wazuh.

Wazuh – GitHub

INTEGRATION

Lab Created By: MUHAMMAD MOIZ UD DIN RAFAY

Follow Me: linkedin.com/in/moizuddinrafay

Wazuh Integration with GitHub

Integrating Wazuh with GitHub allows for enhanced security monitoring and compliance checks of your repositories. This integration can help detect and respond to potential security threats and vulnerabilities in your codebase and ensure that your repositories adhere to security policies and best practices.

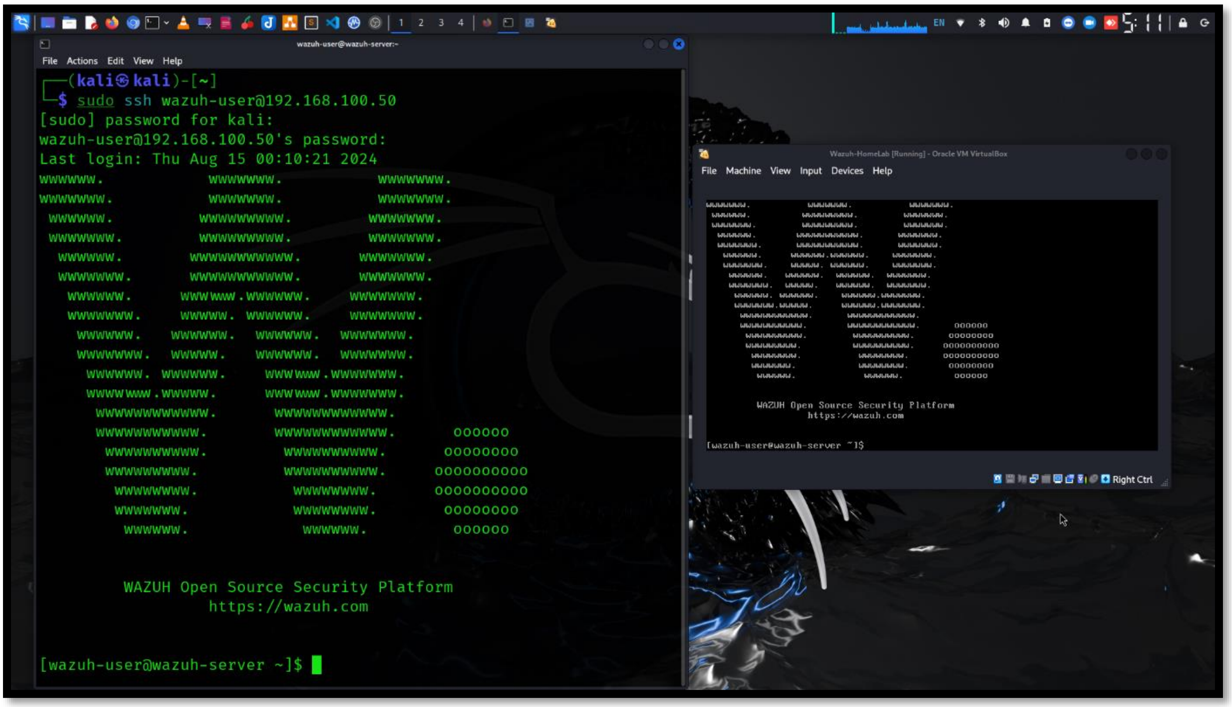
Key Features:

Monitoring and Alerting: Wazuh can monitor GitHub repositories for changes, including new commits, pull requests, and issues. It can alert security teams about suspicious activities, such as unauthorized access or potentially malicious code changes.

Incident Response: In the event of a security incident, Wazuh can automatically trigger incident response actions. For example, it can revoke access tokens, restrict repository access, or notify the security team for further investigation.

Audit and Reporting: Wazuh provides detailed logs and reports on activities within GitHub repositories, making it easier to audit changes and demonstrate compliance with regulatory requirements.

Here is my Wazuh server running on virtualbox.

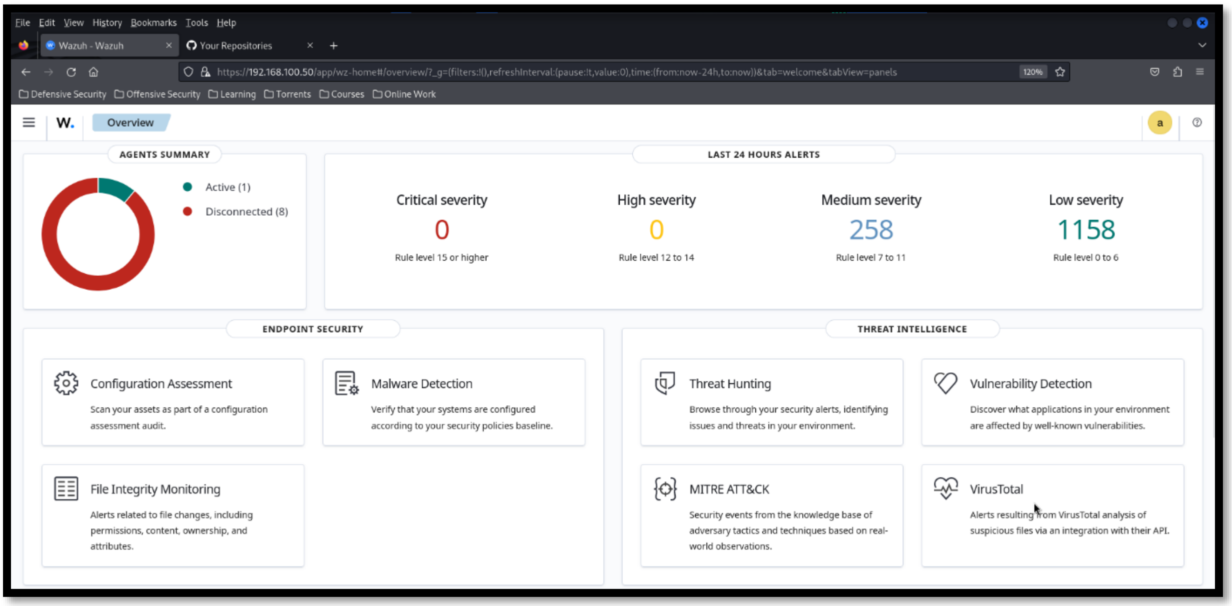


wazuh-user@wazuh-server:~
File Actions Edit View Help
Wazuh-HomeLab [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Right Ctrl

```
┌──(kali㉿kali)-[~]
└─$ sudo ssh wazuh-user@192.168.100.50
[sudo] password for kali:
wazuh-user@192.168.100.50's password:
Last login: Thu Aug 15 00:10:21 2024
wwwwww.           wwwwwww.          wwwwwww.
wwwwwww.          wwwwwww.          wwwwwww.
 wwwwww.         wwwwwwwww.        wwwwwww.
 wwwwwww.        wwwwwwwww.        wwwwwww.
  wwwwww.       wwwwwwwwwww.      wwwwwww.
  wwwwwww.      wwwwwwwwwww.      wwwwwww.
   wwwwww.     wwwwww.wwwwww.    wwwwwww.
   wwwwwww.    wwwww. wwwwww.    wwwwwww.
    wwwwww.   wwwwww.  wwwwww.  wwwwwww.
    wwwwwww.  wwwww.   wwwwww.  wwwwwww.
     wwwwww. wwwwww.    wwwwww.wwwwwww.
     wwwwwww.wwwww.     wwwwww.wwwwwww.
      wwwwwwwwwwww.      wwwwwwwwwwww.
      wwwwwwwwwww.       wwwwwwwwwwww.       oooooo
       wwwwwwwwww.        wwwwwwwwww.       oooooooo
       wwwwwwwww.         wwwwwwwwww.      oooooooooo
        wwwwwwww.          wwwwwwww.       oooooooooo
        wwwwwww.           wwwwwwww.        oooooooo
         wwwwww.            wwwwww.          oooooo


         WAZUH Open Source Security Platform
                  https://wazuh.com


[wazuh-user@wazuh-server ~]$ 
```

```
         WAZUH Open Source Security Platform
                  https://wazuh.com

[wazuh-user@wazuh-server ~]$
```

Wazuh Dashboard



File Edit View History Bookmarks Tools Help
Wazuh - Wazuh
Your Repositories
https://192.168.100.50/app/wz-home#/overview/?_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:now-24h,to:now))&tab=welcome&tabView=panels
120%
Defensive Security
Offensive Security
Learning
Torrents
Courses
Online Work
W.
Overview
a

AGENTS SUMMARY

- Active (1)
- Disconnected (8)

LAST 24 HOURS ALERTS

Critical severity	High severity	Medium severity	Low severity
0	0	258	1158
Rule level 15 or higher	Rule level 12 to 14	Rule level 7 to 11	Rule level 0 to 6

ENDPOINT SECURITY

Configuration Assessment
Scan your assets as part of a configuration assessment audit.

Malware Detection
Verify that your systems are configured according to your security policies baseline.

File Integrity Monitoring
Alerts related to file changes, including permissions, content, ownership, and attributes.

