Vajra Endpoint Detection and Response tool

Frontend Guide

Version 1.1
January 2024

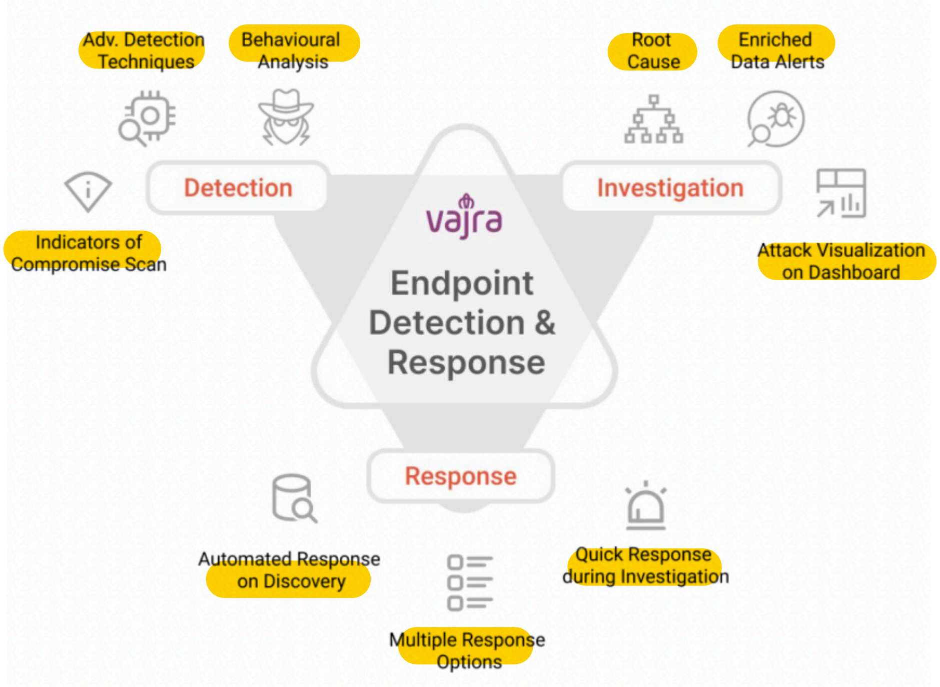
Introduction

Our Vajra Tool is a comprehensive solution designed to empower organizations and enterprises in their efforts to identify, investigate, and remediate security threats within their networks. The tool offers a wide range of features and capabilities that support threat detection, analysis, and response, making it an invaluable asset for enhancing cybersecurity posture. The two main functionalities are as follows:

- **Continuous Monitoring**: Process of continually gathering granular system information in and recording it to perform historical analysis on the data and to understand about activities performed in the past. System logs are critical for security analysis to detect malicious behaviors. Our tool enables gathering contextualized data which is important for getting better visibility if the system activities and correlating them for any malicious activity.

- **Proactive Threat Detection:** This is the process of systematically analyzing the system logs and detection for any malicious activity in real time. Our tool performs real-time threat detection using MITRE ATT&CK and GTFOBins frameworks and provides alerts. The tool has the capability for live threat hunting and provides remediation capabilities.

Features


Adv. Detection Techniques
Behavioural Analysis
Root Cause
Enriched Data Alerts
Detection
vajra
Endpoint Detection & Response
Investigation
Indicators of Compromise Scan
Attack Visualization on Dashboard
Response
Automated Response on Discovery
Quick Response during Investigation
Multiple Response Options

- Effective monitoring and detection of threats in real-time.
- Query information from the endpoint in the real-time.
- Vajra is able to interact with the system and even block threats in the future.
- Rule engine of Vajra is capable of analyzing and detecting threats in real time.

Tech Stack

Vajra Frontend has been developed using modern web technologies and libraries:

- React
- Bootstrap
- Material-UI (MUI)
- React Chart.js 2
- Typescript

Vajra Frontend uses API calls to NodeJS backend

Getting Started

Installation

To begin using Vajra Tool, follow the installation instructions provided in the documentation. Once the installation process is complete, you can access the UI for the tool through a web browser.

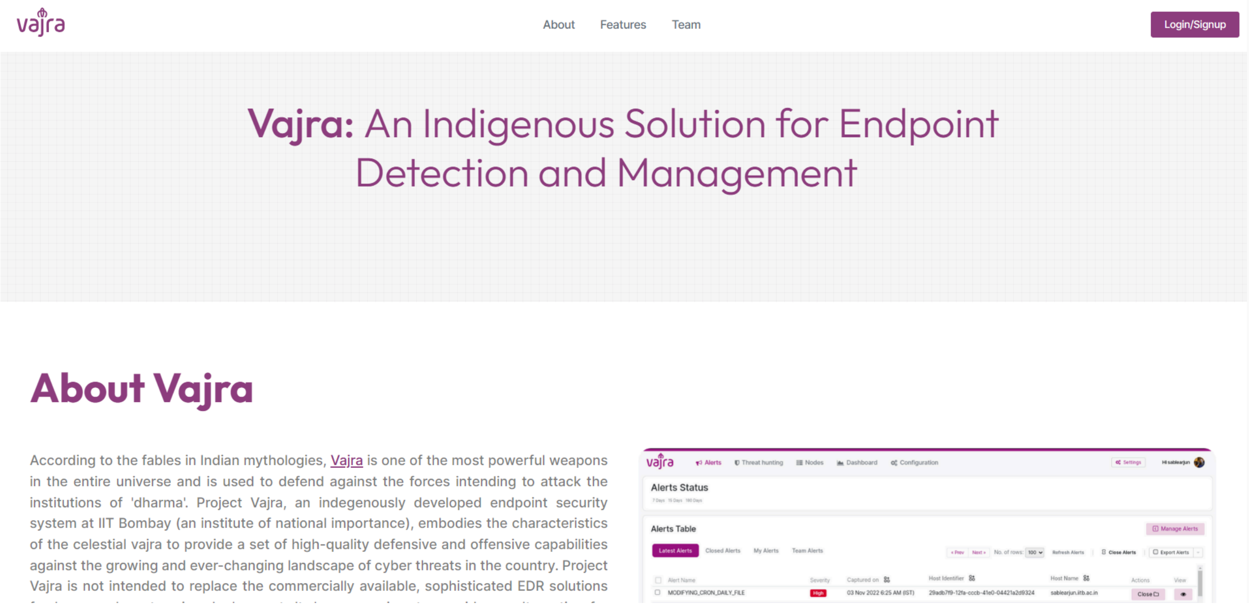
Website Structure

```
Website
├── Home Page
├── Login Page
├── Nodes Page
│   └── Node View Page
│       ├── Details Tab
│       ├── Graph Tab
│       ├── Container List Tab
│       └── Run Query Tab
├── Alerts Page
│   └── Alert View Page
│       ├── MetaData Tab
│       ├── Detection Graph Tab
│       ├── Signal Table Tab
│       └── Reference Log Tab
├── Threat Hunting Page
├── Dashboard Page
├── Configuration Page
├── Rules Page
│   ├── Python Rules Tab
│   ├── Rule Builder Tab
│   ├── Yara Files Tab
│   ├── IP Files Tab
│   └── Display Backend Rules Tab
└── Settings
    ├── Overview Tab
    ├── Data Purging Tab
    ├── Email Settings Tab
    ├── User Settings Tab
    ├── Permissions Tab
    └── Group Settings Tab
```

Navigating the Interface

Home Page

The home page serves as the central hub for introduction, features, and team of the tool.



Vajra: An Indigenous Solution for Endpoint Detection and Management

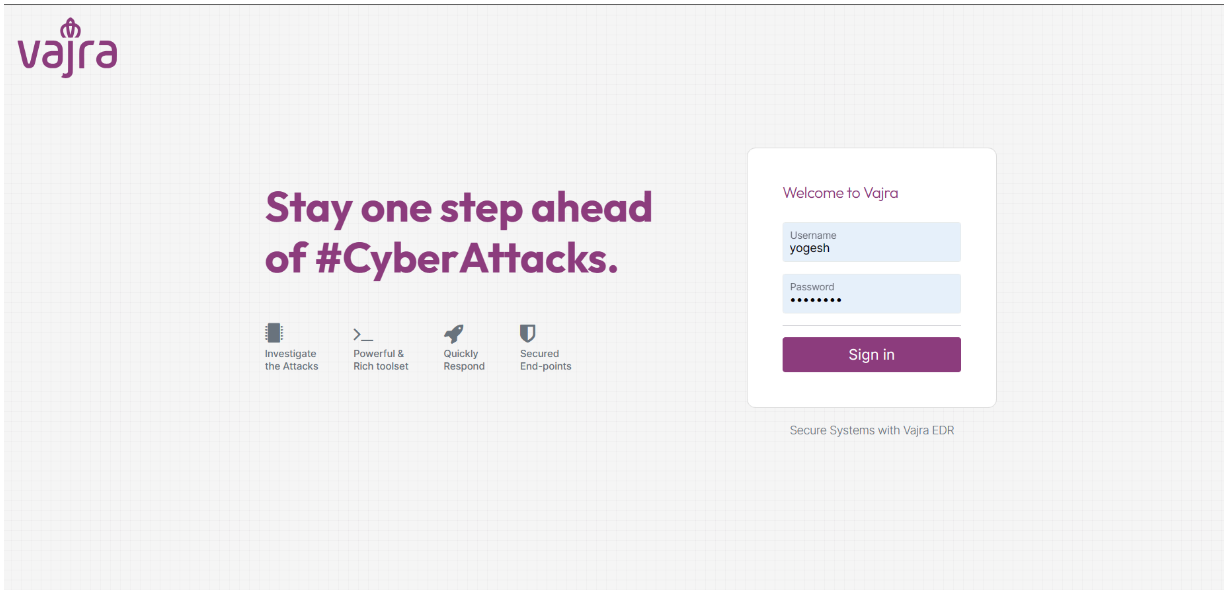
About Vajra

According to the fables in Indian mythologies, Vajra is one of the most powerful weapons in the entire universe and is used to defend against the forces intending to attack the institutions of 'dharma'. Project Vajra, an indegenously developed endpoint security system at IIT Bombay (an institute of national importance), embodies the characteristics of the celestial vajra to provide a set of high-quality defensive and offensive capabilities against the growing and ever-changing landscape of cyber threats in the country. Project Vajra is not intended to replace the commercially available, sophisticated EDR solutions

