WAZUH OPEN SOURCE SECURITY PLATFORM

REDBACK OPERATIONS

OWNER OF DOCUMENT:

Name:	Team:	Position:
Lachlan Harrison	Cyber Security Team - Blue Team	Junior

Last Modified: September 8th 2024

Redback Operations

wazuh.

CONTENTS

Redback Operations

wazuh.

MODULE 1:
CAPABILITIES OF WAZUH

CAPABILITIES

- Wazuh is a free and open-source tool utilized for many reasons/features which will be further discussed.
- While utilizing this tool, opportunities for learning present itself.
- Easy to deploy and is accessible on our documentation.
- Can send alerts via a preferred method. (Email, Slack)
- A SIEM tool. (Security Information and Event Management)
- Only requires a Linux server (Ubuntu, Debian) due to its simplicity along with another computer to monitor its output.
- Can also be implemented onto a docker.
- Relatively easy deployment method on VirtualBox servers. (Accessible on our documentation)
- Provides a unique learning experience in areas of securing devices and mitigating vulnerabilities.
- System requirements are not too large.

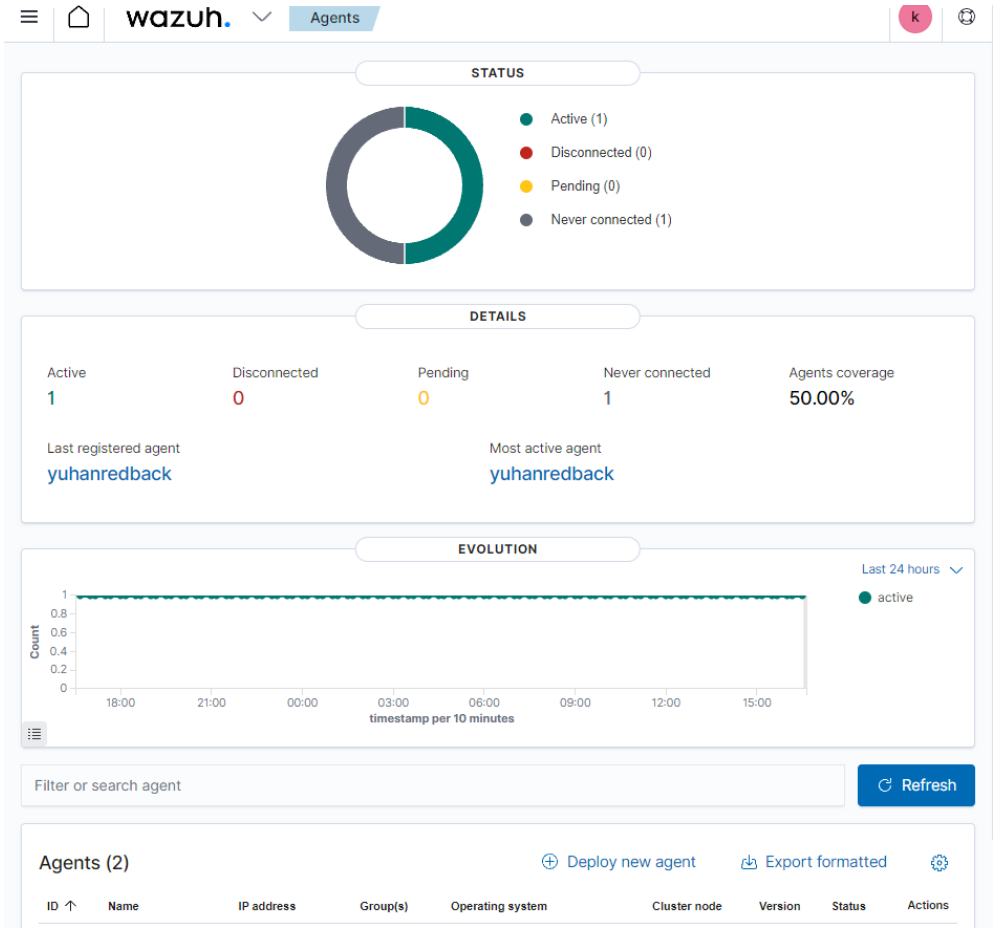
Link to Implementation of Wazuh: https://redback-operations.github.io/redback-documentation/docs/cybersecurity/research/ids-and-wazuh/wazuh-implementation-guide
Link to Implementation of Wazuh on Virtual Machine: https://redback-operations.github.io/redback-documentation/docs/cybersecurity/research/ids-and-wazuh/deploying-wazuh

SYSTEM REQUIREMENTS:

MINIMUM:		RECOMMENDED:	
RAM	CPU	RAM	CPU
2GB	2 Cores	4GB	8 Cores

SIMPLISTIC USER INTERFACE:

- The Wazuh User Interface is relatively easy to navigate.
- Once an agent is connected, analysis can begin.
- User Interface informs many different security alerts, MITRE techniques, Authentication failures/success.