THREAT INTELLIGENCE

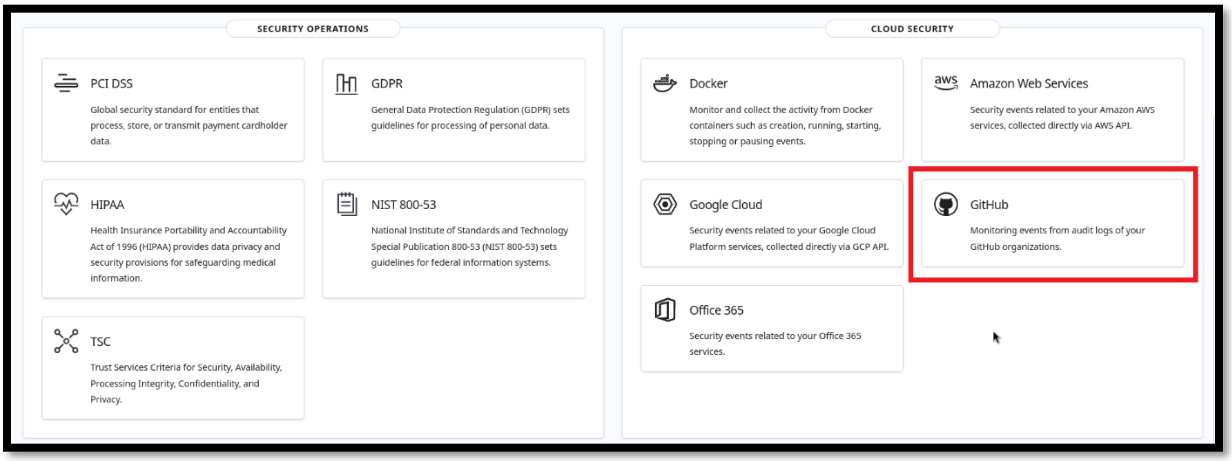
Threat Hunting
Browse through your security alerts, identifying issues and threats in your environment.

Vulnerability Detection
Discover what applications in your environment are affected by well-known vulnerabilities.

MITRE ATT&CK
Security events from the knowledge base of adversary tactics and techniques based on real-world observations.

VirusTotal
Alerts resulting from VirusTotal analysis of suspicious files via an integration with their API.

Scroll down in Wazuh-dashboard and go to “Cloud Security” and select “Github” for integration. Make sure you have an account on GitHub.



SECURITY OPERATIONS

PCI DSS

Global security standard for entities that process, store, or transmit payment cardholder data.

GDPR

General Data Protection Regulation (GDPR) sets guidelines for processing of personal data.

HIPAA

Health Insurance Portability and Accountability Act of 1996 (HIPAA) provides data privacy and security provisions for safeguarding medical information.

NIST 800-53

National Institute of Standards and Technology Special Publication 800-53 (NIST 800-53) sets guidelines for federal information systems.

TSC

Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy.

CLOUD SECURITY

Docker

Monitor and collect the activity from Docker containers such as creation, running, starting, stopping or pausing events.

Amazon Web Services

Security events related to your Amazon AWS services, collected directly via AWS API.

Google Cloud

Security events related to your Google Cloud Platform services, collected directly via GCP API.

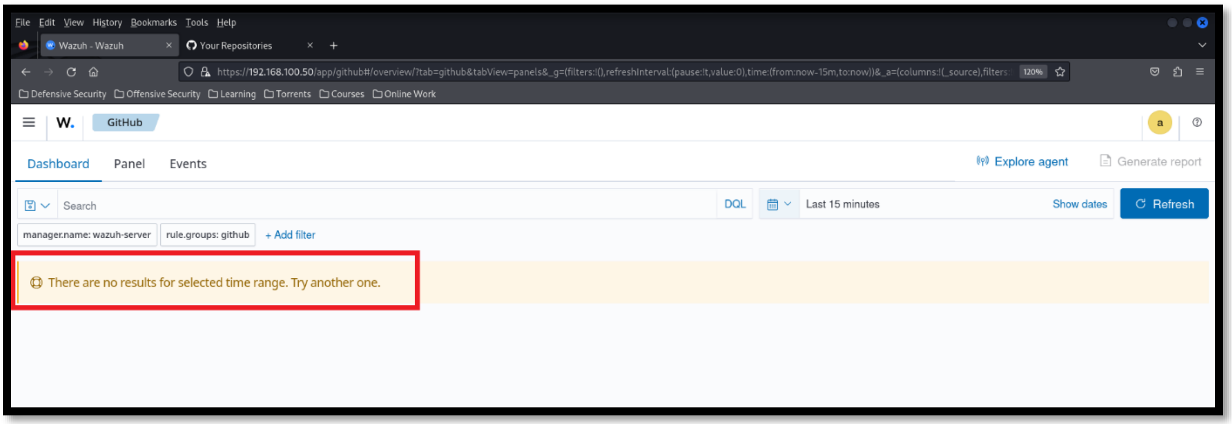
GitHub

Monitoring events from audit logs of your GitHub organizations.

Office 365

Security events related to your Office 365 services.

After selecting there is no logs by default.



https://192.168.100.50/app/github#/overview/?tab=github&tabView=panels&_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:now-15m,to:now))&_a=(columns:!(_source),filters

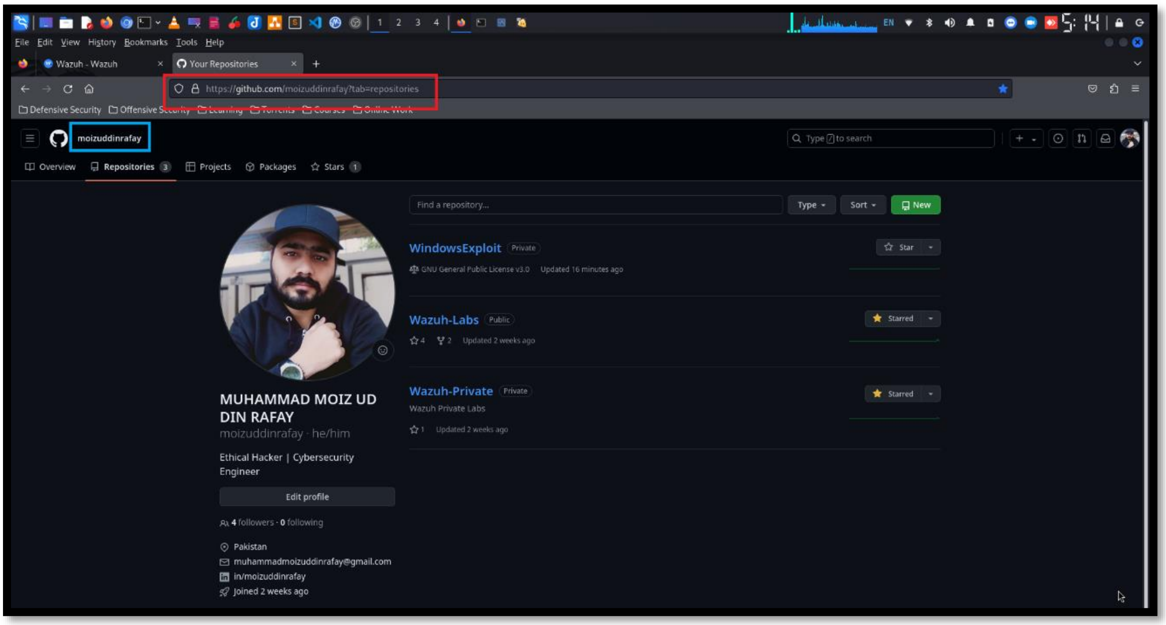
Last 15 minutes

manager.name: wazuh-server

rule.groups: github

There are no results for selected time range. Try another one.

Now login to GitHub account. I am using my own account for integration.



https://github.com/moizuddinrafay?tab=repositories

moizuddinrafay

WindowsExploit Private

GNU General Public License v3.0 Updated 16 minutes ago

Wazuh-Labs Public

4 2 Updated 2 weeks ago

Wazuh-Private Private

Wazuh Private Labs

1 Updated 2 weeks ago

MUHAMMAD MOIZ UD DIN RAFAY

moizuddinrafay · he/him

Ethical Hacker | Cybersecurity Engineer

4 followers · 0 following

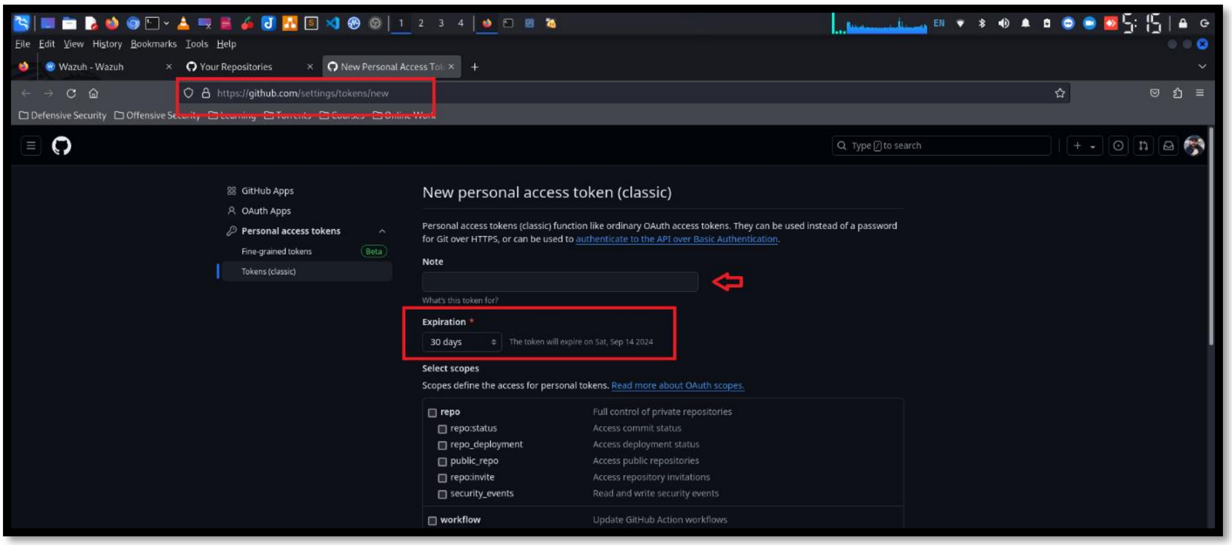
Pakistan

muhammadmoizuddinrafay@gmail.com

in/moizuddinrafay

Joined 2 weeks ago

You can visit this link: https://github.com/settings/tokens/new for generate new token for Wazuh integration.



New personal access token (classic)

Personal access tokens (classic) function like ordinary OAuth access tokens. They can be used instead of a password for Git over HTTPS, or can be used to authenticate to the API over Basic Authentication.

Note

What's this token for?