□	Alert Name	Severity	Captured on	Host Identifier	Host Name	Actions	View
□	MODIFYING_CRON_DAILY_FILE	High	03 Nov 2022 6:25 AM (IST)	29adb7f9-12fa-cccb-41e0-04421a2d9324	sablearjun.iitb.ac.in	Close	👁

Login

Upon accessing the Vajra Tool, log in using your credentials. The login page ensures secure access to the tool's features and functionalities.



Stay one step ahead of #CyberAttacks.

Welcome to Vajra

Username: yogesh

Password: ••••••••

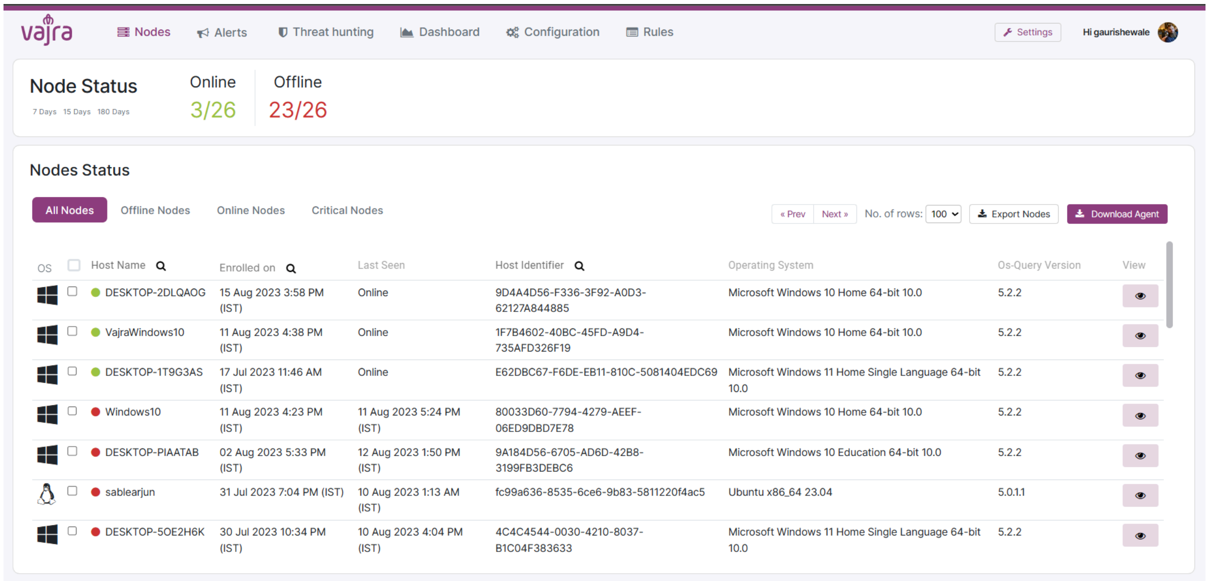
Secure Systems with Vajra EDR

Login Page APIs:

/auth/login	Used for logging in the user

Nodes Page

The nodes page allows users to manage network nodes. It provides an overview of all connected nodes and their status.



Node Status

7 Days 15 Days 180 Days

Online 3/26

Offline 23/26

Nodes Status

No. of rows: 100

OS	□	Host Name	Enrolled on	Last Seen	Host Identifier	Operating System	Os-Query Version	View
	□	● DESKTOP-2DLQAOG	15 Aug 2023 3:58 PM (IST)	Online	9D4A4D56-F336-3F92-A0D3-62127A844885	Microsoft Windows 10 Home 64-bit 10.0	5.2.2	
	□	● VajraWindows10	11 Aug 2023 4:38 PM (IST)	Online	1F7B4602-40BC-45FD-A9D4-735AFD326F19	Microsoft Windows 10 Home 64-bit 10.0	5.2.2	
	□	● DESKTOP-1T9G3AS	17 Jul 2023 11:46 AM (IST)	Online	E62DBC67-F6DE-EB11-810C-5081404EDC69	Microsoft Windows 11 Home Single Language 64-bit 10.0	5.2.2	
	□	● Windows10	11 Aug 2023 4:23 PM (IST)	11 Aug 2023 5:24 PM (IST)	80033D60-7794-4279-AEEF-06ED9DBD7E78	Microsoft Windows 10 Home 64-bit 10.0	5.2.2	
	□	● DESKTOP-PIAATAB	02 Aug 2023 5:33 PM (IST)	12 Aug 2023 1:50 PM (IST)	9A184D56-6705-AD6D-42B8-3199FB3DEBC6	Microsoft Windows 10 Education 64-bit 10.0	5.2.2	
	□	● sablearjun	31 Jul 2023 7:04 PM (IST)	10 Aug 2023 1:13 AM (IST)	fc99a636-8535-6ce6-9b83-5811220f4ac5	Ubuntu x86_64 23.04	5.0.1.1	
	□	● DESKTOP-5OE2H6K	30 Jul 2023 10:34 PM (IST)	10 Aug 2023 4:04 PM (IST)	4C4C4544-0030-4210-8037-B1C04F383633	Microsoft Windows 11 Home Single Language 64-bit 10.0	5.2.2	

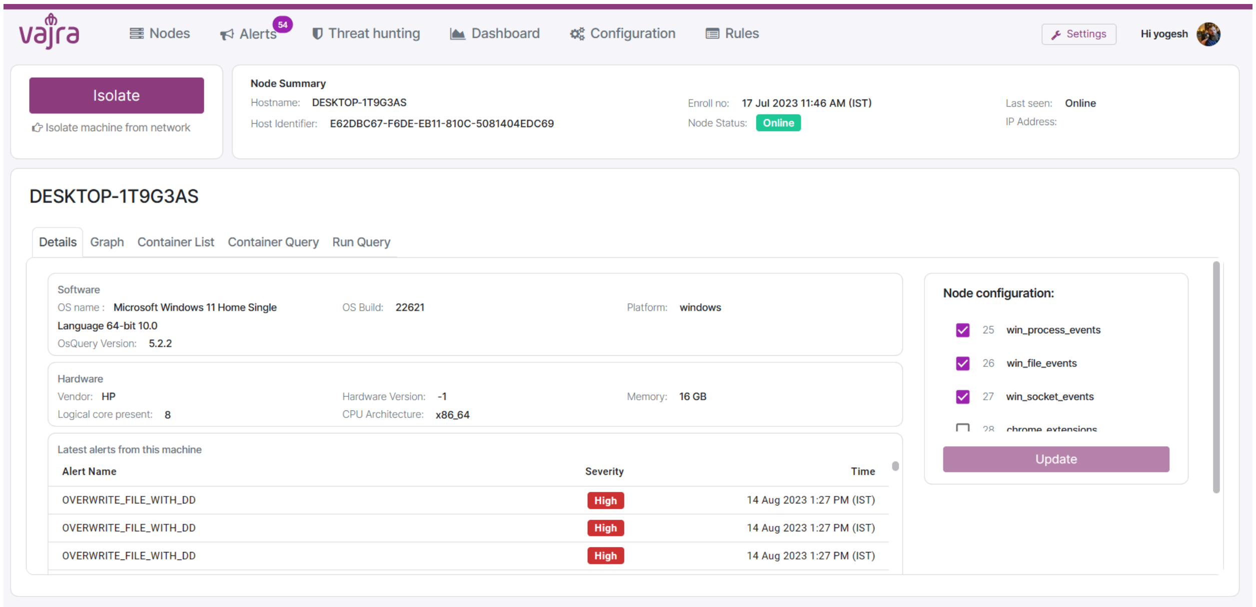
Node Page APIs:

/node/list	Used for fetching list of all nodes and their status

Diving Deep: Node Management

- Node View Page Details

This page provides detailed information about a specific node in the network. It includes essential node attributes and status indicators. We have the option to isolate the node from network as well as re-enroll the node in network.



