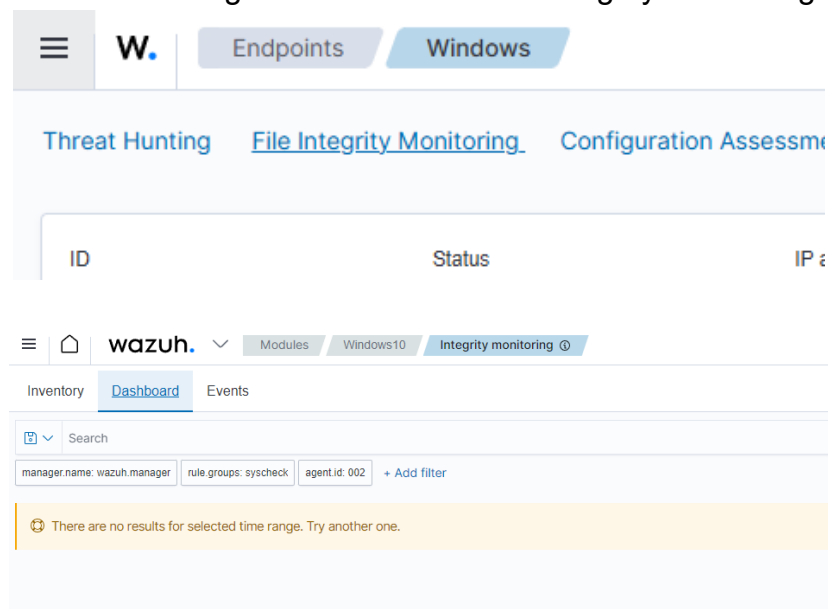
Wazuh has already scanned and inventoried all the default files it will look for and the windows registry keys. By default it will scan every twelve hours and alert you if anything changes. However, with files, we're going to set up real time notifications

4.1 File Integrity Monitoring

Open your Windows VM.

Open file explorer and navigate to `C:\Program Files(x86)\ossec-agent` (which you'll need admin access for)

Find `ossec.conf` and open it in a text editor (notepad is the default). This is the configuration file for your agent.

In that file, do a ctrl + f and search for `<syscheck>`
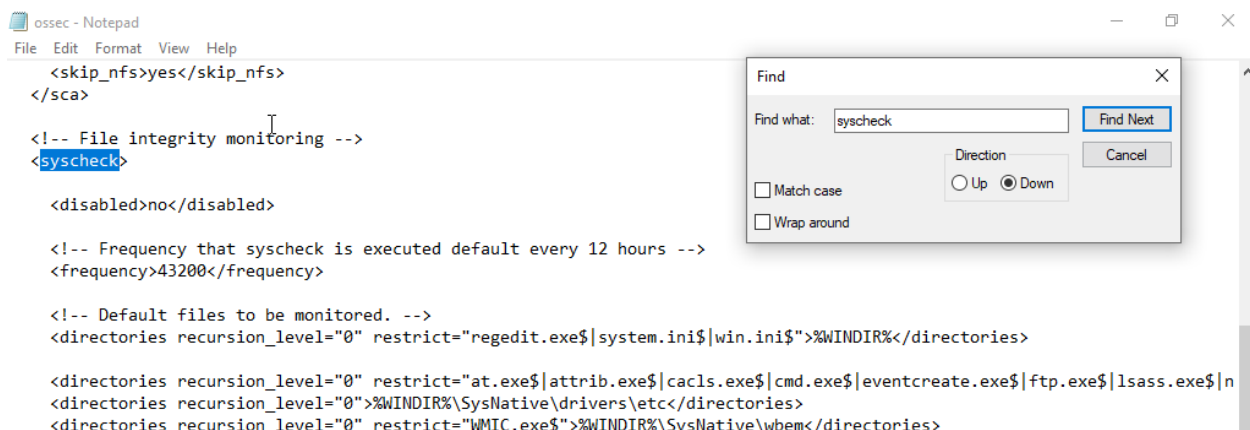
You can see several lines surrounded by `<directories>` tags. These are the directories that the system is currently configured to monitor.

Choose a place among the directories options and add the following configuration:

```
<directories realtime="yes" report_changes="yes"
check_all="yes">C:\Users\YourUsernameHere\Desktop</directories>
```

This enables real time alerts and will check and report any changes that are made to the files in your listed directory.

```
<!-- File integrity monitoring -->
<syscheck>

  <disabled>no</disabled>

  <!-- Frequency that syscheck is executed default every 12 hours -->
  <frequency>43200</frequency>

  <!-- Default files to be monitored. -->
  <directories recursion_level="0" restrict="regedit.exe$|system.ini$|win.ini$">%WINDIR%</directories>

  <directories recursion_level="0" restrict="at.exe$|attrib.exe$|cacls.exe$|cmd.exe$|eventcreate.exe$|ftp.exe$|lsass.exe$|n
  <directories recursion_level="0">%WINDIR%\SysNative\drivers\etc</directories>
  <directories recursion_level="0" restrict="WMIC.exe$">%WINDIR%\SysNative\wbem</directories>
  <directories recursion_level="0" restrict="powershell.exe$">%WINDIR%\SysNative\WindowsPowerShell\v1.0</directories>
  <directories recursion_level="0" restrict="winrm.vbs$">%WINDIR%\SysNative</directories>

  <!-- 32-bit programs. -->
  <directories recursion_level="0" restrict="at.exe$|attrib.exe$|cacls.exe$|cmd.exe$|eventcreate.exe$|ftp.exe$|lsass.exe$|n
  <directories recursion_level="0">%WINDIR%\System32\drivers\etc</directories>
  <directories recursion_level="0" restrict="WMIC.exe$">%WINDIR%\System32\wbem</directories>
  <directories recursion_level="0" restrict="powershell.exe$">%WINDIR%\System32\WindowsPowerShell\v1.0</directories>
  <directories recursion_level="0" restrict="winrm.vbs$">%WINDIR%\System32</directories>

  <directories realtime="yes" report_changes="yes" check_all="yes">C:\Users\Win10\Desktop</directories>

  <directories realtime="yes">%PROGRAMDATA%\Microsoft\Windows\Start Menu\Programs\Startup</directories>

  <ignore>%PROGRAMDATA%\Microsoft\Windows\Start Menu\Programs\Startup\desktop.ini</ignore>
```
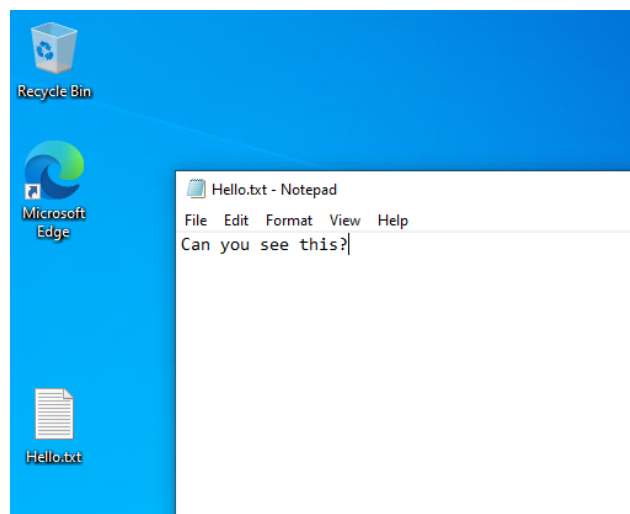
Save the file.