Expiration *

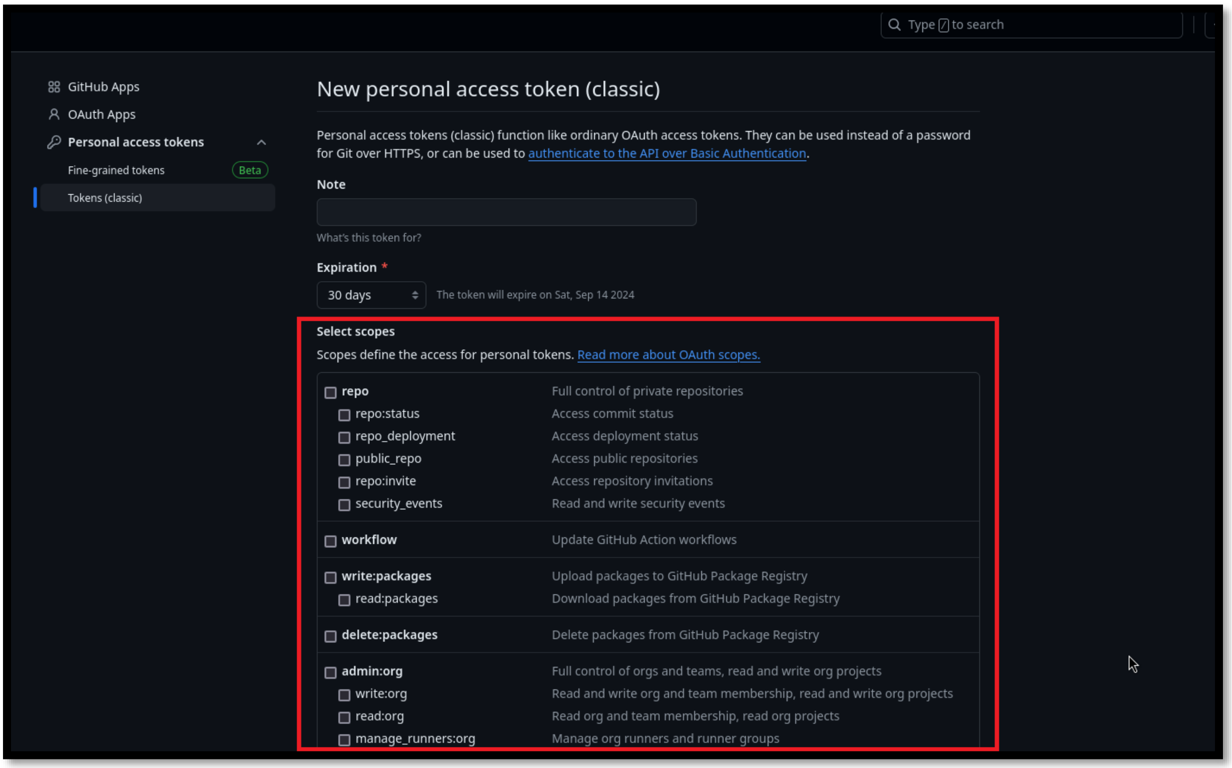
30 days The token will expire on Sat, Sep 14 2024

Select scopes

Scopes define the access for personal tokens. Read more about OAuth scopes.

□ repo	Full control of private repositories
□ repo:status	Access commit status
□ repo_deployment	Access deployment status
□ public_repo	Access public repositories
□ repo:invite	Access repository invitations
□ security_events	Read and write security events
□ workflow	Update GitHub Action workflows

You can select “Expiration” and “Scop”.



New personal access token (classic)

Personal access tokens (classic) function like ordinary OAuth access tokens. They can be used instead of a password for Git over HTTPS, or can be used to authenticate to the API over Basic Authentication.

Note

What's this token for?

Expiration *

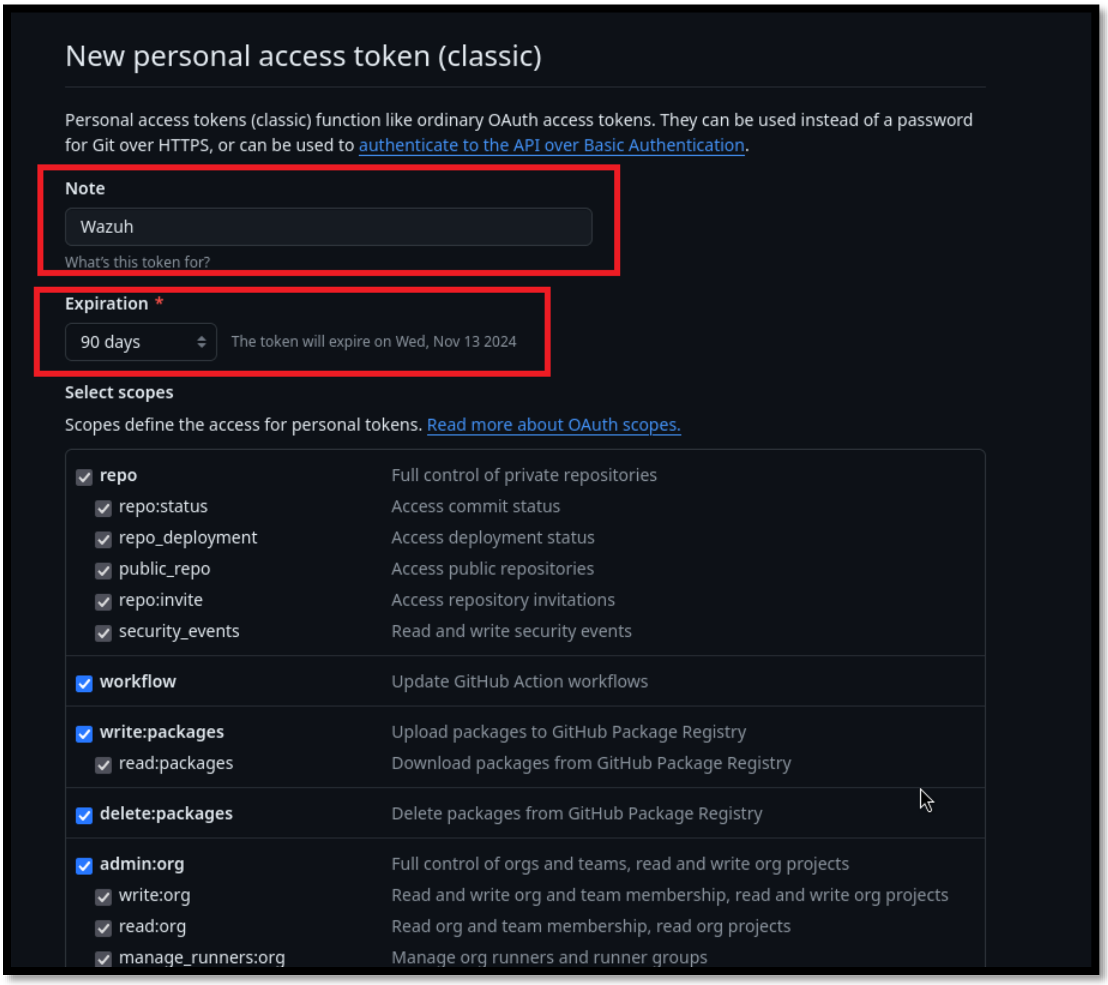
30 days The token will expire on Sat, Sep 14 2024

Select scopes

Scopes define the access for personal tokens. Read more about OAuth scopes.

□ repo	Full control of private repositories
□ repo:status	Access commit status
□ repo_deployment	Access deployment status
□ public_repo	Access public repositories
□ repo:invite	Access repository invitations
□ security_events	Read and write security events
□ workflow	Update GitHub Action workflows
□ write:packages	Upload packages to GitHub Package Registry
□ read:packages	Download packages from GitHub Package Registry
□ delete:packages	Delete packages from GitHub Package Registry
□ admin:org	Full control of orgs and teams, read and write org projects
□ write:org	Read and write org and team membership, read and write org projects
□ read:org	Read org and team membership, read org projects
□ manage_runners:org	Manage org runners and runner groups

Creating new "token" for Wazuh integration.



New personal access token (classic)

Personal access tokens (classic) function like ordinary OAuth access tokens. They can be used instead of a password for Git over HTTPS, or can be used to authenticate to the API over Basic Authentication.

Note

Wazuh

What's this token for?

Expiration *

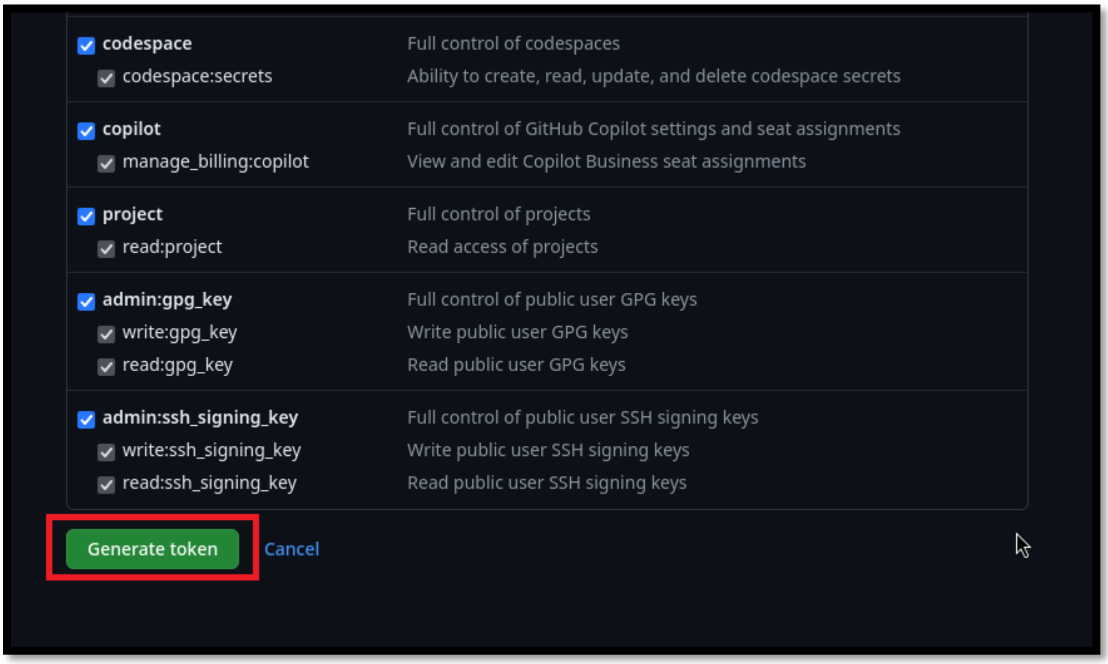
90 days The token will expire on Wed, Nov 13 2024

Select scopes

Scopes define the access for personal tokens. Read more about OAuth scopes.