Node Summary
Hostname: DESKTOP-1T9G3AS
Host Identifier: E62DBC67-F6DE-EB11-810C-5081404EDC69
Enroll no: 17 Jul 2023 11:46 AM (IST)
Node Status: Online
Last seen: Online
IP Address:

DESKTOP-1T9G3AS

Software
OS name : Microsoft Windows 11 Home Single Language 64-bit 10.0
OS Build: 22621
Platform: windows
OsQuery Version: 5.2.2

Hardware
Vendor: HP
Hardware Version: -1
Memory: 16 GB
Logical core present: 8
CPU Architecture: x86_64

Node configuration:

☑ 25 win_process_events
☑ 26 win_file_events
☑ 27 win_socket_events
□ 28 chrome_extensions

Latest alerts from this machine

Alert Name	Severity	Time
OVERWRITE_FILE_WITH_DD	High	14 Aug 2023 1:27 PM (IST)
OVERWRITE_FILE_WITH_DD	High	14 Aug 2023 1:27 PM (IST)
OVERWRITE_FILE_WITH_DD	High	14 Aug 2023 1:27 PM (IST)

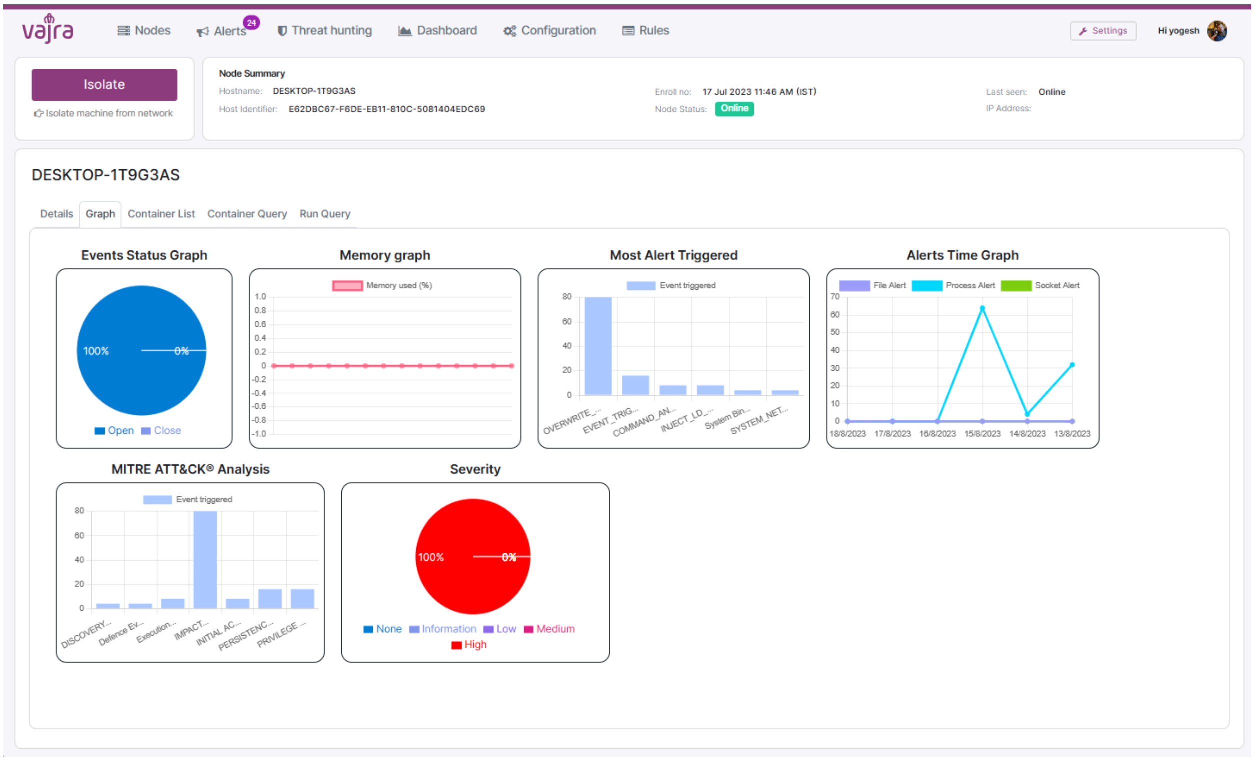
APIs used:

/node/query	Used for fetching list of all nodes and their status in Details Tab
/node/config	Used for updating node config
/node/memory_health	For displaying memory health graph in Graph Tab
/config/list	Used for fetching all configurations

/dashboard/events_count	For displaying open close events info in Graph Tab
/dashboard/alert_count	For displaying top 10 alerts and their count in Graph Tab
/dashboard/weekly_alert_count	For displaying weekly alert count on the node in Graph tab
/dashboard/mitre_analysis	For displaying mitre analysis attacks and their quantity in Graph Tab
/dashboard/severity_count	For displaying severity - count values in Graph Tab

- Graph Tab

The graph tab presents visual representation alerts on selected node status, assisting in identifying potential attacks.



Node Summary

Hostname: DESKTOP-1T9G3AS

Host Identifier: E62DBC67-F6DE-EB11-810C-5081404EDC69

Enroll no: 17 Jul 2023 11:46 AM (IST)

Node Status: Online

Last seen: Online

IP Address:

DESKTOP-1T9G3AS

- Container List Tab

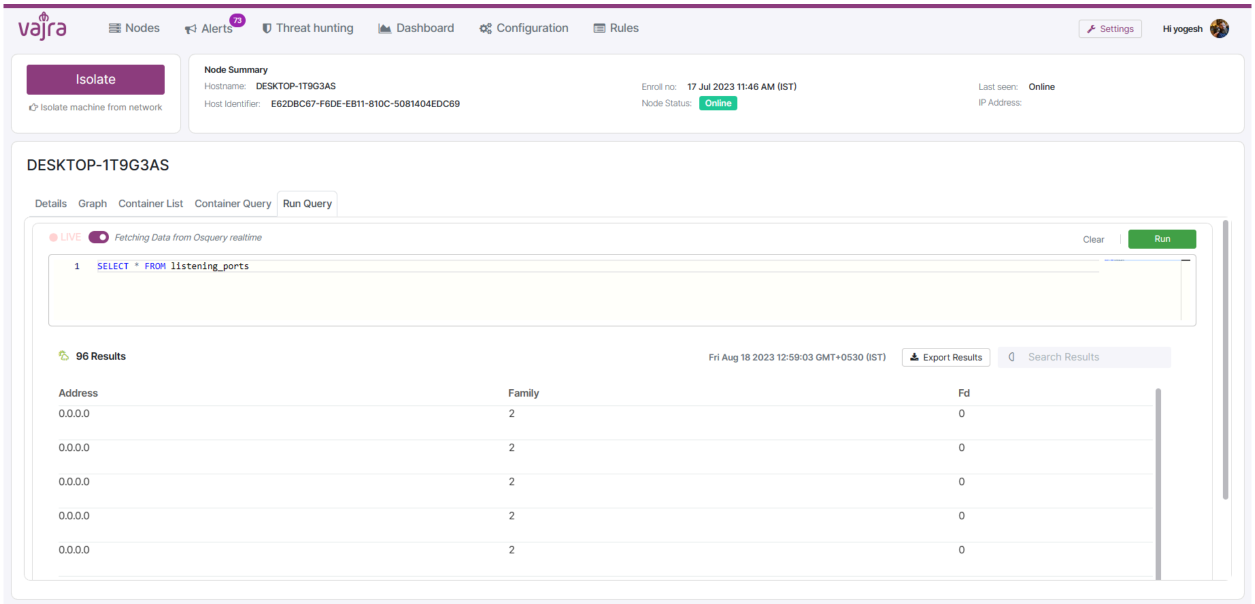
For containerized environments, this tab displays a list of containers associated with the selected node.

- Container Query Tab

Users can execute queries on active containers in this tab, allowing for detailed analysis.

- Run Query Tab

This tab lets users run custom SQL queries on the selected node's live data for deeper investigation. This feature can be availed via the Threat Hunting page as well.



Node Summary
Hostname: DESKTOP-1T9G3AS
Host Identifier: E62DBC67-F6DE-EB11-810C-5081404EDC69
Enroll no: 17 Jul 2023 11:46 AM (IST)
Node Status: Online
Last seen: Online
IP Address:

DESKTOP-1T9G3AS

```
SELECT * FROM listening_ports
```

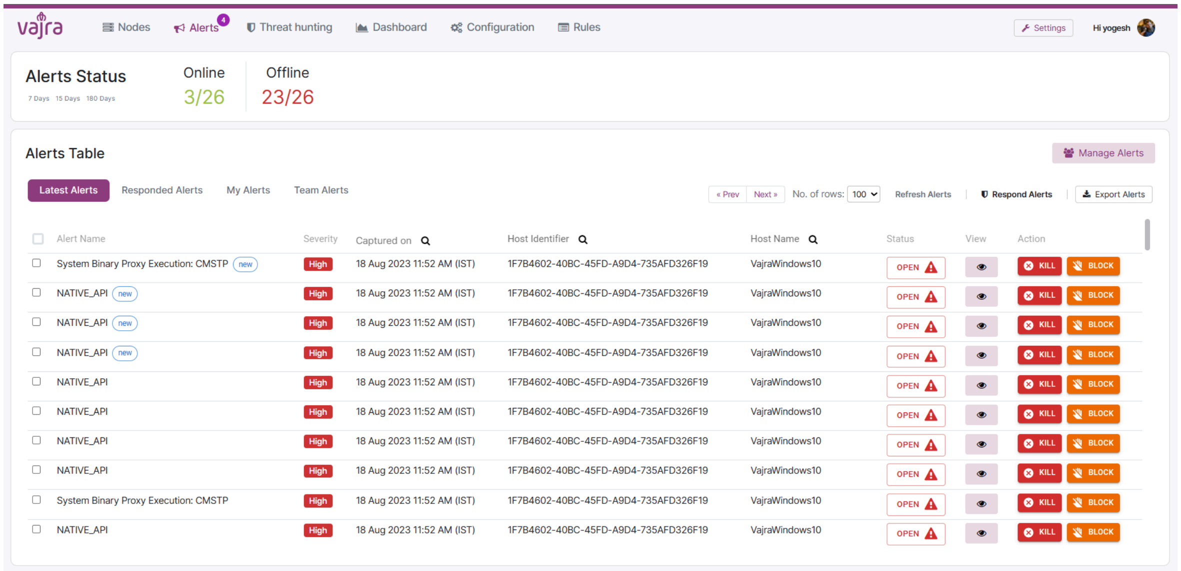
96 Results

Fri Aug 18 2023 12:59:03 GMT+0530 (IST)

Address	Family	Fd
0.0.0.0	2	0
0.0.0.0	2	0
0.0.0.0	2	0
0.0.0.0	2	0
0.0.0.0	2	0

Alerts Page

The alerts page displays a list of generated security alerts. It facilitates the monitoring and investigation of potential threats.