Open PowerShell as an administrator and enter the command:

```
restart-service -name wazuh
```

Look at the Wazuh dashboard again, notice that there are still no items.

On your Windows VM desktop, create a text file and put some something inside it.

Give Wazuh a few seconds to sync, then on the dashboard click refresh in the top-right. If everything is set up properly, you will see real time alerts on the dashboard.
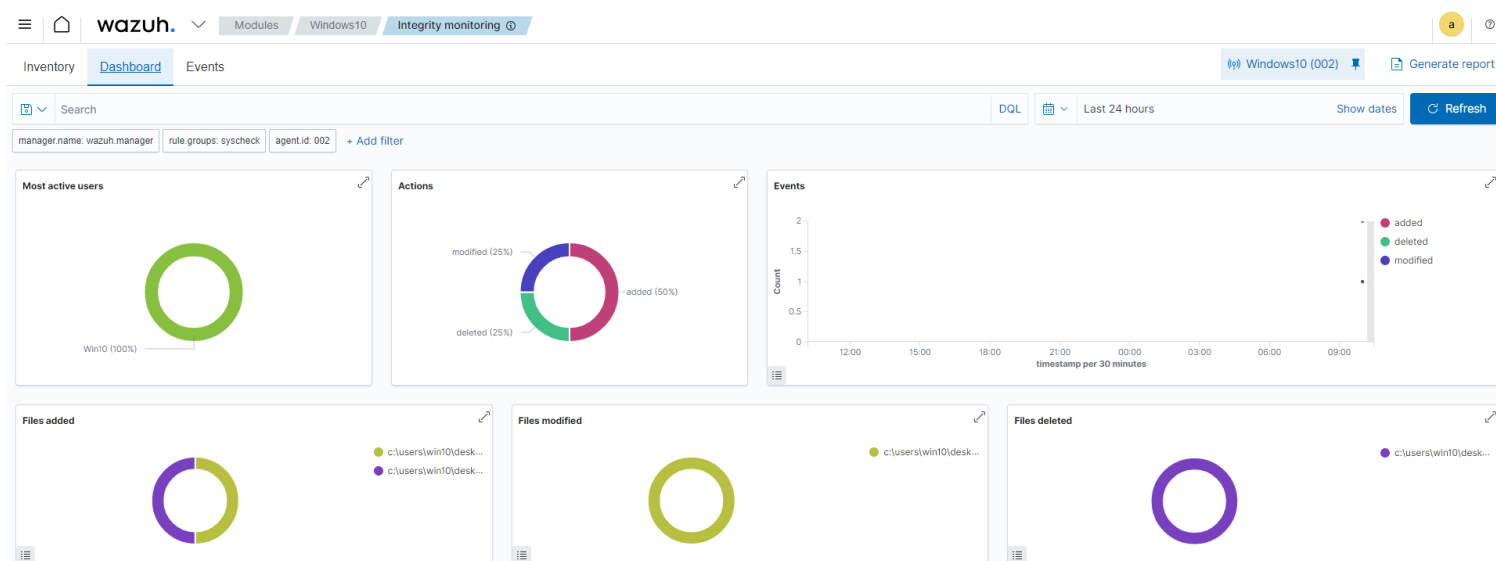
Yours may look different depending on what you did with your file, but you can see that on mine I have two file alerts: a file deletion, and a file modification. This aligns with creating a new file, renaming it (effectively deleting the old file and making a new one with the new name), and modifying its contents by adding text inside.

Click on events in the top left and let's see what went on with our Desktop directory. You should see a list of the events that it scanned, matching the actions you took
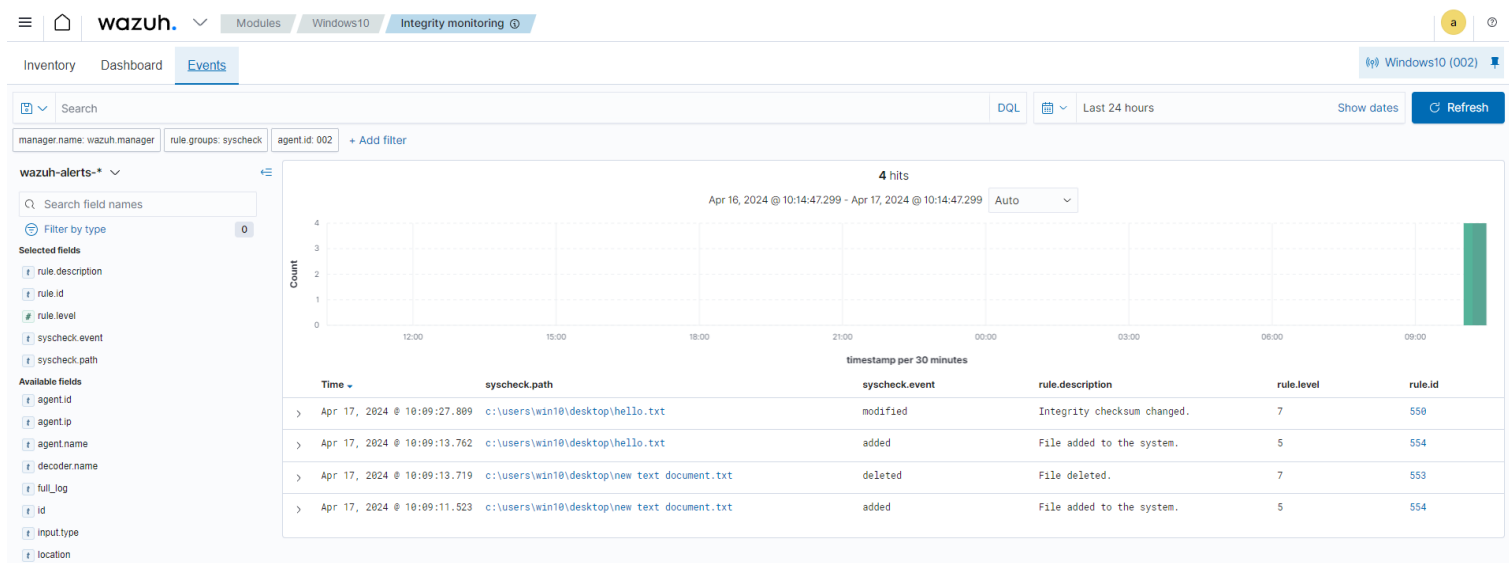
Go back to your Windows VM and change the text inside your .txt file. Save it and refresh the Wazuh Events page again. What changed? Expand the new alert and take

note of the `rule.description` of the rule that got triggered and the `syscheck.diff` that shows what changed.

Now you have your first integrity monitoring event, **go complete Question 5**, then proceed with the next section of the lab.

4.2 Windows Registry Monitoring

We can do the same kind of thing with the Windows Registry. Go back to the Inventory tab and navigate to the Windows Registry section with all the registry keys that Wazuh automatically monitors.

Let's add a custom key. Open the Registry Editor from the start menu on the Windows machine.