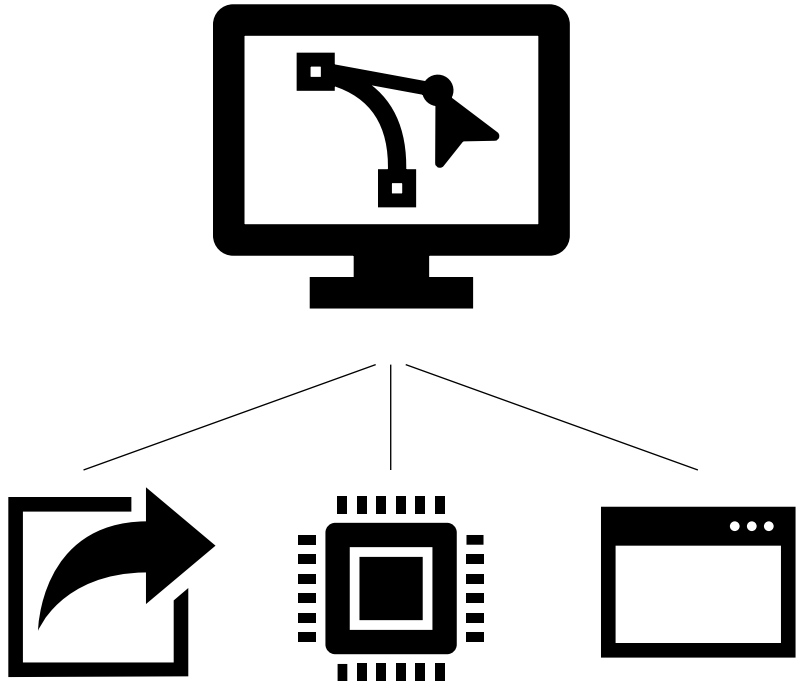
Note: This is the Dashboard of Redback Operations where we only have two agents deployed as of current document creation

Redback Operations

wazuh.

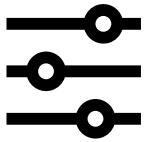
SUMMARISING MODULE:

- In this module we covered:
- The benefits and capabilities that Wazuh can offer.
- The system requirements to run Wazuh.
- The simplicity of the UI.



MODULE 2:
WHAT CAN WE LEARN FROM WAZUH?

AREAS OF LEARNING



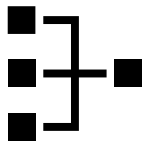
- Security configurations

- Vulnerabilities

- MITRE ATT&CK Framework

- Compliance Standards

- Cyber Attacks



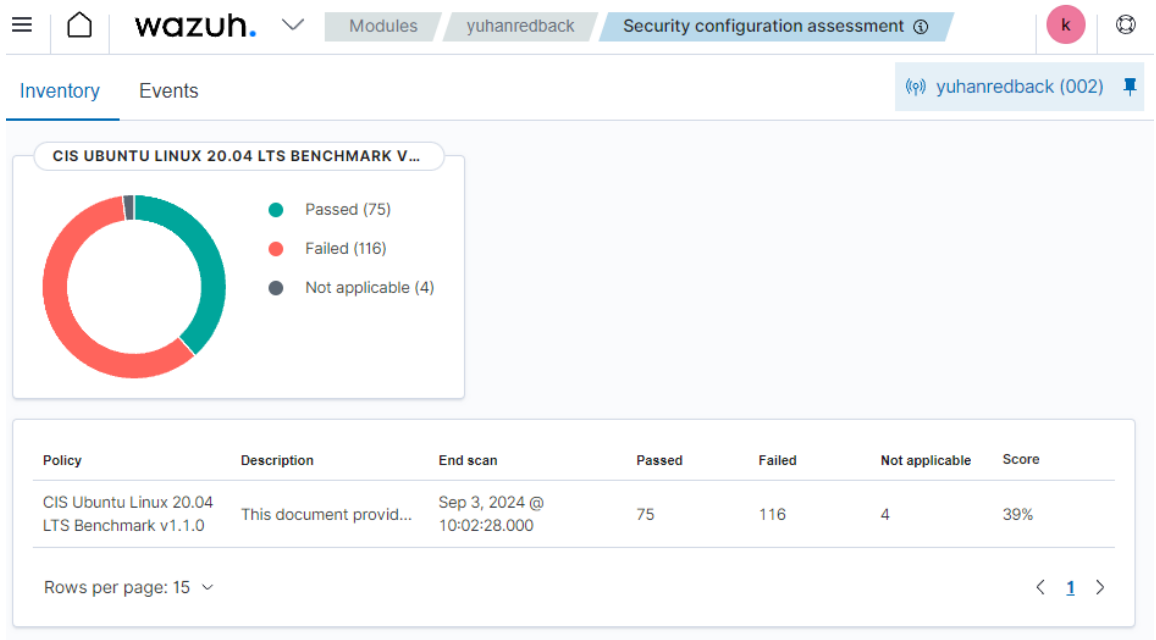
- Linked Agents

Note: There are many areas of learning opportunities within Wazuh, these are just some of the main areas. Some are also bundled together as well.