Alerts Status

7 Days 15 Days 180 Days

Online 3/26

Offline 23/26

Alerts Table

□	Alert Name	Severity	Captured on	Host Identifier	Host Name	Status	View	Action
□	System Binary Proxy Execution: CMSTP new	High	18 Aug 2023 11:52 AM (IST)	1F7B4602-40BC-45FD-A9D4-735AFD326F19	VajraWindows10	OPEN		KILL BLOCK
□	NATIVE_API new	High	18 Aug 2023 11:52 AM (IST)	1F7B4602-40BC-45FD-A9D4-735AFD326F19	VajraWindows10	OPEN		KILL BLOCK
□	NATIVE_API new	High	18 Aug 2023 11:52 AM (IST)	1F7B4602-40BC-45FD-A9D4-735AFD326F19	VajraWindows10	OPEN		KILL BLOCK
□	NATIVE_API new	High	18 Aug 2023 11:52 AM (IST)	1F7B4602-40BC-45FD-A9D4-735AFD326F19	VajraWindows10	OPEN		KILL BLOCK
□	NATIVE_API	High	18 Aug 2023 11:52 AM (IST)	1F7B4602-40BC-45FD-A9D4-735AFD326F19	VajraWindows10	OPEN		KILL BLOCK
□	NATIVE_API	High	18 Aug 2023 11:52 AM (IST)	1F7B4602-40BC-45FD-A9D4-735AFD326F19	VajraWindows10	OPEN		KILL BLOCK
□	NATIVE_API	High	18 Aug 2023 11:52 AM (IST)	1F7B4602-40BC-45FD-A9D4-735AFD326F19	VajraWindows10	OPEN		KILL BLOCK
□	NATIVE_API	High	18 Aug 2023 11:52 AM (IST)	1F7B4602-40BC-45FD-A9D4-735AFD326F19	VajraWindows10	OPEN		KILL BLOCK
□	System Binary Proxy Execution: CMSTP	High	18 Aug 2023 11:52 AM (IST)	1F7B4602-40BC-45FD-A9D4-735AFD326F19	VajraWindows10	OPEN		KILL BLOCK
□	NATIVE_API	High	18 Aug 2023 11:52 AM (IST)	1F7B4602-40BC-45FD-A9D4-735AFD326F19	VajraWindows10	OPEN		KILL BLOCK

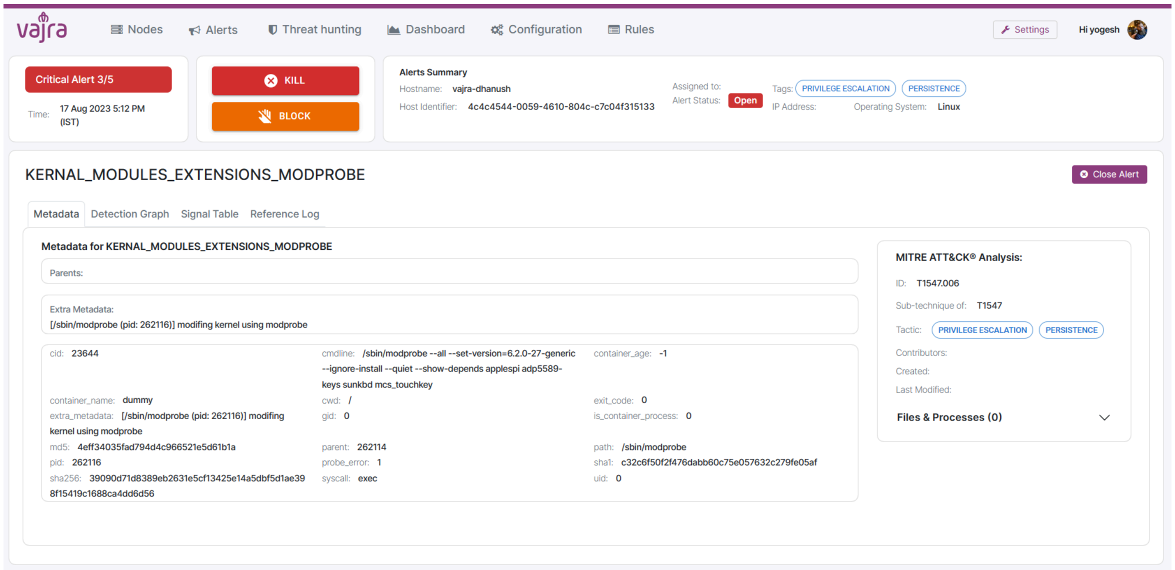
Alert Page APIs:

/events/list	Used for fetching list of all events and their status

Diving Deep: Alert Management

- Alert View Page Metadata

This page offers in-depth information about a specific alert, aiding in investigation and response. Users can view the metadata associated with an alert, providing contextual information for analysis.



Critical Alert 3/5

Time: 17 Aug 2023 5:12 PM (IST)

Alerts Summary

Hostname: vajra-dhanush

Host Identifier: 4c4c4544-0059-4610-804c-c7c04f315133

Assigned to:

Alert Status: Open

Tags: PRIVILEGE ESCALATION PERSISTENCE

IP Address:

Operating System: Linux

KERNAL_MODULES_EXTENSIONS_MODPROBE

Metadata for KERNAL_MODULES_EXTENSIONS_MODPROBE

Parents:

Extra Metadata:
[/sbin/modprobe (pid: 262116)] modifing kernel using modprobe

cid: 23644

cmdline: /sbin/modprobe --all --set-version=6.2.0-27-generic --ignore-install --quiet --show-depends applespi adp5589-keys sunkbd mcs_touchkey

container_age: -1

container_name: dummy

cwd: /

exit_code: 0

extra_metadata: [/sbin/modprobe (pid: 262116)] modifing kernel using modprobe

gid: 0

is_container_process: 0

md5: 4eff34035fad794d4c966521e5d61b1a

parent: 262114

path: /sbin/modprobe

pid: 262116

probe_error: 1

sha1: c32c6f50f2f476dabb60c75e057632c279fe05af

sha256: 39090d71d8389eb2631e5cf13425e14a5dbf5d1ae398f15419c1688ca4dd6d56

syscall: exec

uid: 0

MITRE ATT&CK® Analysis:

ID: T1547.006

Sub-technique of: T1547

Tactic: PRIVILEGE ESCALATION PERSISTENCE

Contributors:

Created:

Last Modified:

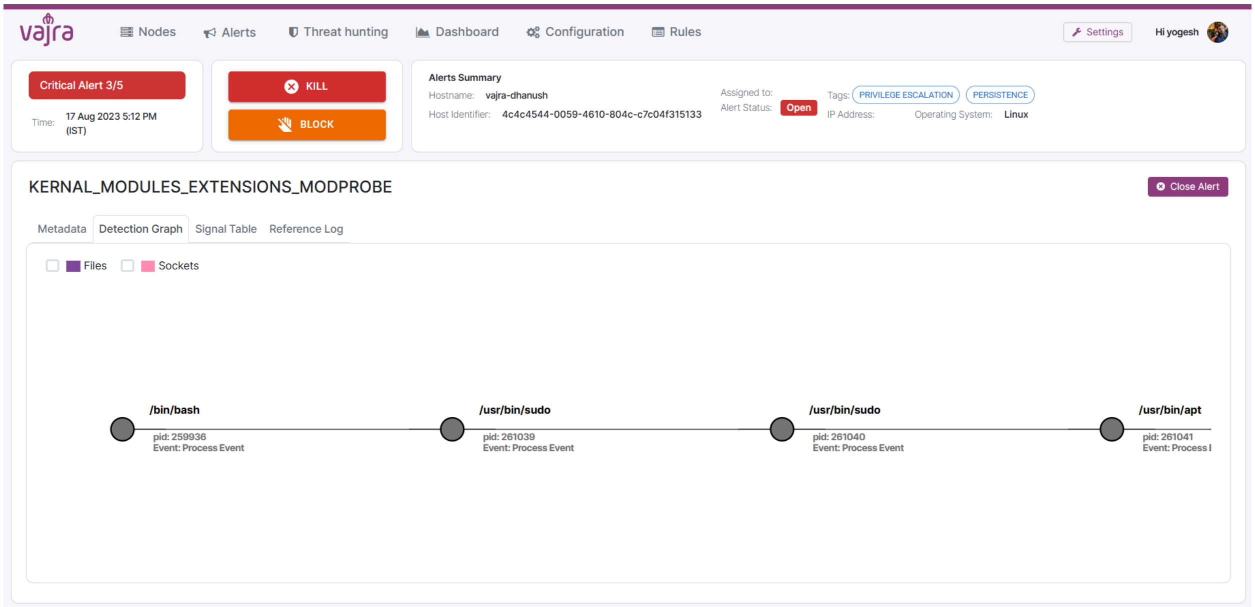
Files & Processes (0)

APIs:

/api/assign_event	Used for assigning event to user
/event/graph	Used for generating graph and signal table of event to be displayed in Detection Graph Tab and Signal Table Graph
/event/query	Used for fetching node related data
/event/update	Used for updating the event status
/node/log_list	Used for displaying log list in Reference Log

- Detection Graph Tab

A visual representation of an alert's detection path is presented here, helping users understand the alert's origin.