Expand the `HKEY_LOCAL_MACHINE/SOFTWARE` and right click on `Classes`. Select `New > Key` and name it `customkey`.
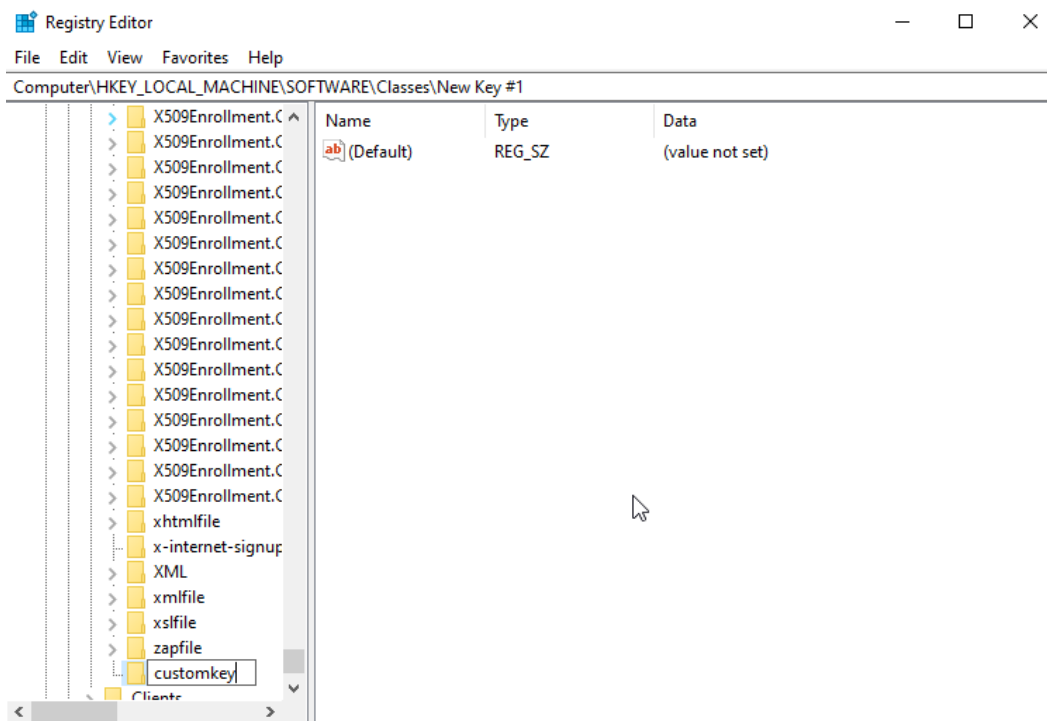
Right click on `(Default)` and change the value to something fun.
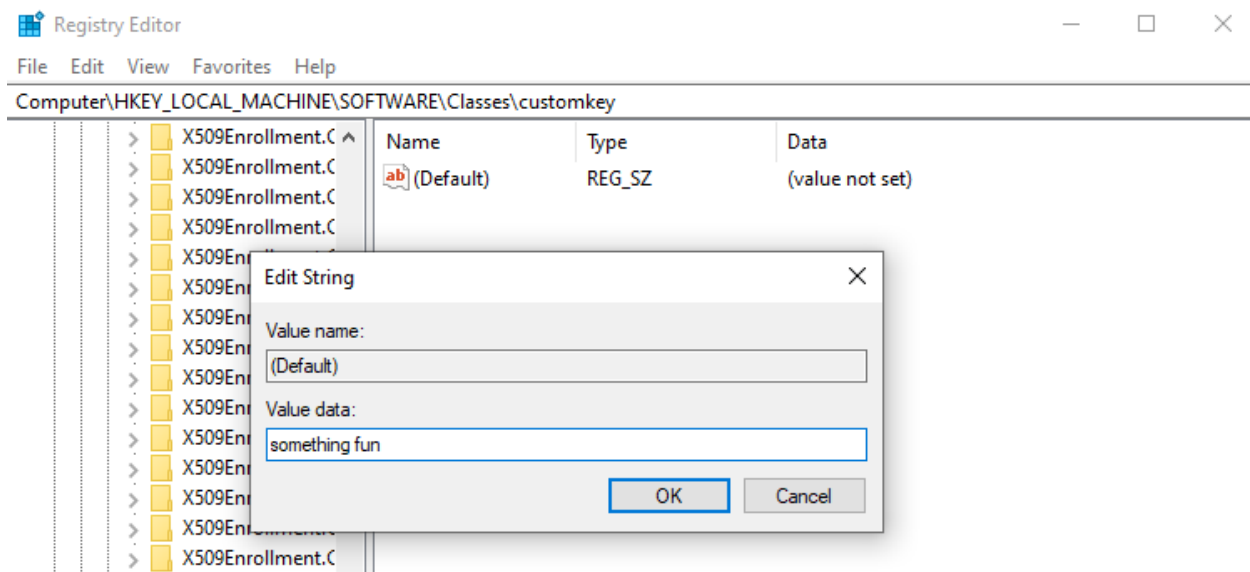
In the list of keys on the left, right click your custom key and select `Copy Key Name.`

Back in the `ossec.conf` file in 4.1, scroll down to the bottom of the list of registry keys. Before the section labeled 'Registry keys to ignore', add another line:

`<windows_registry>Paste\Your\Key\Location</windows_registry>`

We're also going to change the frequency that the registry keys get scanned – or else you'll be here for a long time. Scroll up in the `ossec.conf` file until you find a line with `<frequency>` tags. Change the value from 43200 (which is 12 hours in seconds) to 30, so it scans every half minute.

Save the file, then open PowerShell as an administrator again and restart your Wazuh service
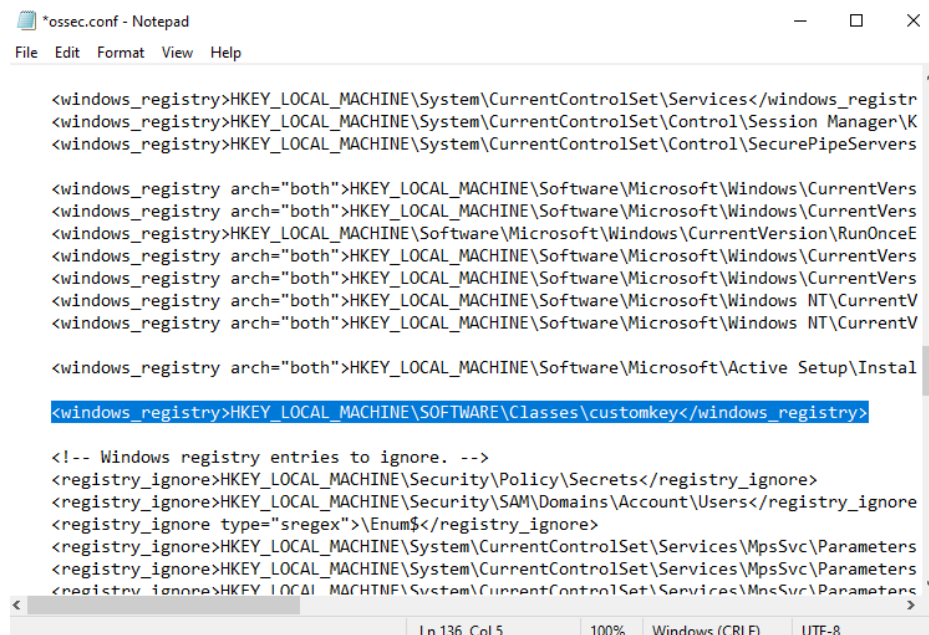
```
restart-service -name wazuh
```

Open the Wazuh dashboard again, make sure that you're on the Integrity monitoring module of your Windows VM. Go to the Inventory and look at the Windows Registry. There are thousands of default keys, so filter for your custom one. You may have to wait roughly thirty seconds for it to show up.