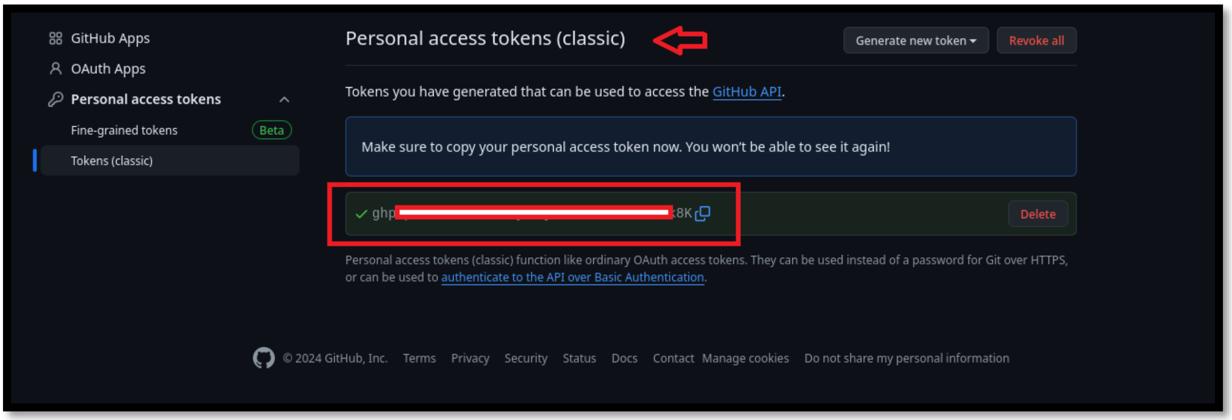
☑ repo	Full control of private repositories
☑ repo:status	Access commit status
☑ repo_deployment	Access deployment status
☑ public_repo	Access public repositories
☑ repo:invite	Access repository invitations
☑ security_events	Read and write security events
☑ workflow	Update GitHub Action workflows
☑ write:packages	Upload packages to GitHub Package Registry
☑ read:packages	Download packages from GitHub Package Registry
☑ delete:packages	Delete packages from GitHub Package Registry
☑ admin:org	Full control of orgs and teams, read and write org projects
☑ write:org	Read and write org and team membership, read and write org projects
☑ read:org	Read org and team membership, read org projects
☑ manage_runners:org	Manage org runners and runner groups

After selecting the scope, click on "Generate token".



☑ codespace	Full control of codespaces
☑ codespace:secrets	Ability to create, read, update, and delete codespace secrets
☑ copilot	Full control of GitHub Copilot settings and seat assignments
☑ manage_billing:copilot	View and edit Copilot Business seat assignments
☑ project	Full control of projects
☑ read:project	Read access of projects
☑ admin:gpg_key	Full control of public user GPG keys
☑ write:gpg_key	Write public user GPG keys
☑ read:gpg_key	Read public user GPG keys
☑ admin:ssh_signing_key	Full control of public user SSH signing keys
☑ write:ssh_signing_key	Write public user SSH signing keys
☑ read:ssh_signing_key	Read public user SSH signing keys

Here is token.



Personal access tokens (classic)

Tokens you have generated that can be used to access the GitHub API.

Make sure to copy your personal access token now. You won't be able to see it again!

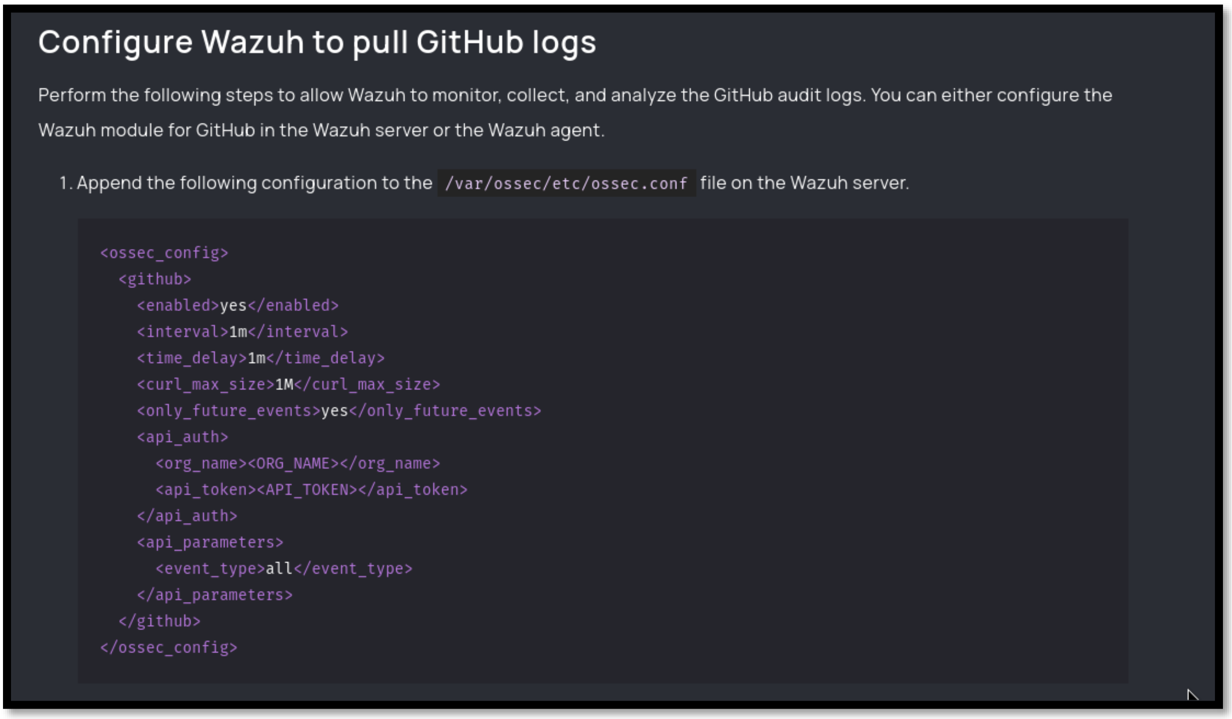
✓ [redacted]

Personal access tokens (classic) function like ordinary OAuth access tokens. They can be used instead of a password for Git over HTTPS, or can be used to authenticate to the API over Basic Authentication.

© 2024 GitHub, Inc. Terms Privacy Security Status Docs Contact Manage cookies Do not share my personal information

You can follow this configuration.

Link: https://documentation.wazuh.com/current/cloud-security/github/monitoring-github-activity.html



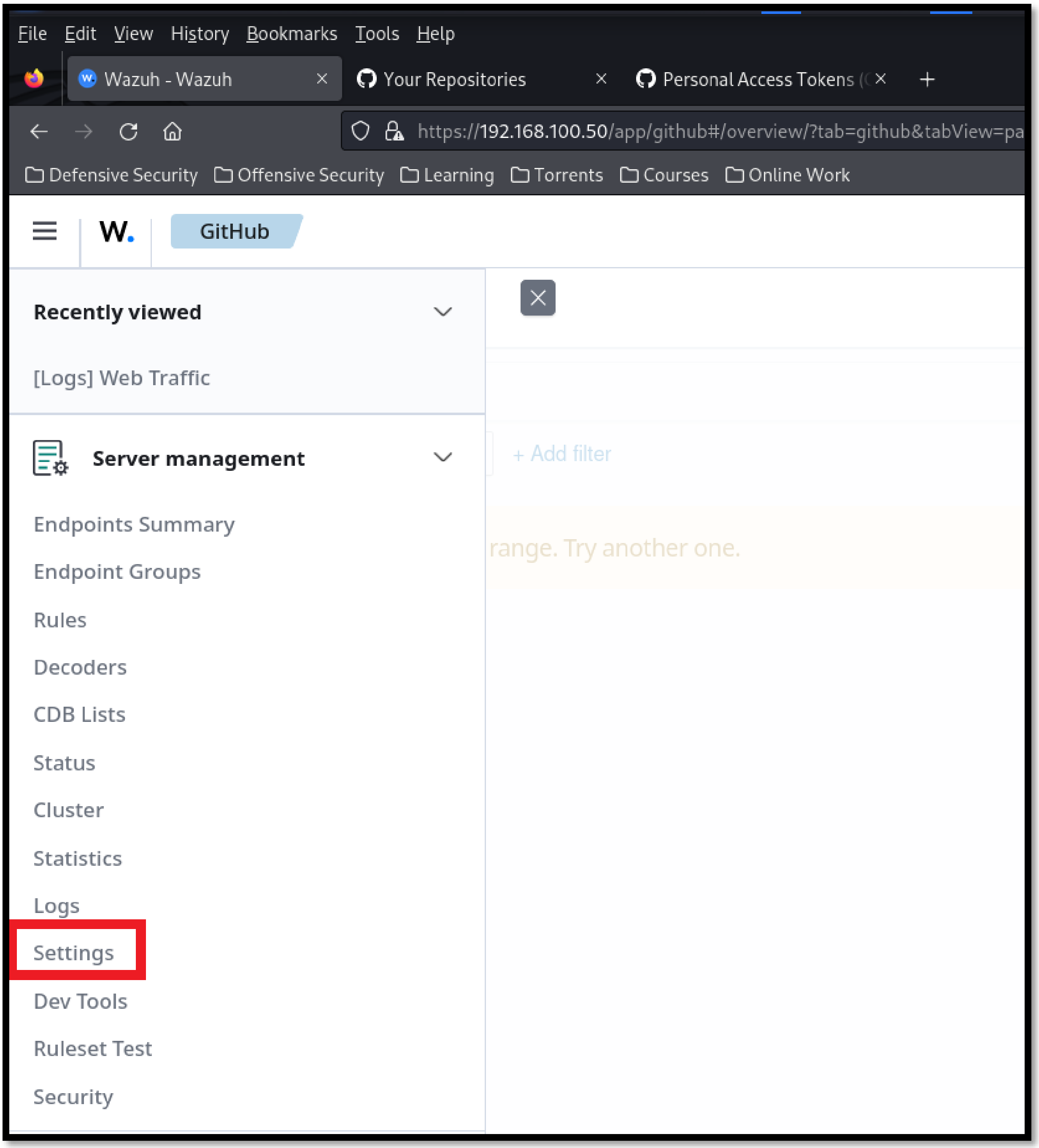
Configure Wazuh to pull GitHub logs

Perform the following steps to allow Wazuh to monitor, collect, and analyze the GitHub audit logs. You can either configure the Wazuh module for GitHub in the Wazuh server or the Wazuh agent.