Critical Alert 3/5

Time: 17 Aug 2023 5:12 PM (IST)

Alerts Summary

Hostname: vajra-dhanush

Host Identifier: 4c4c4544-0059-4610-804c-c7c04f315133

Assigned to:

Alert Status: Open

Tags: PRIVILEGE ESCALATION PERSISTENCE

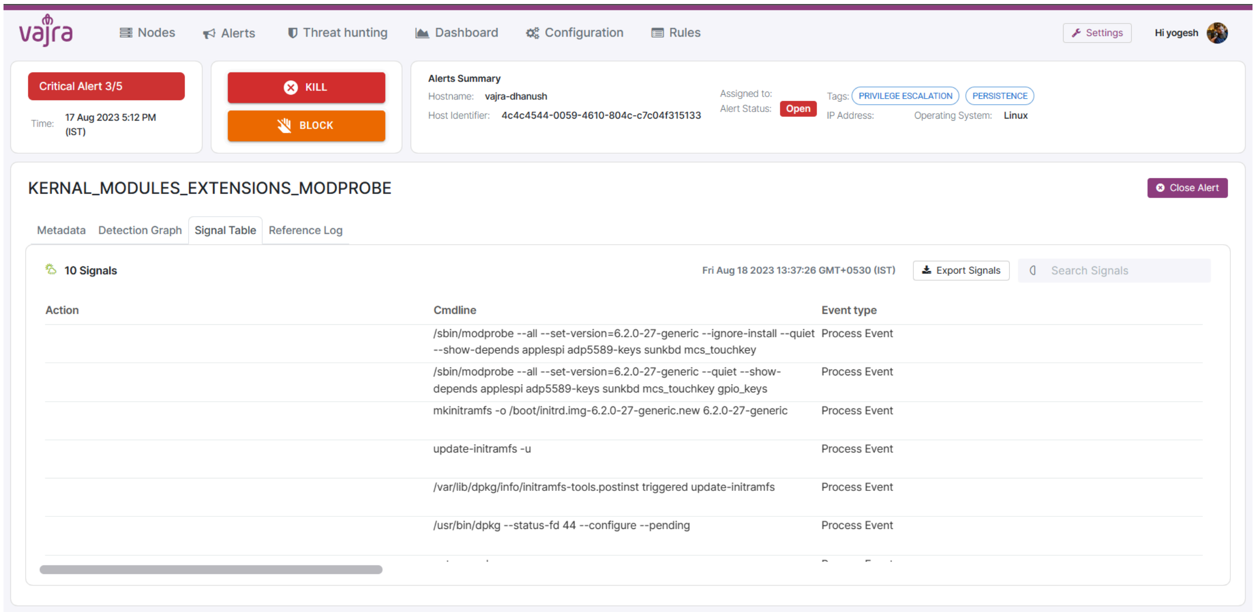
IP Address:

Operating System: Linux

KERNAL_MODULES_EXTENSIONS_MODPROBE

- Signal Table Tab

Users can examine the raw signals and data related to an alert in tabular form.



Critical Alert 3/5

Time: 17 Aug 2023 5:12 PM (IST)

Alerts Summary

Hostname: vajra-dhanush

Host Identifier: 4c4c4544-0059-4610-804c-c7c04f315133

Assigned to:

Alert Status: Open

Tags: PRIVILEGE ESCALATION PERSISTENCE

IP Address:

Operating System: Linux

KERNAL_MODULES_EXTENSIONS_MODPROBE

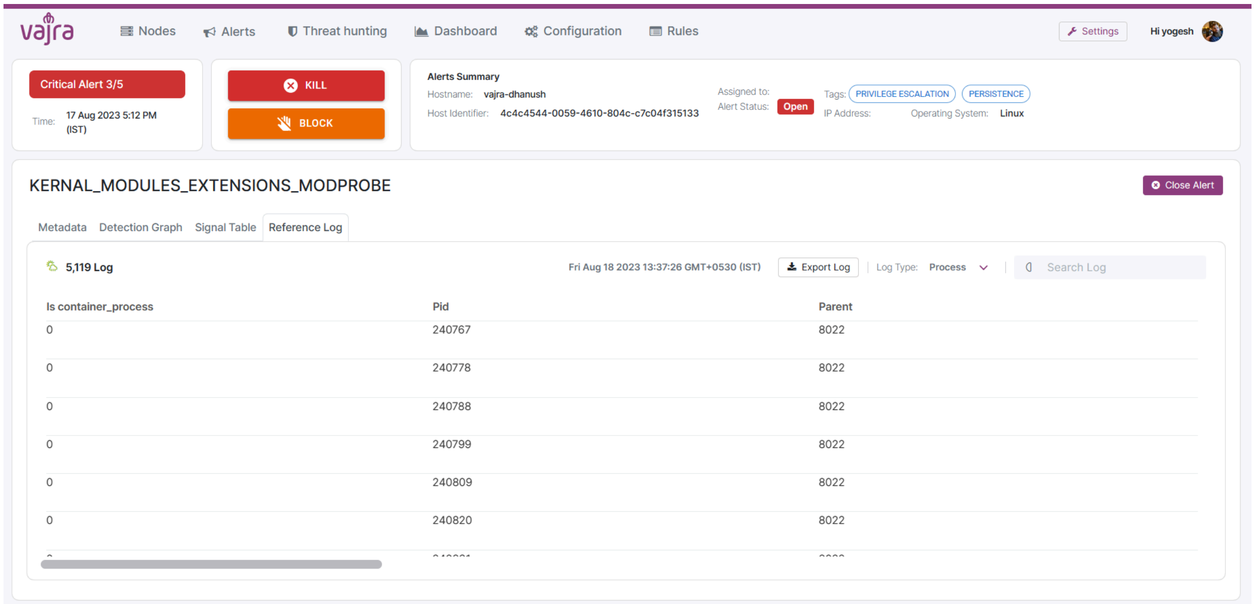
10 Signals

Fri Aug 18 2023 13:37:26 GMT+0530 (IST)

Action	Cmdline	Event type
	/sbin/modprobe --all --set-version=6.2.0-27-generic --ignore-install --quiet --show-depends applespi adp5589-keys sunkbd mcs_touchkey	Process Event
	/sbin/modprobe --all --set-version=6.2.0-27-generic --quiet --show-depends applespi adp5589-keys sunkbd mcs_touchkey gpio_keys	Process Event
	mkinitramfs -o /boot/initrd.img-6.2.0-27-generic.new 6.2.0-27-generic	Process Event
	update-initramfs -u	Process Event
	/var/lib/dpkg/info/initramfs-tools.postinst triggered update-initramfs	Process Event
	/usr/bin/dpkg --status-fd 44 --configure --pending	Process Event

- Reference Log Tab

For additional context, this tab displays relevant logs (± 10 mins) related to the alert in question.