You've found the key! Now you know that Wazuh is looking at it and monitoring it.

Go complete Question 6 and then proceed with the rest of this section.

Let's go to events. You'll see some registry changes, which will come from our scans, but no events to do with your custom key yet. So, let's go make a change to the key.

Pull up the registry editor in the Windows VM again, and change the Value data to something else, click OK, then go monitor your Wazuh server dashboard. Again, this may take up to 30 seconds.
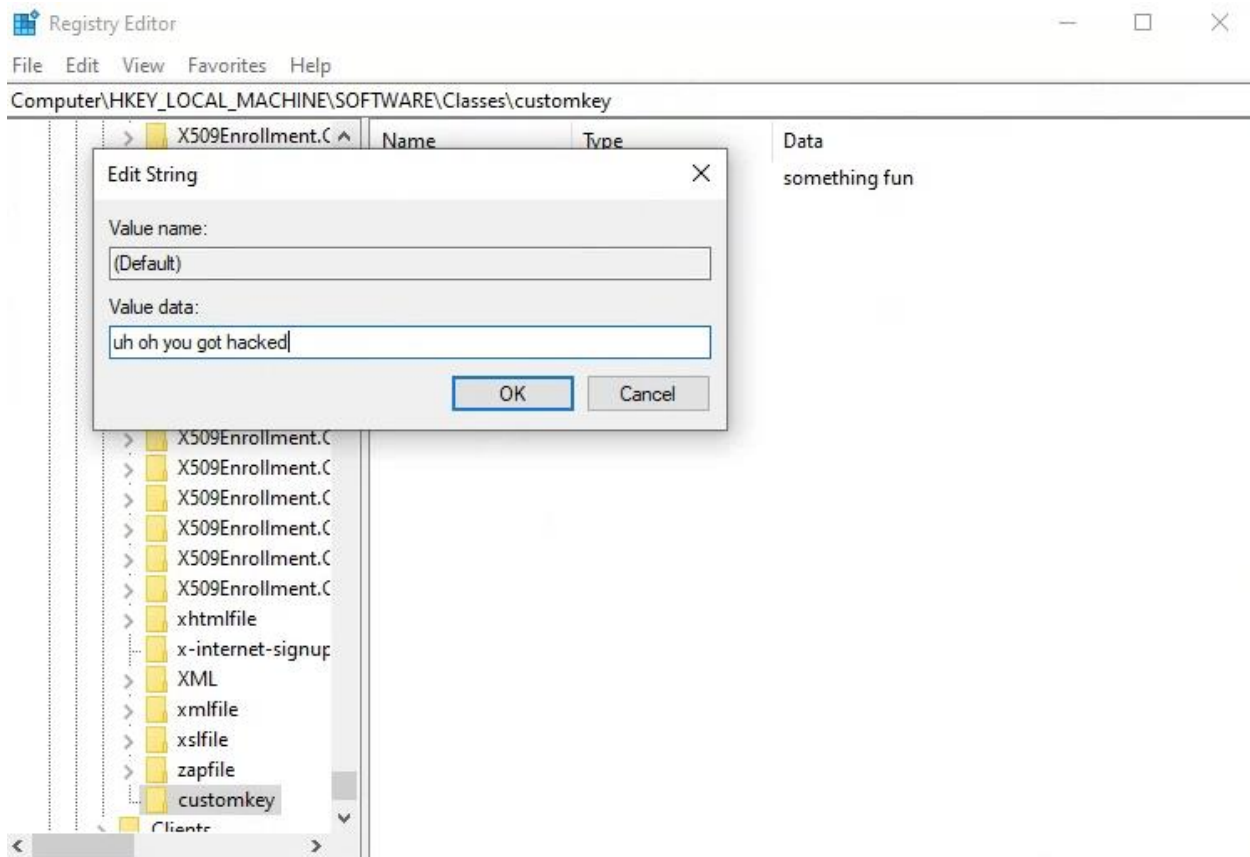
After it scans, you'll see your register key has been modified.
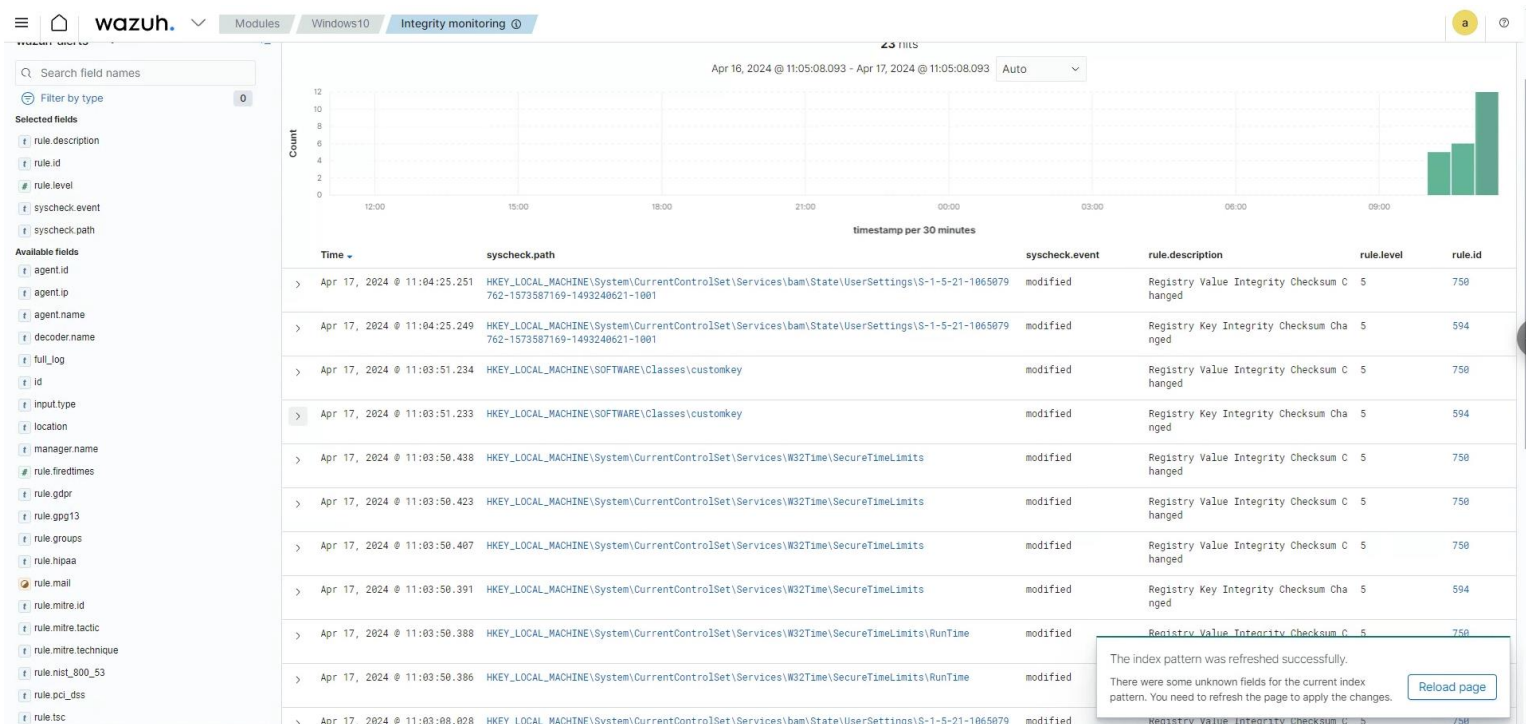
If you didn't already know, the Windows Registry is a database for storing all kinds of operating system and program-related settings. Often other windows tools (such as the Settings app) really are just friendly interfaces for modifying a registry key.