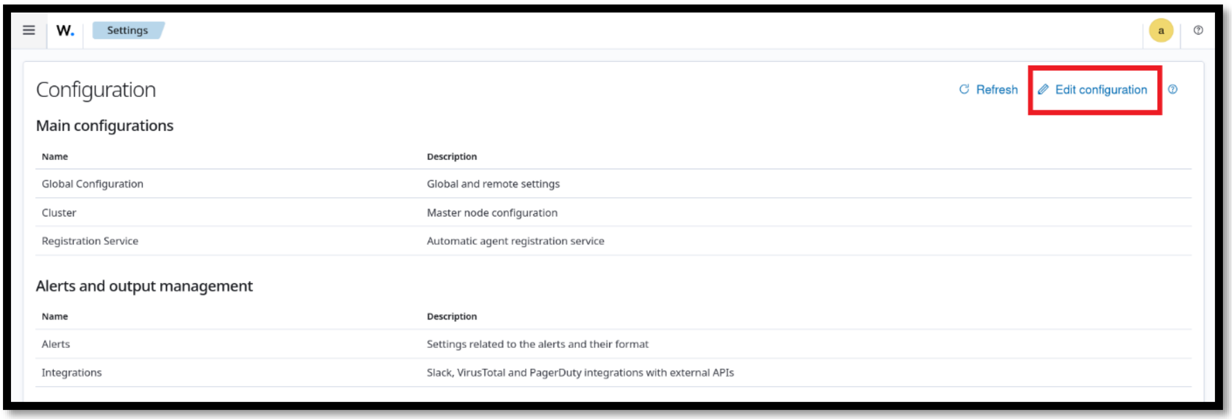
1. Append the following configuration to the `/var/ossec/etc/ossec.conf` file on the Wazuh server.

```
<ossec_config>
  <github>
    <enabled>yes</enabled>
    <interval>1m</interval>
    <time_delay>1m</time_delay>
    <curl_max_size>1M</curl_max_size>
    <only_future_events>yes</only_future_events>
    <api_auth>
      <org_name><ORG_NAME></org_name>
      <api_token><API_TOKEN></api_token>
    </api_auth>
    <api_parameters>
      <event_type>all</event_type>
    </api_parameters>
  </github>
</ossec_config>
```

In Wazuh-dashboard go to “Server Management” and select “Settings”.



Now we have to edit “ossec.conf”.



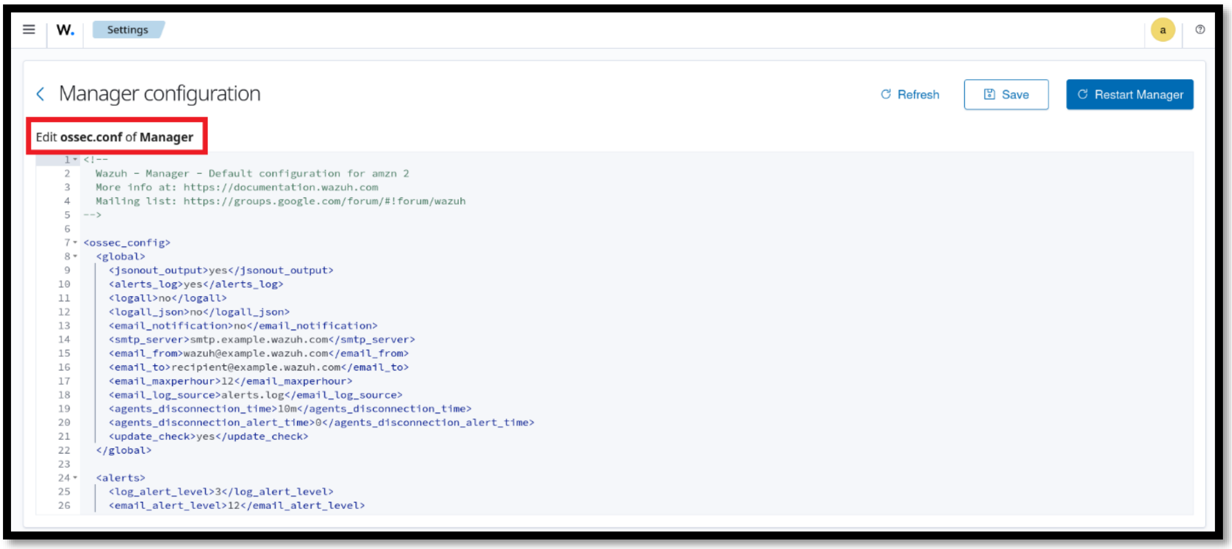
Configuration

Main configurations

Name	Description
Global Configuration	Global and remote settings
Cluster	Master node configuration
Registration Service	Automatic agent registration service

Alerts and output management

Name	Description
Alerts	Settings related to the alerts and their format
Integrations	Slack, VirusTotal and PagerDuty integrations with external APIs