Critical Alert 3/5

Time: 17 Aug 2023 5:12 PM (IST)

Alerts Summary

Hostname: vajra-dhanush

Host Identifier: 4c4c4544-0059-4610-804c-c7c04f315133

Assigned to:

Alert Status: Open

Tags: PRIVILEGE ESCALATION PERSISTENCE

IP Address:

Operating System: Linux

KERNAL_MODULES_EXTENSIONS_MODPROBE

5,119 Log

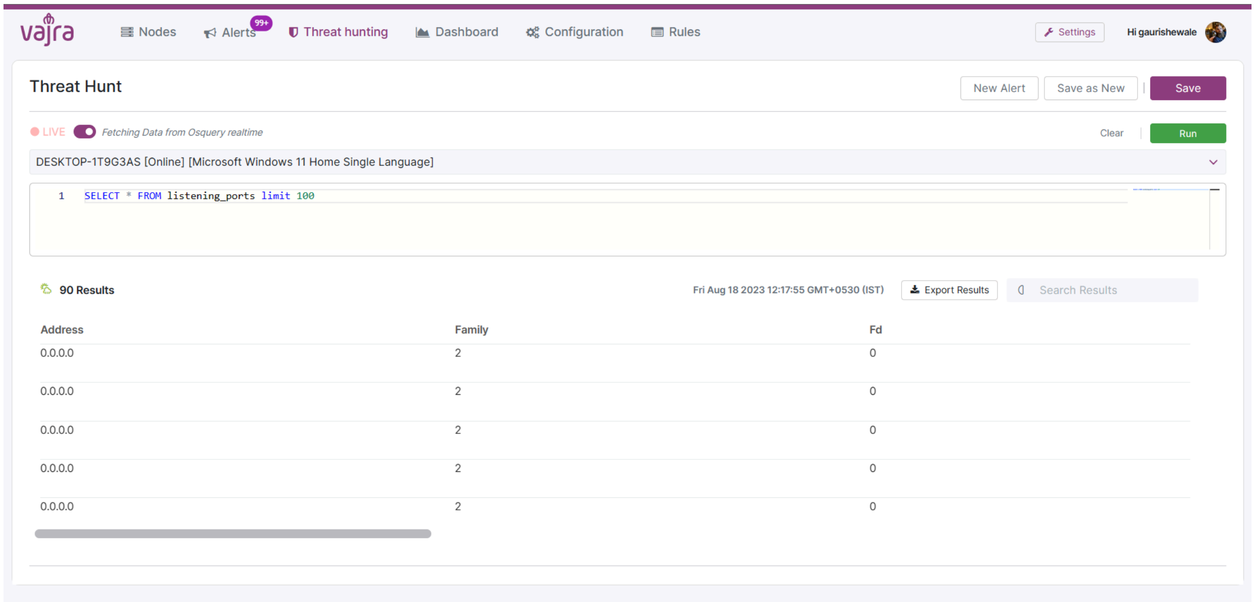
Fri Aug 18 2023 13:37:26 GMT+0530 (IST)

Log Type: Process

Is container_process	Pid	Parent
0	240767	8022
0	240778	8022
0	240788	8022
0	240799	8022
0	240809	8022
0	240820	8022

Threat Hunting Page

The threat hunting page enables advanced users to proactively search for potential threats and execute live SQL queries on the online nodes.



Threat Hunt

LIVE *Fetching Data from Osquery realtime*

DESKTOP-1T9G3AS [Online] [Microsoft Windows 11 Home Single Language]

```
SELECT * FROM listening_ports limit 100
```

90 Results

Fri Aug 18 2023 12:17:55 GMT+0530 (IST)

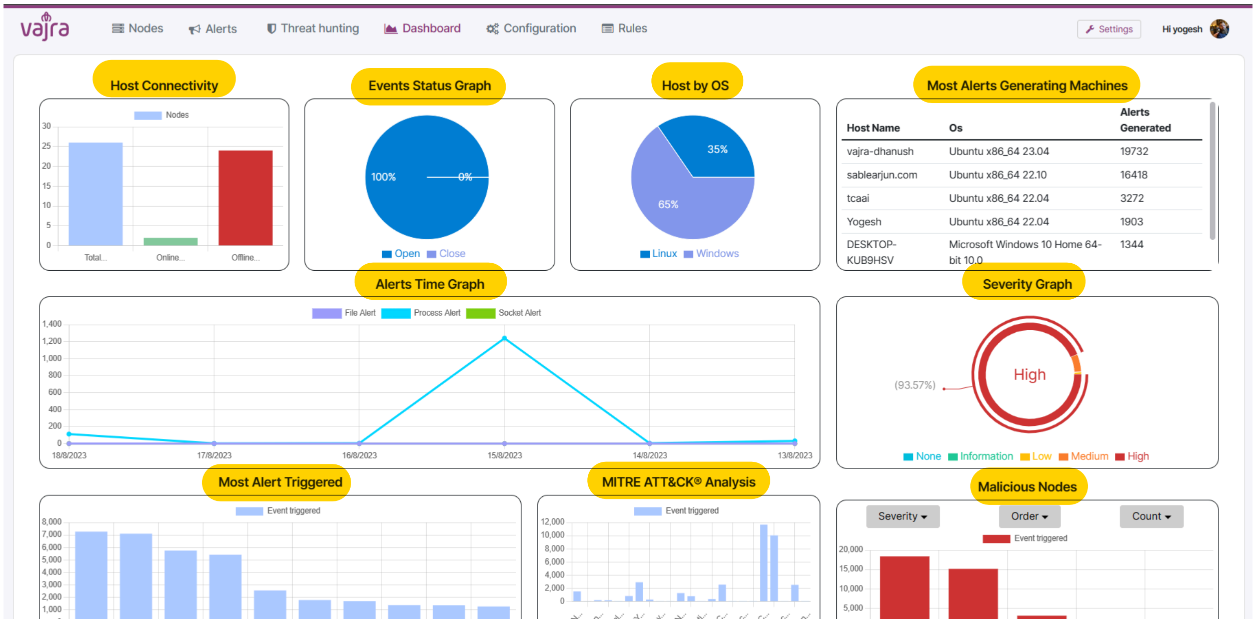
Address	Family	Fd
0.0.0.0	2	0
0.0.0.0	2	0
0.0.0.0	2	0
0.0.0.0	2	0
0.0.0.0	2	0

Threat Hunting Page APIs:

/node/list	Used for fetching list of all nodes and their status
/node/historical_data	Used for running input query on database
/scheduled_queries/schedule	Used for scheduling live queries
/scheduled_queries/status	Used for checking query status
/scheduled_queries/response	Used for fetching query results

Dashboard

The dashboard offers various visualizations and reports, providing a quick snapshot of the node's security status.



Host Name	Os	Alerts Generated
vajra-dhanush	Ubuntu x86_64 23.04	19732
sablearjun.com	Ubuntu x86_64 22.10	16418
tcaai	Ubuntu x86_64 22.04	3272
Yogesh	Ubuntu x86_64 22.04	1903
DESKTOP-KUB9HSV	Microsoft Windows 10 Home 64-bit 10.0	1344

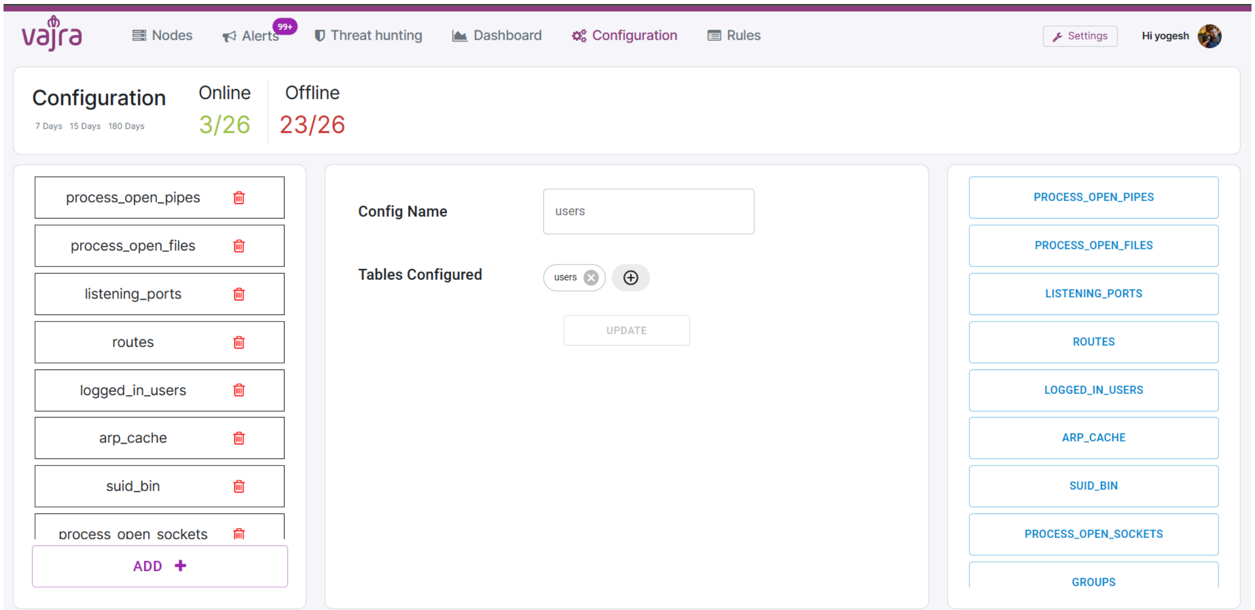
Dashboard APIs:

/dashboard/events_count	For displaying open close events information pie graph

/dashboard/os_count	For displaying OS count in Pie Graph
/dashboard/alert_count	For displaying top 10 alerts and their count in Bar Graph
/dashboard/weekly_alert_count	For displaying weekly alert count on the node in Line graph
/dashboard/mitre_analysis	For displaying mitre analysis attacks and their quantity in Bar Graph
/dashboard/severity_count	For displaying severity - count values in Pie Graph
/dashboard/high_risk_count	For displaying list of top 5 alert generating machines
/dashboard/node_alert_count	For displaying top 5 node information and alert severity in Bar graph

Configuration

The configuration section allows users to customize configuration tables, which can then be selected for each node to monitor data.