One common thing that might be changed from malware is in `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run`. This key controls which programs run on system startup, which an attacker can use to automatically run a malicious program behind the scenes. Let's simulate a malware attack here.

Open that file path in the registry editor and right click on the empty space on the right side of the screen. Select `new -> string_value`

Name it, and give it the location for Internet Explorer in the Value data field

`"C:\Program Files\Internet Explorer\iexplore.exe"`
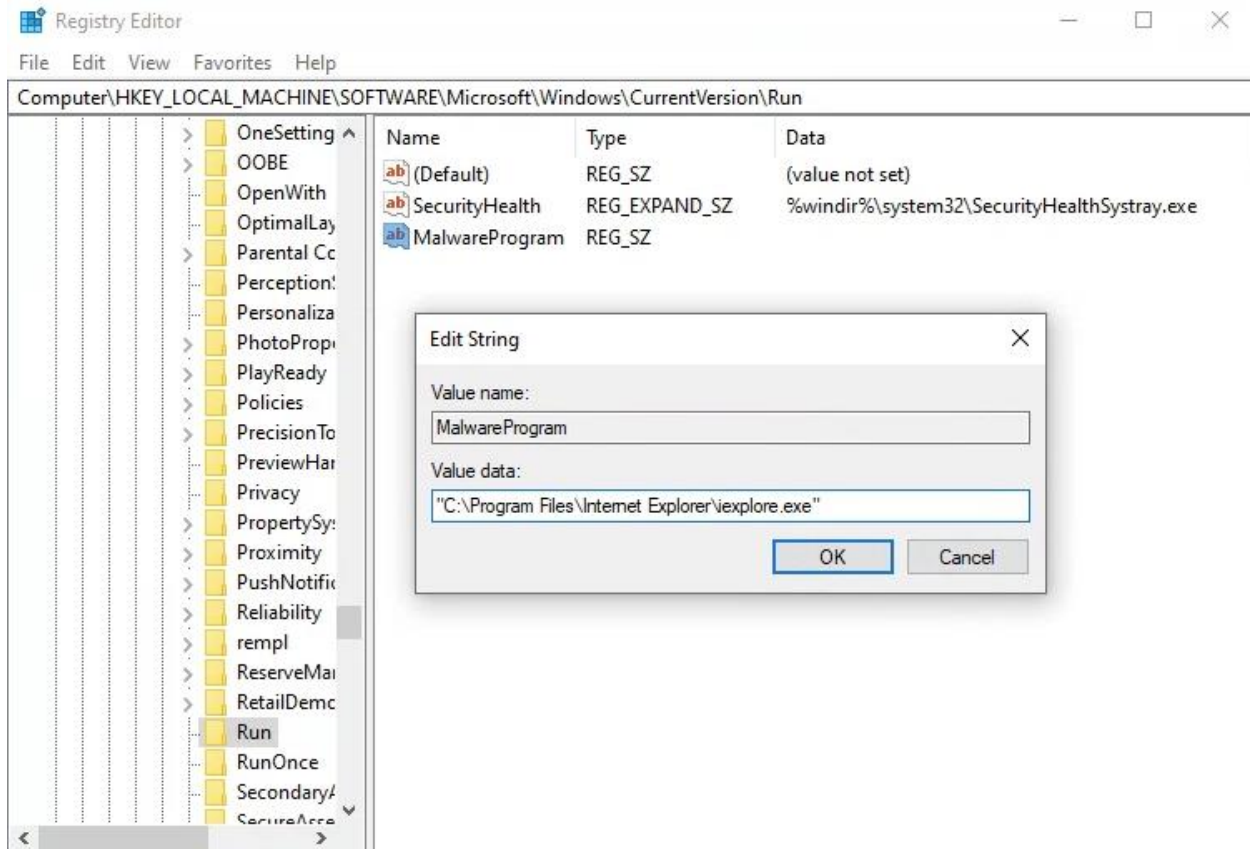
Refresh the Wazuh Events page, and since that directory is monitored by default, you should see that a registry key was added
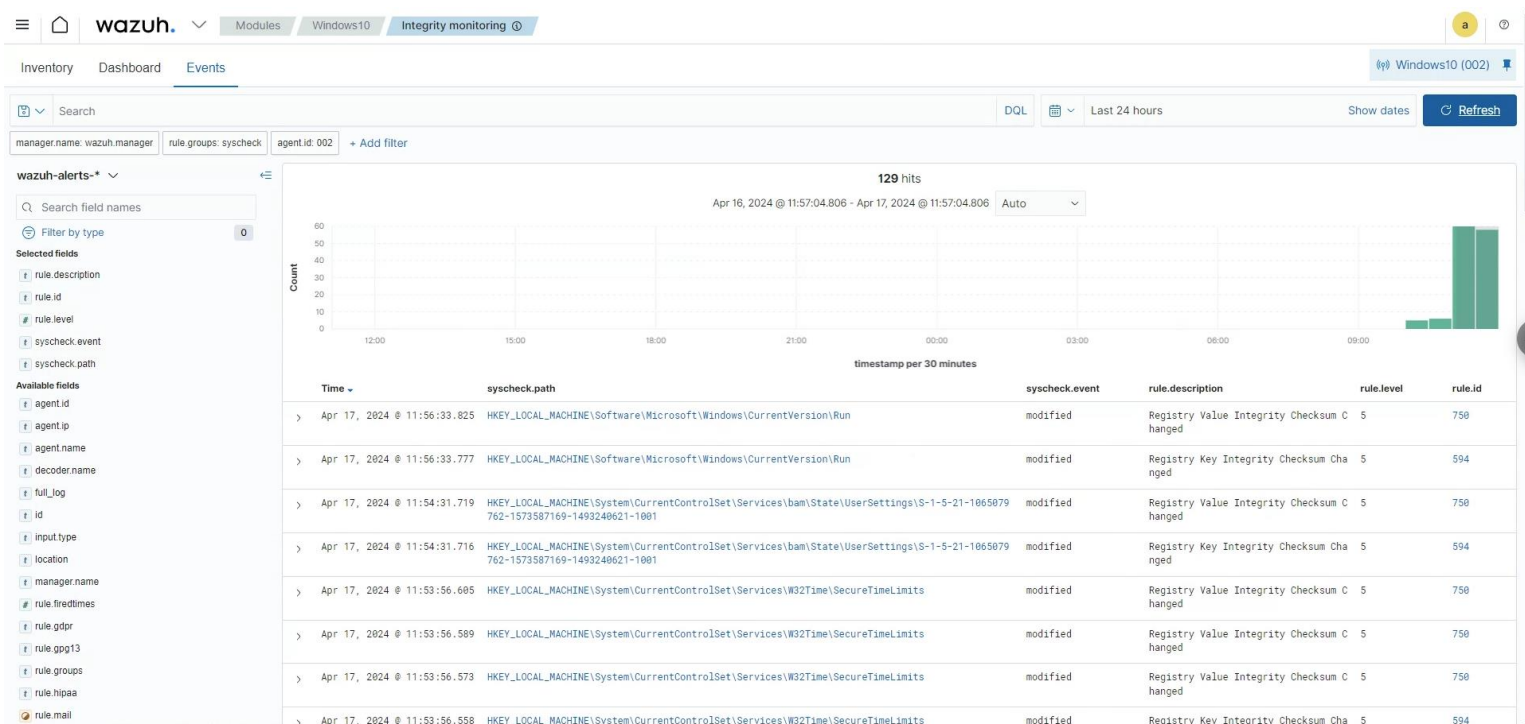
That's all we'll do for now on file integrity, but you can see how powerful a tool that can be. Next, we'll move on and set up vulnerability scanning