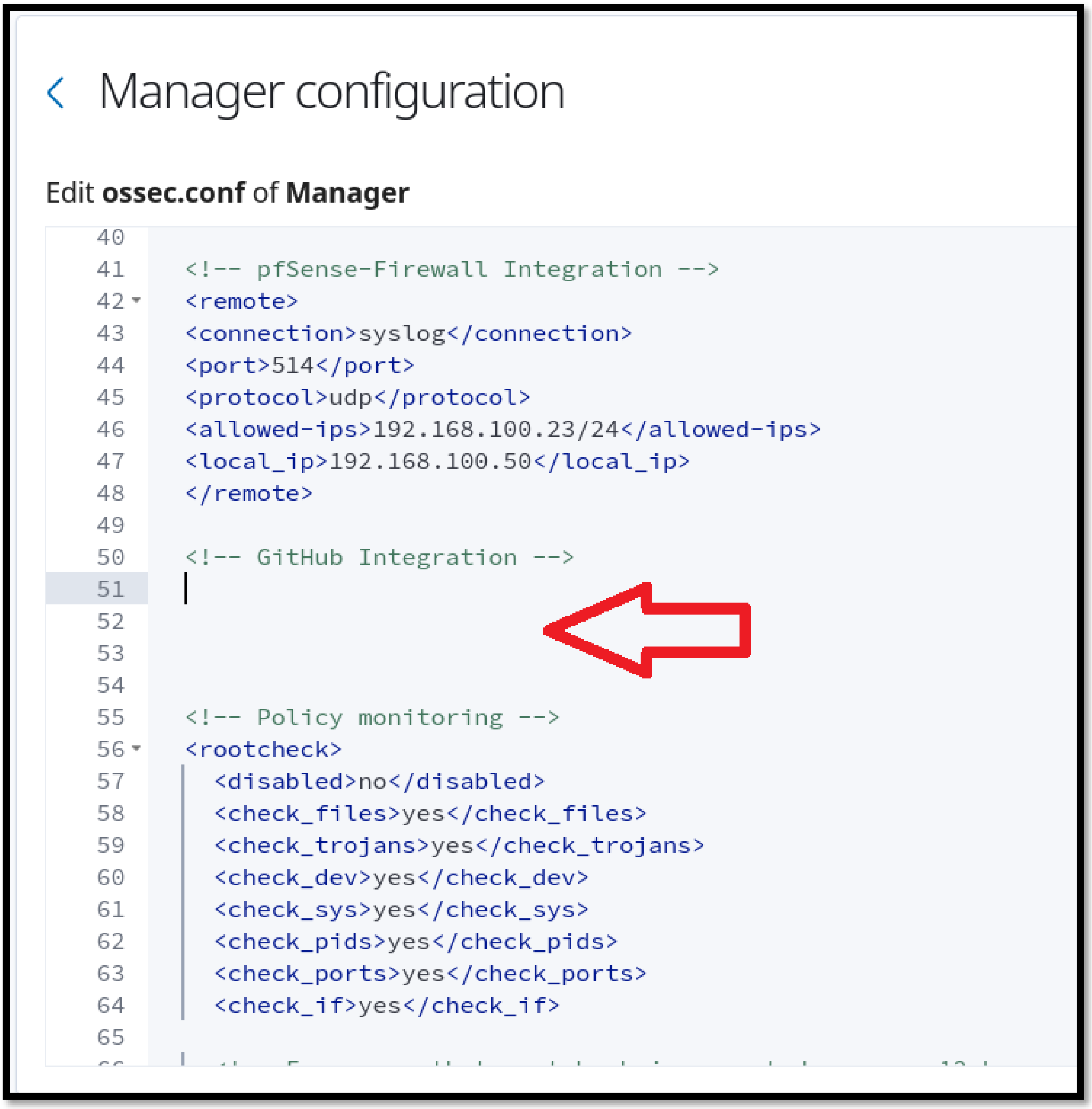
Manager configuration

Edit **ossec.conf** of **Manager**

```
<!--
  Wazuh - Manager - Default configuration for amzn 2
  More info at: https://documentation.wazuh.com
  Mailing list: https://groups.google.com/forum/#!forum/wazuh
-->

<ossec_config>
  <global>
    <jsonout_output>yes</jsonout_output>
    <alerts_log>yes</alerts_log>
    <logall>no</logall>
    <logall_json>no</logall_json>
    <email_notification>no</email_notification>
    <smtp_server>smtp.example.wazuh.com</smtp_server>
    <email_from>wazuh@example.wazuh.com</email_from>
    <email_to>recipient@example.wazuh.com</email_to>
    <email_maxperhour>12</email_maxperhour>
    <email_log_source>alerts.log</email_log_source>
    <agents_disconnection_time>10m</agents_disconnection_time>
    <agents_disconnection_alert_time>0</agents_disconnection_alert_time>
    <update_check>yes</update_check>
  </global>

  <alerts>
    <log_alert_level>3</log_alert_level>
    <email_alert_level>12</email_alert_level>
```

```
 <github>
   <enabled>yes</enabled>
   <interval>1m</interval>
   <time_delay>1m</time_delay>
   <curl_max_size>1M</curl_max_size>
   <only_future_events>yes</only_future_events>
   <api_auth>
   <org_name><ORG_NAME></org_name>
   <api_token><API_TOKEN></api_token>
   </api_auth>
  <api_parameters>
  <event_type>all</event_type>
  </api_parameters>
</github>
```

We have to add configuration here.

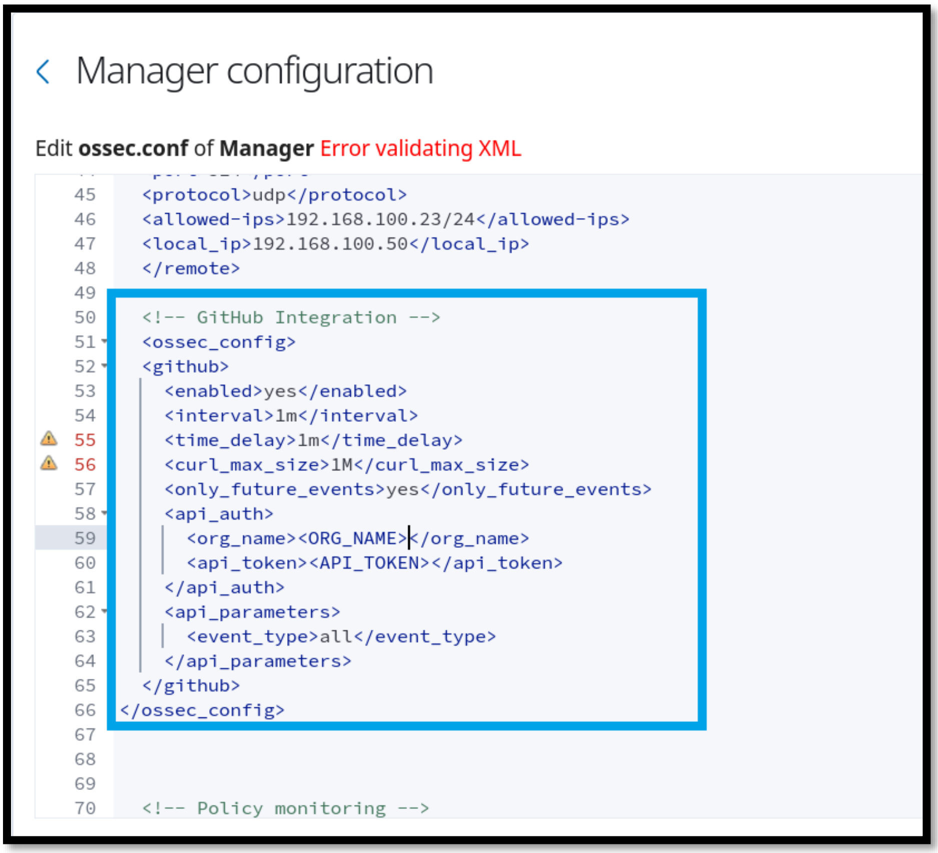


Manager configuration

Edit **ossec.conf** of **Manager**

```

<!-- pfSense-Firewall Integration -->
<remote>
<connection>syslog</connection>
<port>514</port>
<protocol>udp</protocol>
<allowed-ips>192.168.100.23/24</allowed-ips>
<local_ip>192.168.100.50</local_ip>
</remote>

<!-- GitHub Integration -->




<!-- Policy monitoring -->
<rootcheck>
  <disabled>no</disabled>
  <check_files>yes</check_files>
  <check_trojans>yes</check_trojans>
  <check_dev>yes</check_dev>
  <check_sys>yes</check_sys>
  <check_pids>yes</check_pids>
  <check_ports>yes</check_ports>
  <check_if>yes</check_if>

```

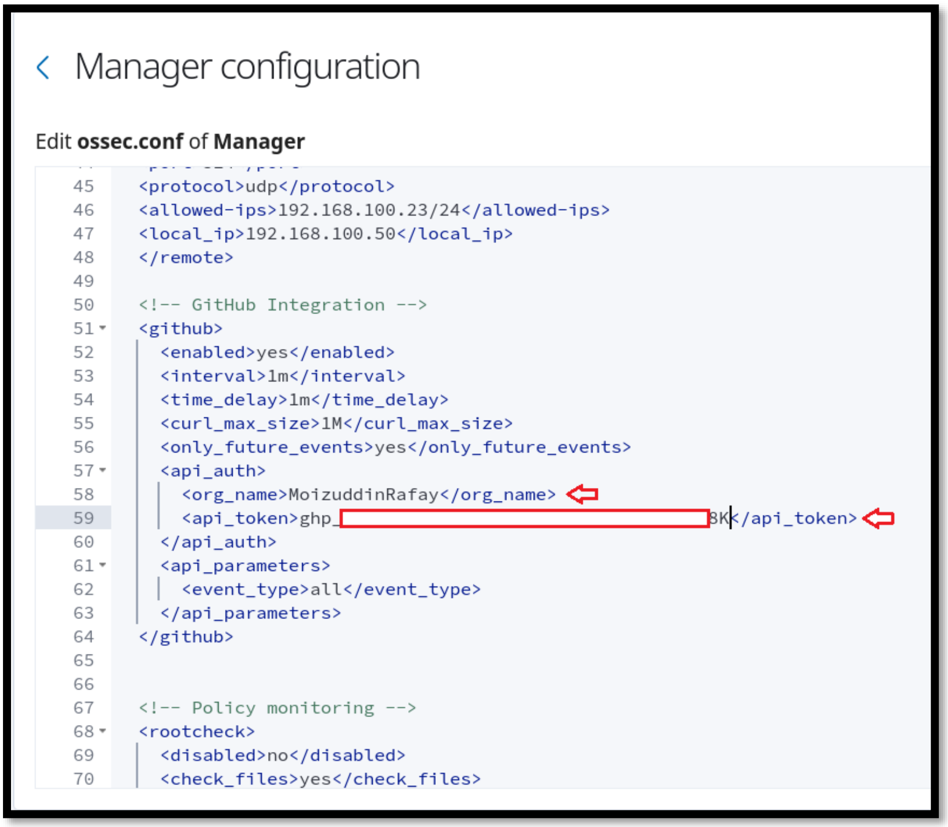
Follow the same and add “GitHub” generated token in configuration.



Manager configuration

Edit **ossec.conf** of **Manager** Error validating XML

```
  <protocol>udp</protocol>
  <allowed-ips>192.168.100.23/24</allowed-ips>
  <local_ip>192.168.100.50</local_ip>
  </remote>

  <!-- GitHub Integration -->
  <ossec_config>
  <github>
    <enabled>yes</enabled>
    <interval>1m</interval>
    <time_delay>1m</time_delay>
    <curl_max_size>1M</curl_max_size>
    <only_future_events>yes</only_future_events>
    <api_auth>
      <org_name><ORG_NAME></org_name>
      <api_token><API_TOKEN></api_token>
    </api_auth>
    <api_parameters>
      <event_type>all</event_type>
    </api_parameters>
  </github>
</ossec_config>



  <!-- Policy monitoring -->
```

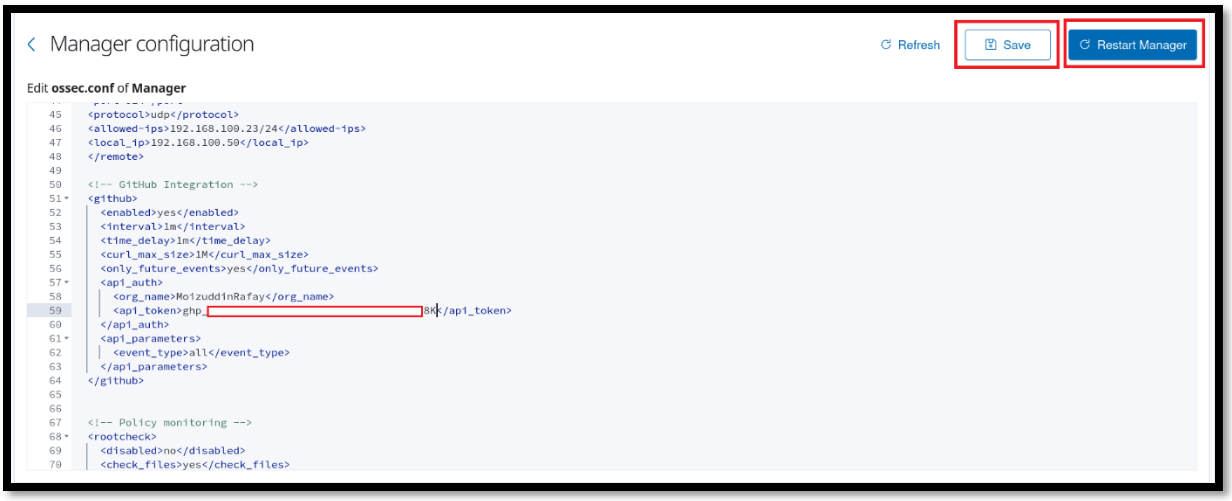


Manager configuration

Edit **ossec.conf** of **Manager**

```
  <protocol>udp</protocol>
  <allowed-ips>192.168.100.23/24</allowed-ips>
  <local_ip>192.168.100.50</local_ip>
  </remote>

  <!-- GitHub Integration -->
  <github>
    <enabled>yes</enabled>
    <interval>1m</interval>
    <time_delay>1m</time_delay>
    <curl_max_size>1M</curl_max_size>
    <only_future_events>yes</only_future_events>
    <api_auth>
      <org_name>MoizuddinRafay</org_name>
      <api_token>ghp_[redacted]8K</api_token>
    </api_auth>
    <api_parameters>
      <event_type>all</event_type>
    </api_parameters>
  </github>


  <!-- Policy monitoring -->
  <rootcheck>
    <disabled>no</disabled>
    <check_files>yes</check_files>
```