Config Name: users

Tables Configured: users

Configuration Page APIs:

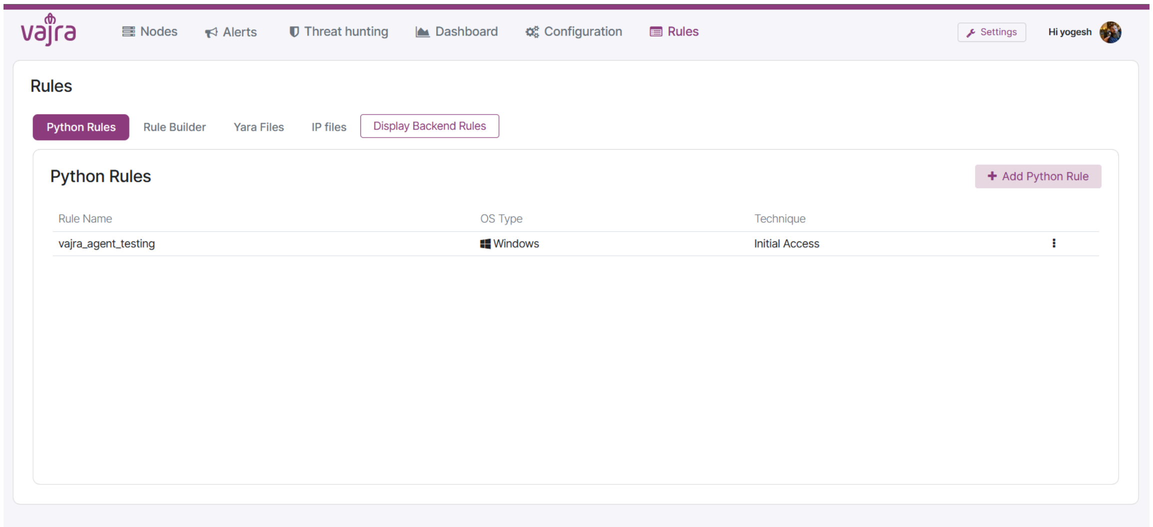
/config/list	Used for fetching list of configurations
/config/add	Used for adding a config query
/config/update	Used for updating a config query
/config/delete	Used for deleting a config query
/config/table_name	Used for fetching tables present in config queries

Rules

This page provides an overview of configured rules for threat detection and response.

- Python Rules Tab

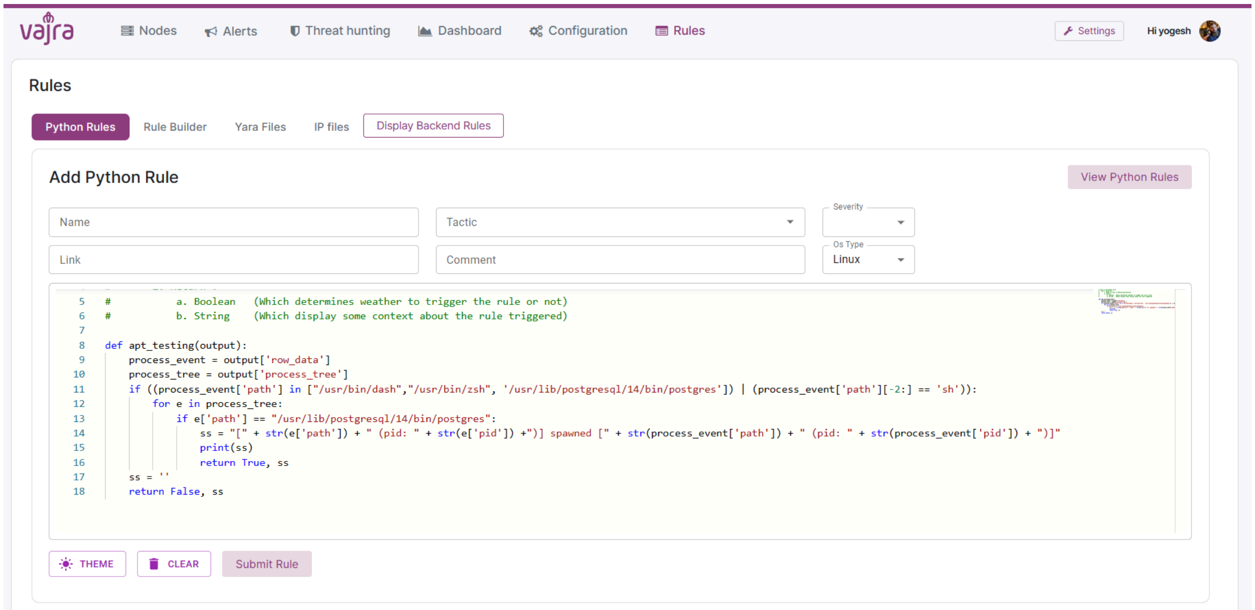
Users can create and manage custom detection rules using Python scripts.



Rules

Python Rules

Rule Name	OS Type	Technique
vajra_agent_testing	Windows	Initial Access



Os Type: Linux

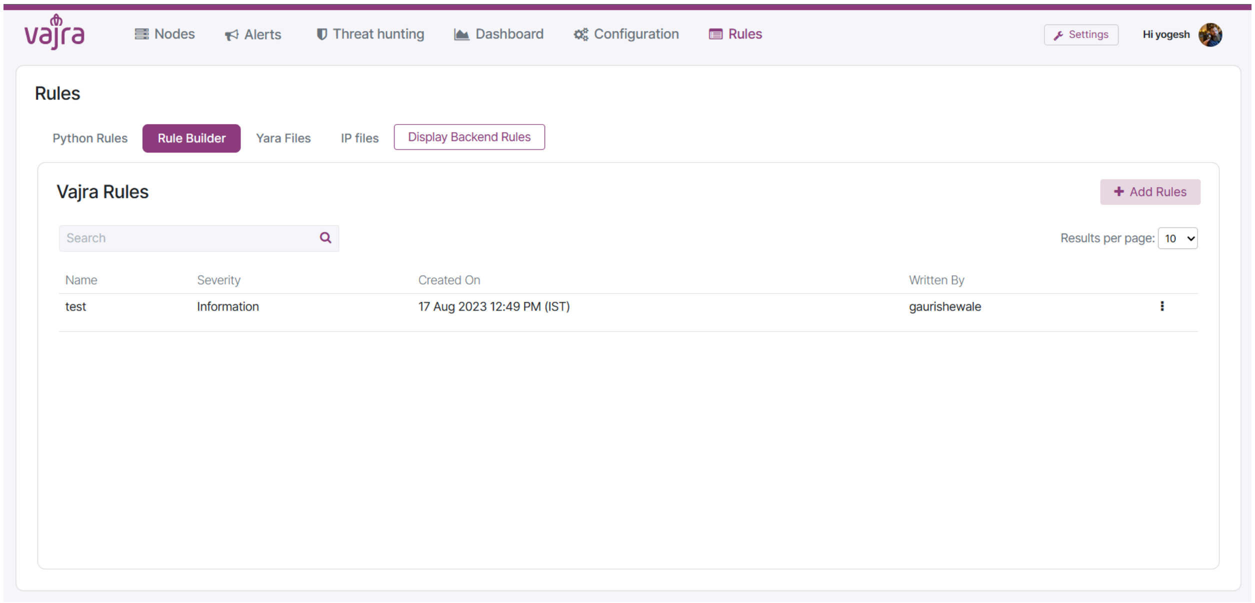
```
#           a. Boolean   (Which determines weather to trigger the rule or not)
#           b. String    (Which display some context about the rule triggered)

def apt_testing(output):
    process_event = output['row_data']
    process_tree = output['process_tree']
    if ((process_event['path'] in ["/usr/bin/dash","/usr/bin/zsh", '/usr/lib/postgresql/14/bin/postgres']) | (process_event['path'][-2:] == 'sh')):
        for e in process_tree:
            if e['path'] == "/usr/lib/postgresql/14/bin/postgres":
                ss = "[" + str(e['path']) + " (pid: " + str(e['pid']) +")] spawned [" + str(process_event['path']) + " (pid: " + str(process_event['pid']) + ")]"
                print(ss)
                return True, ss
    ss = ''
    return False, ss
```

APIs Used :

/python_rules/list_python_rule	Used for fetching list of all python rules
/python_rules/add_python_rule	Used for adding a new python rule
/python_rules/update_python_rule	Used for updating an existing python rule
/python_rules/delete_python_rule	Used for deleting an existing python rule

- Rule Builder Tab

For those without coding experience, this tab offers a graphical interface to design rules.