The Run key allows programs to execute automatically when a user logs in or the system boots up. This ensures that the malicious software remains active even after a system reboot. By using the Run key, attackers can hide their malicious programs within the registry, making them less visible to standard security tools and harder to detect but we can use an EDR tool to help identify this attack pattern

---

Go complete Question 7 and **Question 8**, then proceed with the next section of the lab.

---

5. Customize the Kali Linux Agent

We will now change the configuration on our Kali Linux agent to transmit system logs to Wazuh.

5.1 Transmit SSH Logs

For this portion of the lab, we will configure Kali Linux to transmit SSH logs to Wazuh. This allows us to see who is connecting to a machine, any login failures, and additional details.

Edit config file on Kali:

`sudo nano /var/ossec/etc/ossec.conf`

`sudo systemctl restart wazuh-agent`

SSH into the kali machine from anywhere. On the Wazuh dashboard, navigate to Threat Intelligence > Threat Hunting, and view the dashboard for your Kali instance. Take a screenshot of the logs generated when you log in and log out of SSH.

Go complete <u>Question 8</u> and <u>Question 9</u> then proceed with the next section of the lab.

Conclusion

That concludes this walkthrough. In this lab we configured and installed a Security Information and Event Management tool, managed a small network of VMs, and set up the capability to track vulnerabilities and watch file integrity on those systems.

Deliverables:

Question 1

Take a screenshot of the dashboard, including the two deployed agents and their status.
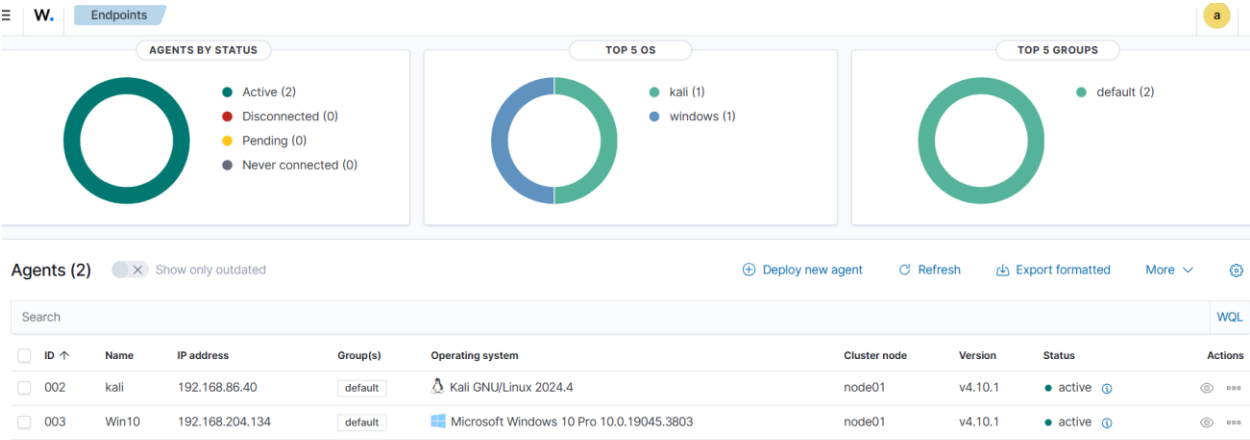
Question 2

Take a screenshot of your test results from the Security Control Assessment.

SYSTEM AUDIT FOR UNIX BASED SYSTEMS

- ● Passed (16)
- ● Failed (1)
- ● Not applicable (6)

System audit for Unix based systems ⓘ

Passed	Failed	Not applicable	Score	End scan
16	1	6	94%	Feb 20, 2025 @ 00:33:53.000

licy

stem audit for Unix based systems

ws per page: 15 ⌄   ‹ 1 ›

Checks (23)   ↻ Refresh   Export formatted

Search				WQL
ID ↑	Title	Target	Result	
3000	SSH Hardening: Port should not be 22	**File:** /etc/ssh/sshd_config	● Passed	⌄
3001	SSH Hardening: Protocol should be set to 2	**File:** /etc/ssh/sshd_config	● Passed	⌄
3002	SSH Hardening: Root account should not be able ...	**File:** /etc/ssh/sshd_config	● Passed	⌄

Question 3

You identified 5 standards of compliance. Research 2 of them, explain what they are, why they are different, and when they are used:

1.**PCI DSS (Payment Card Industry Data Security Standard)**

What it is: PCI DSS is a set of security standards designed to ensure that all companies that handle credit card information maintain a secure environment. It was created by the Payment Card Industry Security Standards Council (PCI SSC).