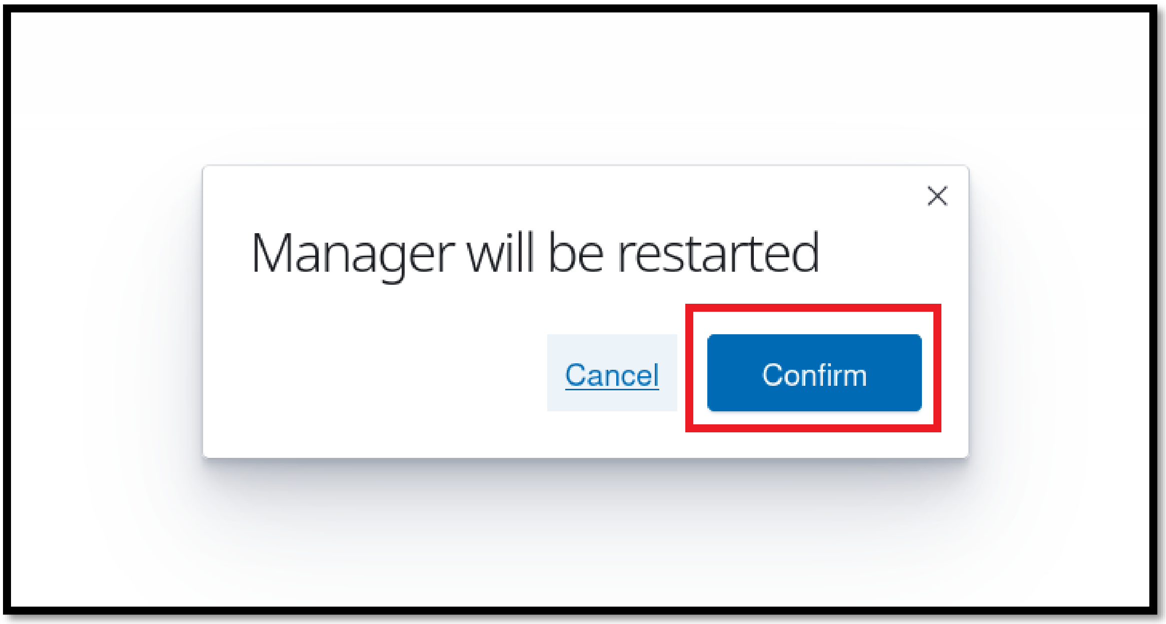
Save the configuration and restart Wazuh-manager.



Edit **ossec.conf** of **Manager**

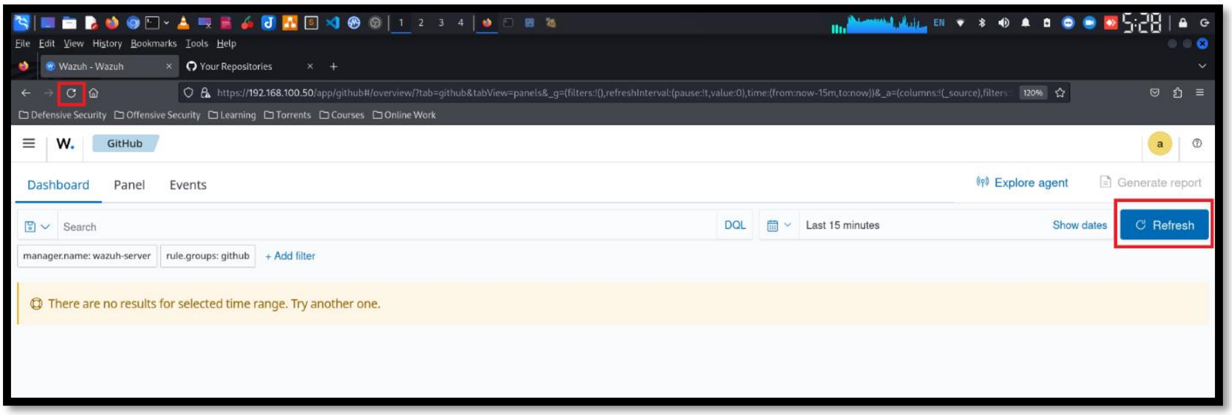
```
<protocol>udp</protocol>
<allowed-ips>192.168.100.23/24</allowed-ips>
<local_ip>192.168.100.50</local_ip>
</remote>

<!-- GitHub Integration -->
<github>
  <enabled>yes</enabled>
  <interval>1m</interval>
  <time_delay>1m</time_delay>
  <curl_max_size>1M</curl_max_size>
  <only_future_events>yes</only_future_events>
  <api_auth>
    <org_name>MoizuddinRafay</org_name>
    <api_token>ghp_[redacted]8K</api_token>
  </api_auth>
  <api_parameters>
    <event_type>all</event_type>
  </api_parameters>
</github>


<!-- Policy monitoring -->
<rootcheck>
  <disabled>no</disabled>
  <check_files>yes</check_files>
```

Restarting Wazuh-manager.



Manager will be restarted

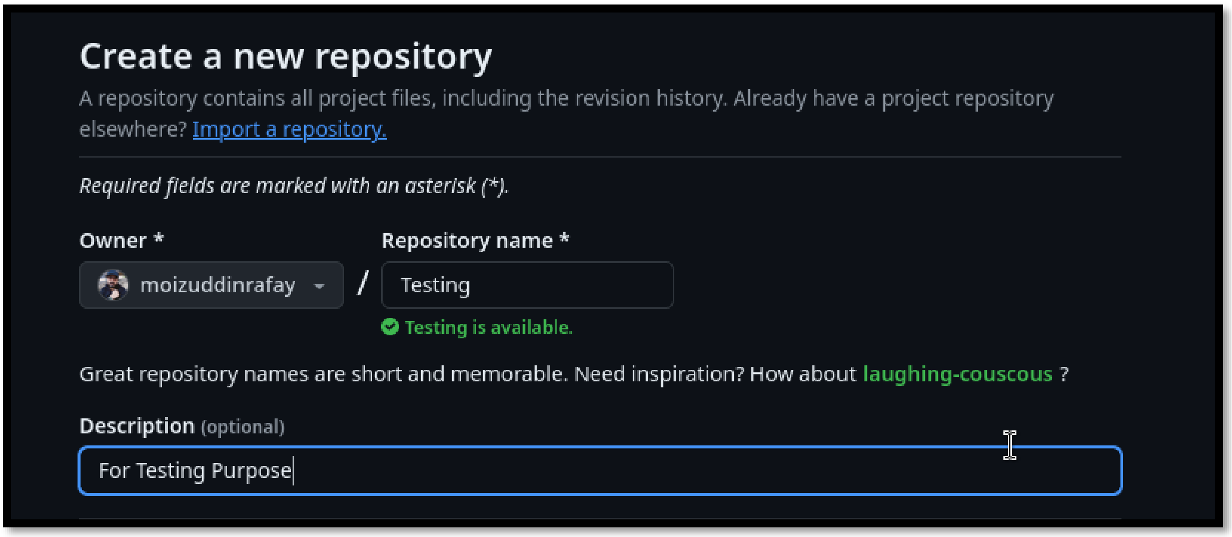
After restarting, there is no logs available.



File Edit View History Bookmarks Tools Help
Wazuh - Wazuh
Your Repositories
https://192.168.100.50/app/github#/overview/?tab=github&tabView=panels&_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:now-15m,to:now))&_a=(columns:!(_source),filters
120%
Defensive Security
Offensive Security
Learning
Torrents
Courses
Online Work
W.
GitHub
Dashboard
Panel
Events
Explore agent
Generate report
Search
DQL
Last 15 minutes
Show dates
Refresh
manager.name: wazuh-server
rule.groups: github
+ Add filter

There are no results for selected time range. Try another one.

Now we have to generate any type of events for confirm integration.



Create a new repository

A repository contains all project files, including the revision history. Already have a project repository elsewhere? Import a repository.

Required fields are marked with an asterisk (*).

