

Lab3-2\_Wazuh  
SEC-350  
Ben W  
SP24

Deliverables:

1. Wazuh accessed on mgmt01

The image shows a terminal window and the Wazuh web interface. The terminal window at the top shows the command `hostname` being executed, resulting in `mgmt01-benjamin`. Below the terminal is the Wazuh web interface. The interface has a header with the Wazuh logo and a navigation menu. The main content area displays agent statistics: Total agents (0), Active agents (0), Disconnected agents (0), Pending agents (0), and Never connected agents (0). A yellow banner below the statistics states: "No agents were added to this manager. Add agent". The interface is divided into two main sections: "SECURITY INFORMATION MANAGEMENT" and "AUDITING AND POLICY MONITORING". Under "SECURITY INFORMATION MANAGEMENT", there are two cards: "Security events" (Browse through your security alerts, identifying issues and threats in your environment) and "Integrity monitoring" (Alerts related to file changes, including permissions, content, ownership and attributes). Under "AUDITING AND POLICY MONITORING", there are two cards: "Policy monitoring" (Verify that your systems are configured according to your security policies baseline) and "System auditing" (Audit users behavior, monitoring command execution and alerting on access to critical files).

```
ben@xubuntu:~/SEC-350$ hostname
mgmt01-benjamin
ben@xubuntu:~/SEC-350$
```

wazuh. / Modules

Total agents 0 Active agents 0 Disconnected agents 0 Pending agents 0 Never connected agents 0

⚠ No agents were added to this manager. [Add agent](#)

**SECURITY INFORMATION MANAGEMENT**

- Security events**  
Browse through your security alerts, identifying issues and threats in your environment.
- Integrity monitoring**  
Alerts related to file changes, including permissions, content, ownership and attributes.

**AUDITING AND POLICY MONITORING**

- Policy monitoring**  
Verify that your systems are configured according to your security policies baseline.
- System auditing**  
Audit users behavior, monitoring command execution and alerting on access to critical files.

2. Agent in wazuh (nginx because web01 is gone)

wazuh. / Agents

DETAILS

Active0

Disconnected0

Pending1

Never connected0

Agents coverage0.00%

Last registered agent  
nginx-benjamin

Most active agent  
-

EVOLUTION

Last 24 hours

No results found

Filter or search agent

Refresh

Agents (1)

Deploy new agent

Export formatted

I. ↑	Name	IP	Group(s)	OS	Cluster ...	V...	Registr...	Last ke...	Status	A...
001	nginx-benja...	172.16...	linux	Ubuntu ...	node01	v...	Dec 3...	Apr 1, ...		

3. Non-existent user login attempt

timestamp per 30 minutes				
Time	rule.description	rule.level	rule.id	
> Apr 21, 2024 @ 13:48:56.110	syslog: User missed the password more than one time	10	2502	
> Apr 21, 2024 @ 13:48:56.105	sshd: Attempt to login using a non-existent user	5	5710	
> Apr 21, 2024 @ 13:48:52.099	sshd: Attempt to login using a non-existent user	5	5710	
> Apr 21, 2024 @ 13:48:48.095	sshd: Attempt to login using a non-existent user	5	5710	
> Apr 21, 2024 @ 13:48:46.100	PAM: User login failed.	5	5503	
> Apr 21, 2024 @ 13:48:44.091	sshd: Attempt to login using a non-existent user	5	5710	

4. <https://github.com/benjamin-weatherill/SEC-350/wiki/Wazuh-Installation-and-Implementation>