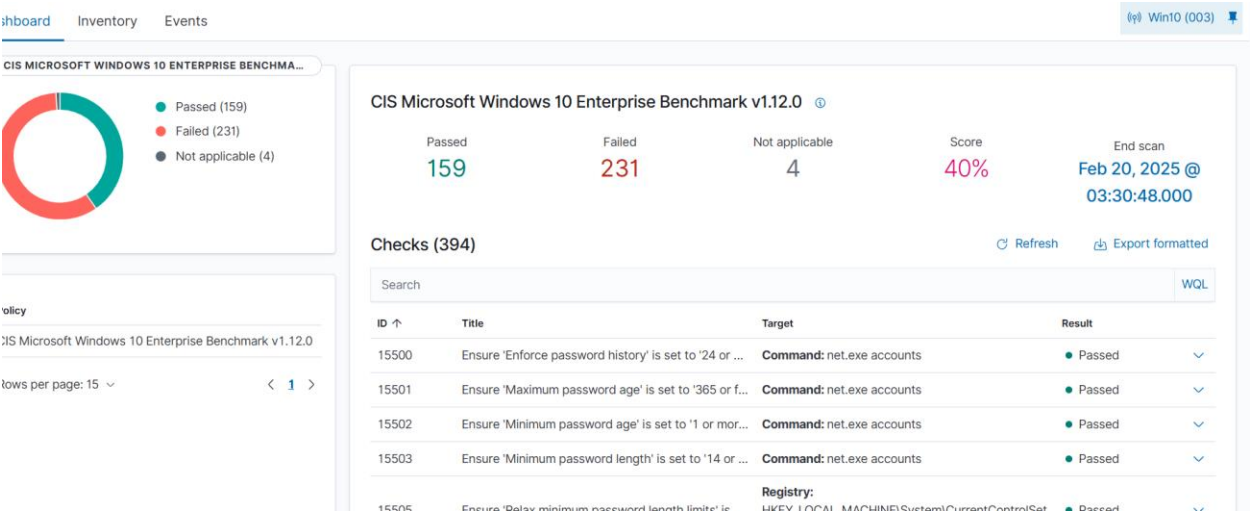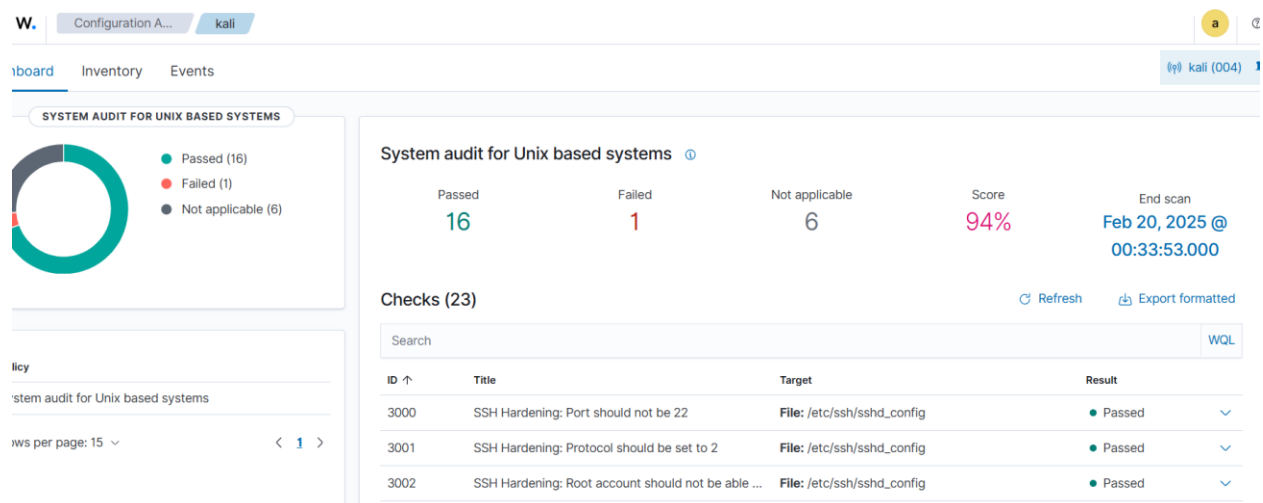**Why it's different**: PCI DSS focuses specifically on protecting payment card data, such as credit and debit card numbers, to prevent fraud and data breaches. It applies to any organization that processes, stores, or transmits cardholder data.

When it's used: Organizations that accept credit card payments, such as retailers, e-commerce sites, and payment processors, must comply with PCI DSS to ensure the security of cardholder data

2. **GDPR (General Data Protection Regulation)**

What it is: GDPR is a comprehensive data protection regulation enacted by the European Union to protect the privacy and personal data of individuals within the EU.

Why it's different: GDPR is broader in scope compared to PCI DSS. It covers all personal data, not just payment information, and applies to any organization that processes the personal data of EU residents, regardless of where the organization is located.

When it's used: Any company that handles the personal data of EU residents, including companies outside the EU, must comply with GDPR. This includes sectors like healthcare, finance, retail, and technology.

Also explain why this type of compliance monitoring might be useful to a company (DO THIS AGAIN)

Compliance monitoring helps companies ensure they meet industry standards and legal requirements, reducing the risk of data breaches, fines, and reputational damage. It also builds trust with customers and partners by demonstrating a commitment to data security and privacy.

Question 4

Take a screenshot of the "Vulnerabilities > Inventory" page of your windows 10 machine in Wazuh. Make sure the screenshot includes the date of the last full scan. After you complete this screenshot, please go research one of the CVEs that your system found and paste the details of the CVE here as well.
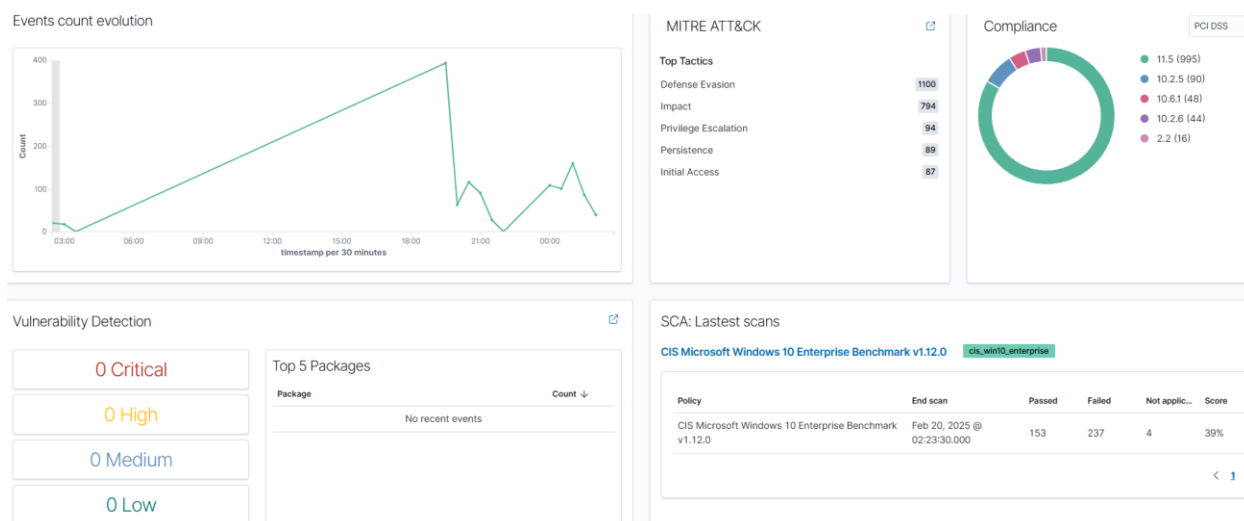
Question 5

Take a screenshot of the Integrity Monitoring events screen showing that Wazuh successfully detected changes to the file integrity of the files on your Windows VM Desktop folder. Make sure `syscheck.diff` displayed.