Owner * moizuddinrafay / Repository name * Testing

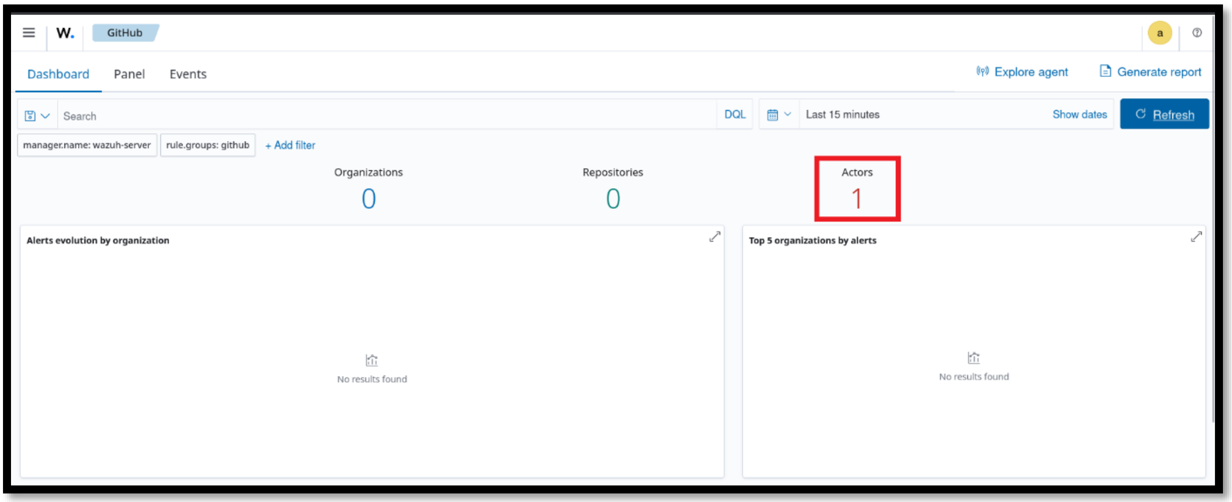
✓ Testing is available.

Great repository names are short and memorable. Need inspiration? How about laughing-couscous ?

Description (optional)

For Testing Purpose

Here you can see event.



Organizations 0

Repositories 0

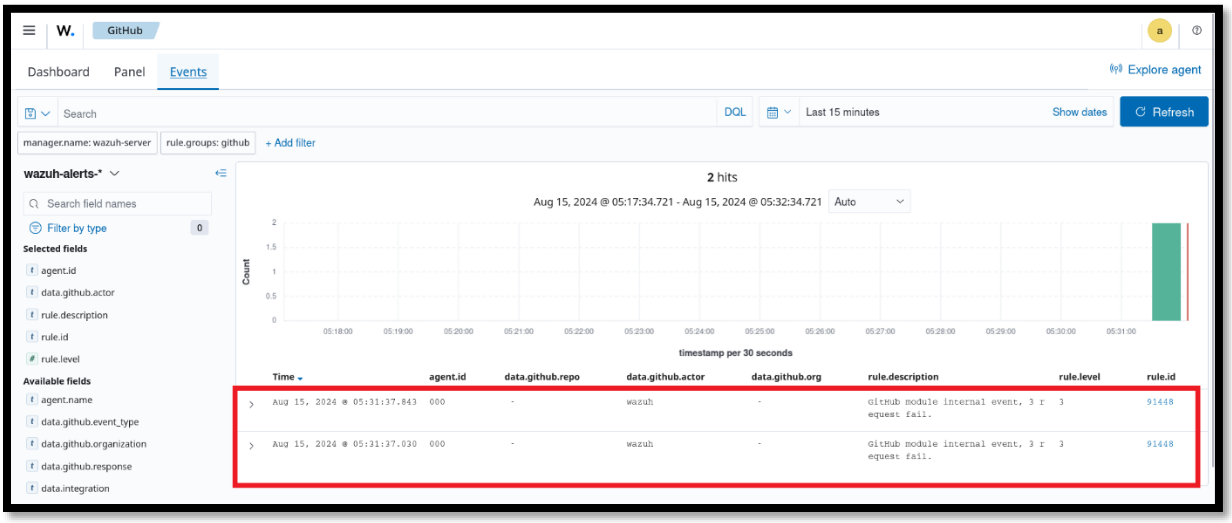
Actors 1

Alerts evolution by organization

No results found

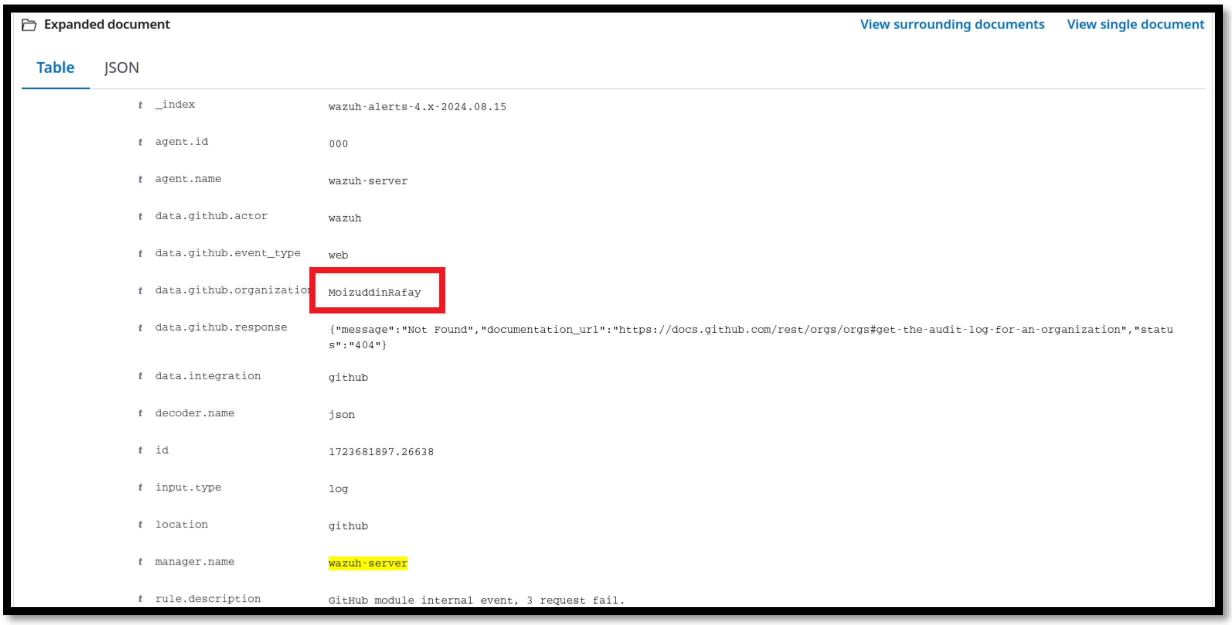
Top 5 organizations by alerts

No results found



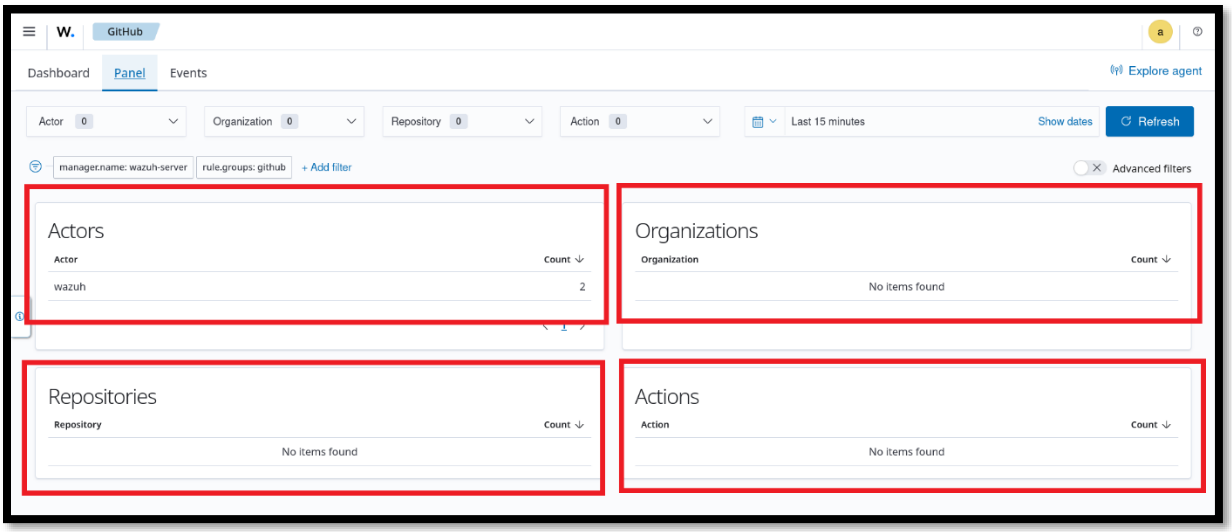
Time	agent.id	data.github.repo	data.github.actor	data.github.org	rule.description	rule.level	rule.id
Aug 15, 2024 @ 05:31:37.843	000	-	wazuh	-	GitHub module internal event, 3 request fail.	3	91448
Aug 15, 2024 @ 05:31:37.030	000	-	wazuh	-	GitHub module internal event, 3 request fail.	3	91448

Logs



t _index	wazuh-alerts-4.x-2024.08.15
t agent.id	000
t agent.name	wazuh-server
t data.github.actor	wazuh
t data.github.event_type	web
t data.github.organizatio	MoizuddinRafay
t data.github.response	{"message":"Not Found","documentation_url":"https://docs.github.com/rest/orgs/orgs#get-the-audit-log-for-an-organization","status":"404"}
t data.integration	github
t decoder.name	json
t id	1723681897.26638
t input.type	log
t location	github
t manager.name	wazuh-server
t rule.description	GitHub module internal event, 3 request fail.

We can get "Actors" "Organizations" "Repositories" "Action" events. My recommendation follow the link: https://documentation.wazuh.com/current/cloud-security/github/monitoring-github-activity.html to generates events.



Actors

Actor	Count
wazuh	2

Organizations

Organization	Count
No items found	

Repositories

Repository	Count
No items found	

Actions

Action	Count
No items found	

SUMMARY:

integrating Wazuh with GitHub, organizations can significantly enhance their DevSecOps capabilities, ensuring that their code repositories remain secure and compliant with organizational standards.

Regards

MUHAMMAD MOIZ UD DIN RAFAY
Ethical Hacker | Cyber Security Analyst

Need Training on Wazuh..?

Contact: +92-3004962168
Email: muhammadmoizuddinrafay@gmail.com
LinkedIn: www.linkedin.com/in/moizuddinrafay