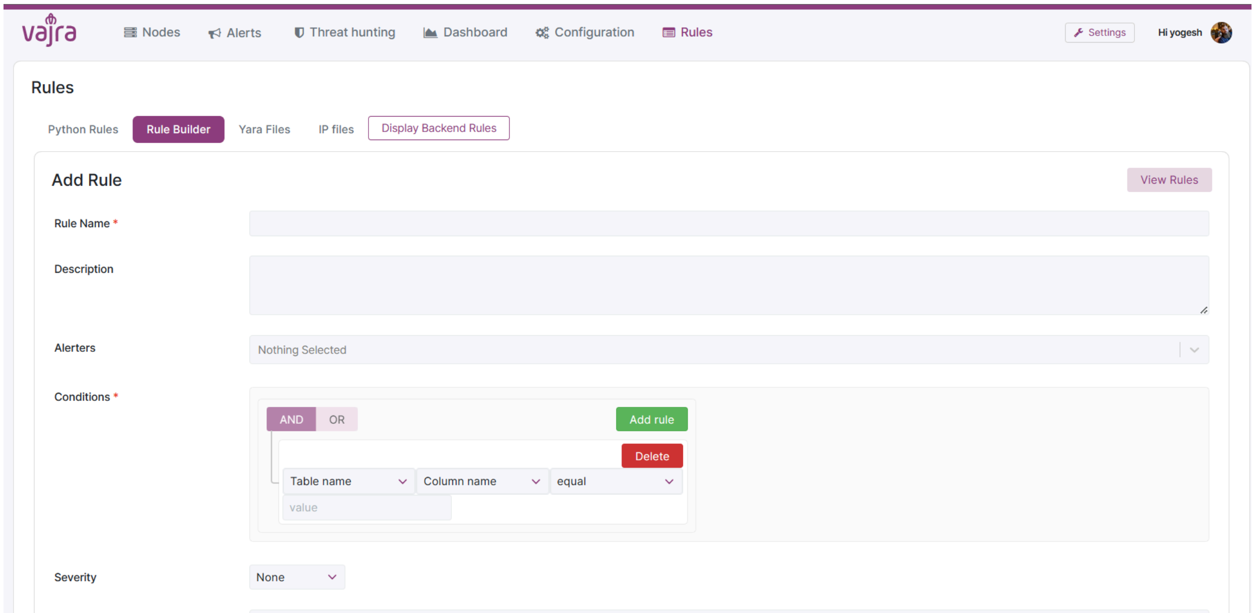


Rules

Vajra Rules

Results per page: 10

Name	Severity	Created On	Written By
test	Information	17 Aug 2023 12:49 PM (IST)	gaurishewale



Rules

Add Rule

Rule Name *

Description

Alerters: Nothing Selected

Conditions *

Table name | Column name | equal

value

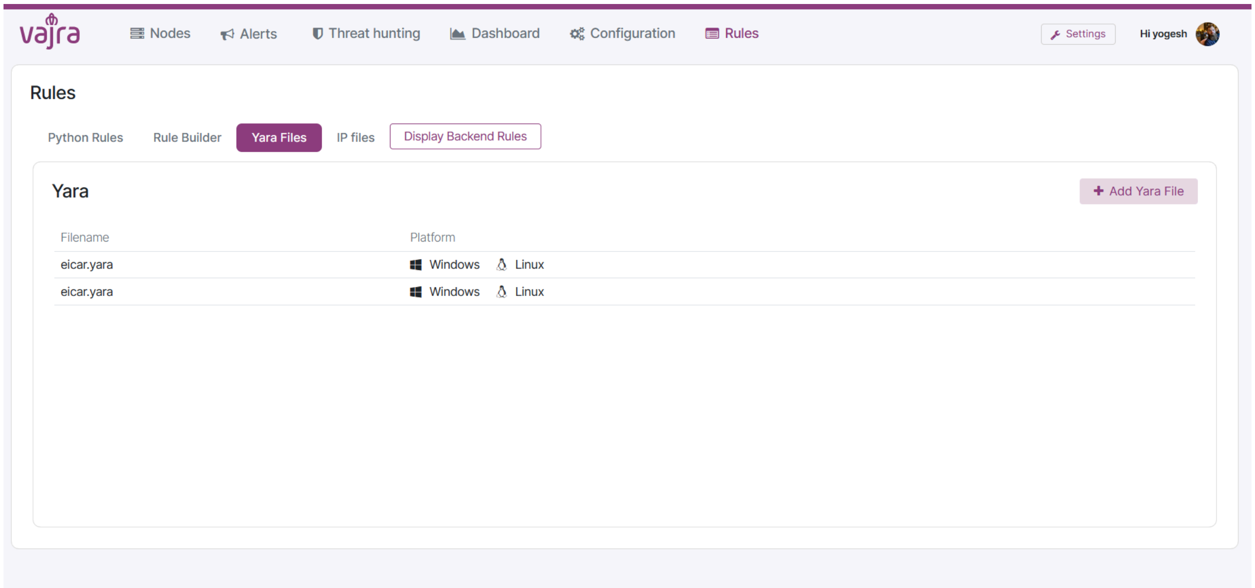
Severity: None

APIs Used :

/rule_builder/rule_list	Used for fetching list of all rule builder rules
/rule_builder/rule_add	Used for adding a new rule builder rule
/rule_builder/rule_updae	Used for updating an existing rule builder rule
/rule_builder/rule_delete	Used for deleting an existing rule builder rule

- Yara Files Tab

Manage and upload Yara rule files for enhanced threat detection.



Rules

Yara

Filename	Platform
eicar.yara	Windows Linux
eicar.yara	Windows Linux

- IP Files Tab

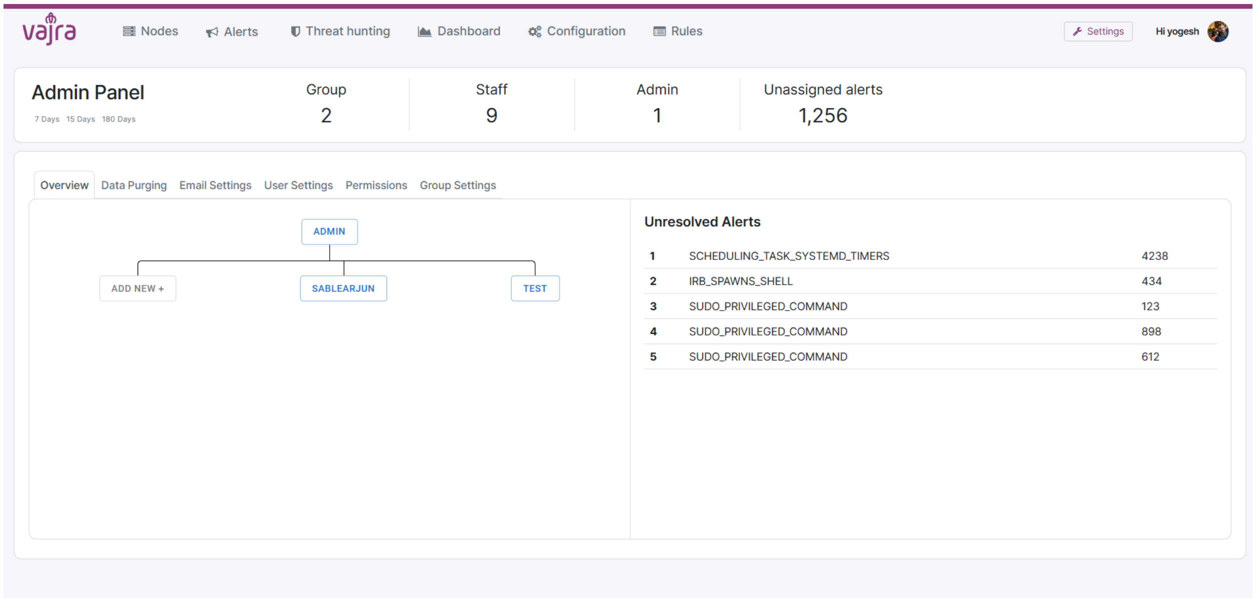
Upload and manage lists of Malicious IP addresses file for enhancing the alert status

- Display Backend Rules

View backend rules that power the tool's detection mechanisms.

Settings

The settings section allows users to configure various tool preferences, integrations, and system parameters.



Admin Panel

Group	Staff	Admin	Unassigned alerts
2	9	1	1,256

Unresolved Alerts

1	SCHEDULING_TASK_SYSTEMD_TIMERS	4238
2	IRB_SPAWNS_SHELL	434
3	SUDO_PRIVILEGED_COMMAND	123
4	SUDO_PRIVILEGED_COMMAND	898
5	SUDO_PRIVILEGED_COMMAND	612

APIs Used :

/api/user_list	Used for fetching list of all users
/auth/register	Used for adding a new user
/settings/manual_purge	Used for updating Manual Purge settings
/settings/data_retention	Used for specifying data retention settings

API Reference

This API reference guide provides details about the various modules and endpoints within the Vajra Tool's API. Each module focuses on a specific aspect of the tool's functionality, such as node management, event handling, user authentication, and more. Additionally, examples of query samples are provided to help you understand how to interact with each endpoint effectively.

This guide consists of 10 modules where each module contains endpoints and example query sample

- /node for Node APIs
- /event for Event APIs
- /auth for User Auth APIs
- /user for User management APIs
- /config for Config APIs
- /dashboard for Dashboard APIs
- /threat_hunting for Threat Hunting APIs
- /python_rules for Python Rule APIs
- /scheduled_queries for Scheduled Query APIs
- /rule_builder for Rule builder APIs

More Details can be found here

Local Machine Setup

[It is assumed that NPM Node and Git is already present in machine]

1. **Install the repository file**

git clone https://github.com/VajraSecurity/VajraSystemApp.git

cd VajraSystemApp

2. **Install the dependencies**

```
npm install
```

3. **Create copy of env.production.local and rename it to env.development.local**

Set

```
REACT_APP_SERVER_URL="http://localhost:4000"
```

4. **Run the application**

```
npm run start
```

Overview

Vajra Tool provides a robust suite of capabilities that aid organizations and enterprises in identifying, investigating, and remediating security threats within their networks. With its comprehensive features and user-friendly interface, the tool equips security teams with the necessary tools to bolster their cybersecurity efforts.