Dashboard   Inventory   Events   ((•)) Win10 (003) 📌

🔍 Search   DQL 📅 ∨ Last 24 hours   Show dates   ↻ Refresh

manager.name: wazuh-server   rule.groups: syscheck   agent.id: 003 ⊜ ⊕ Add filter

3 hits
Feb 18, 2025 @ 02:54:35.030 - Feb 19, 2025 @ 02:54:35.030

⤓ Export Formatted   🗓 711 available fields ⓘ   ≡ Columns ⊞ Density ⇳ **1 fields sorted** ⛶ Full screen

↓ timestamp	agent.name	syscheck.path	syscheck.event	rule.description	rule.level	rule.id	syscheck.diff
🔍 Feb 19, 2025 @ 02:51:47.6...	Win10	c:\users\gid7\desktop\test.txt	modified	Integrity checksum changed.	7	550	< Hel --- > Tigger is alerted
🔍 Feb 19, 2025 @ 02:47:15.5...	Win10	c:\users\gid7\desktop\test.txt	added	File added to the system.	5	554	-
🔍 Feb 19, 2025 @ 02:47:15.3...	Win10	c:\users\gid7\desktop\new text document.txt	deleted	File deleted.	7	553	-

Question 6

Take a screenshot of the registry key you added in this portion of the lab, as it appears in Wazuh. It should be found under the Windows 10 agent > Integrity Monitoring > Inventory > Windows Registry. You can apply the filter by using:

```
file=HKEY_LOCAL_MACHINE\SOFTWARE\Classes\<yourkeyhere>
```

Dashboard   Inventory   Events   ((•)) Win10 (003) 📌

Files (14)   **Windows Registry (6351)**

Registry (1)   ↻ Refresh   ⤓ Export formatted   ⚙

custom		WQL

Registry ↑	Last modified ⚠
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Customkey	Feb 19, 2025 @ 20:00:42.000

Rows per page: 15 ∨   ⟨ **1** ⟩

Question 7

Take a screenshot of the Integrity Monitoring > Events screen showing that Wazuh has captured the changes made to your custom Registry key.

🔍 Feb 19, 2025 @ 20:31:07.1...	Win10	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Ser...	modified	Registry Key Integrity Checksum Changed	5	594
🔍 Feb 19, 2025 @ 20:49:11.1...	Win10	HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Customkey	modified	Registry Key Integrity Checksum Changed	5	594
🔍 Feb 19, 2025 @ 20:49:11.1...	Win10	HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Customkey	modified	Registry Value Integrity Checksum Changed	5	750
🔍 Feb 19, 2025 @ 20:49:08.8...	Win10	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Ser...	modified	Registry Value Integrity Checksum Changed	5	750

Question 8

Take a screenshot of the Integrity Monitoring > Events screen showing that Wazuh has captured changes made to the Internet Explorer registry key.
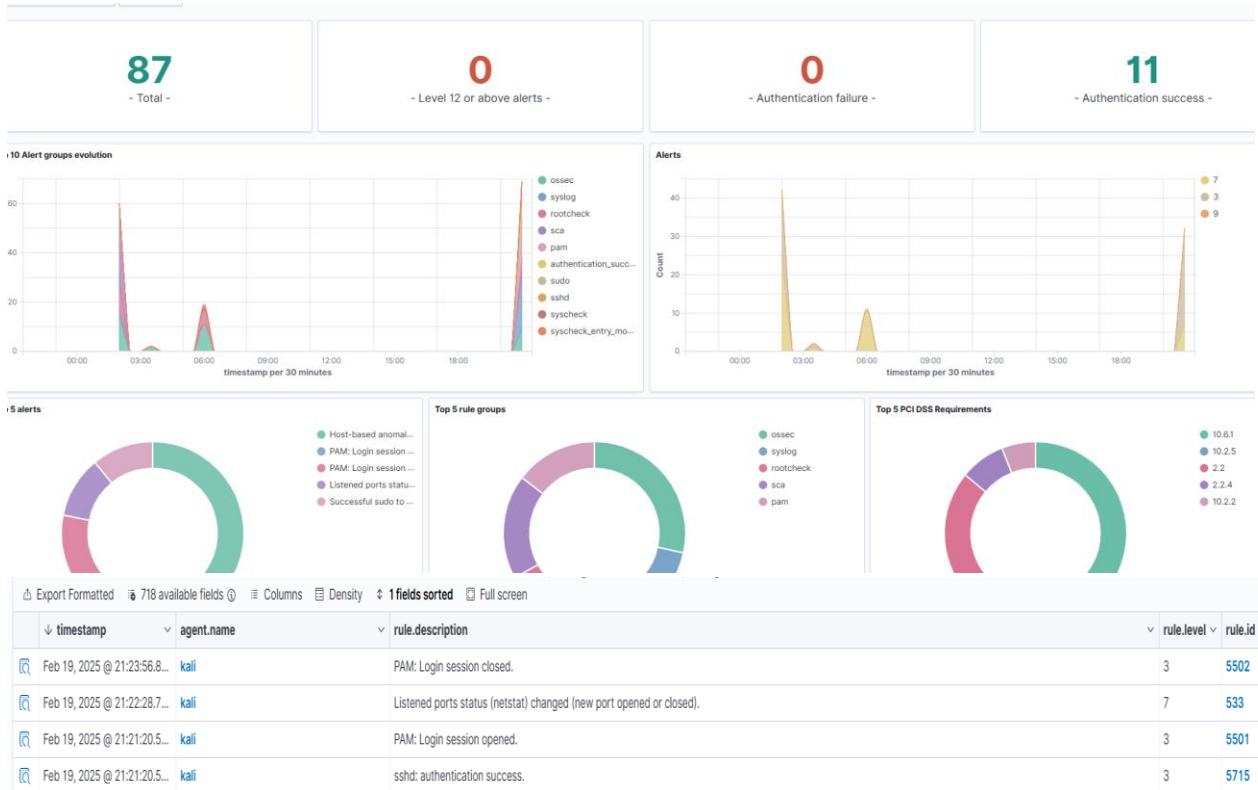

Question 9

Take a screenshot of your Wazuh security alerts screen demonstrating that you have successfully transmitted SSH logs from your Kali Linux machine to Wazuh.

Question 10

You have successfully explored the EDR and SIEM tools offered by Wazuh, now complete the following questions (please don't use an AI chatbot to answer these questions):
1. In your own words, please summarize the benefit of having an EDR solution deployed in your network.

An EDR solution continuously monitors endpoints for suspicious activity, providing real-time threat detection and automated responses to security incidents. It helps identify and contain threats before they spread, reducing the risk of data breaches and system compromises.

2. Can you provide a real-world scenario where an EDR solution could help a cybersecurity analyst to do their job?

A real-world scenario where an EDR solution is useful is detecting ransomware attacks. If an attacker gains access to an employee's computer and begins encrypting files, the EDR system can detect the unusual file modifications, isolate the affected device, and alert security analysts to take action before the ransomware spreads to other systems.

References:

- Wazuh Docker Documentation

  ◦ Wazuh OVA Documentation if needed

- Wazuh Troubleshooting Documentation

Sources related to Section 5.1 – Transmitting Kali Linux Logs

- Configuring Log collection for Linux – Wazuh Documentation

- Log Data collection use cases – Forwarding Linux logs using rsyslog – Wazuh Documentation

- How to configure rsyslog client to send events to Wazuh – Wazuh Blog