MODULE 2 – WHAT CAN WE LEARN FROM WAZUH?

SECURITY CONFIGURATIONS

- Any security configurations that can be implemented Wazuh tells the user so that they can enhance security on their device.
- Also known as misconfigurations. Users may not intentionally configure these.
- Wazuh provides how to configure these misconfigurations properly.
- Secure Configuration Assessments (SCA) inform users of why they need to follow certain actions to reduce risk of compromise and keep themselves protected.

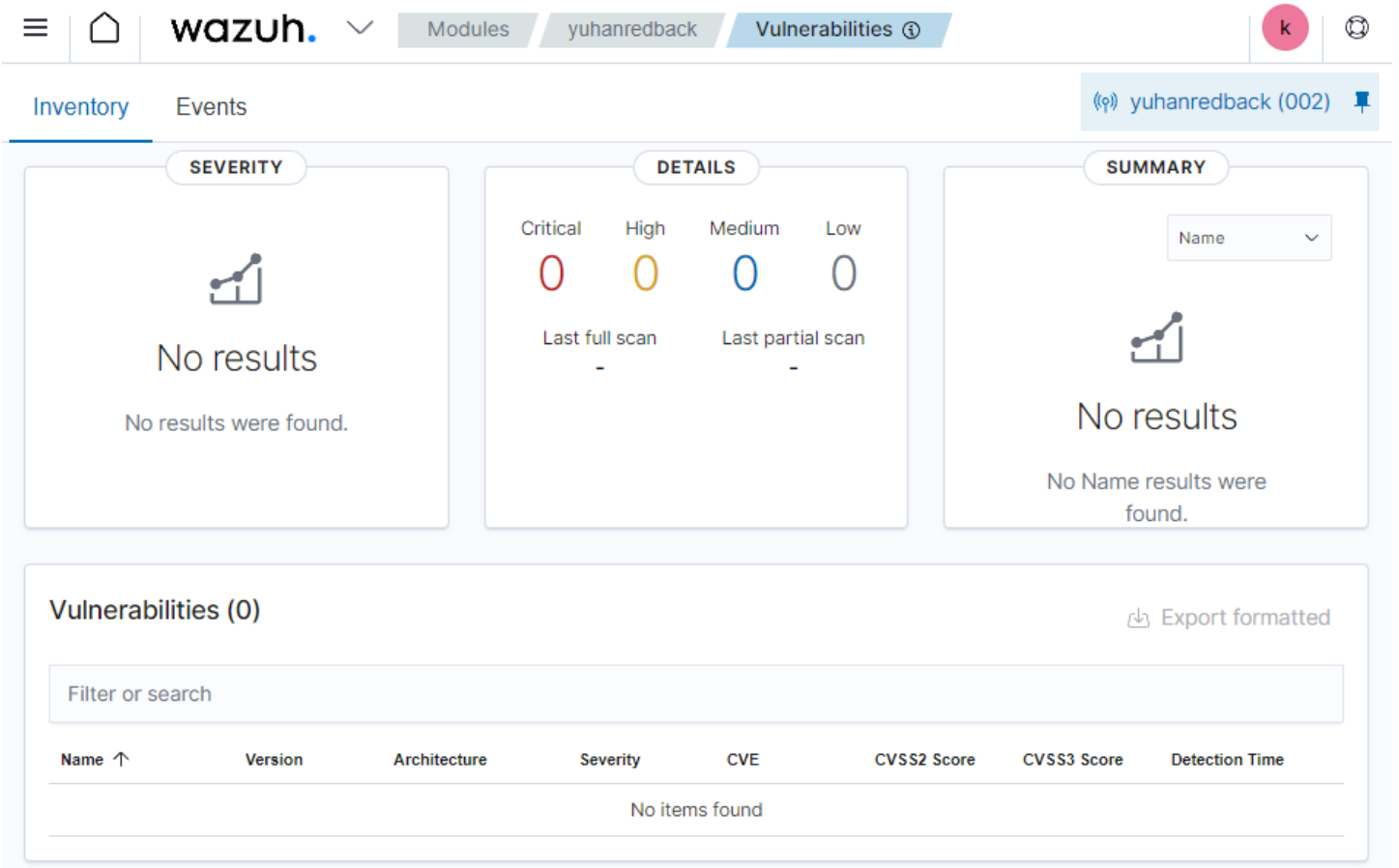


Redback Operations

wazuh.

VULNERABILITIES

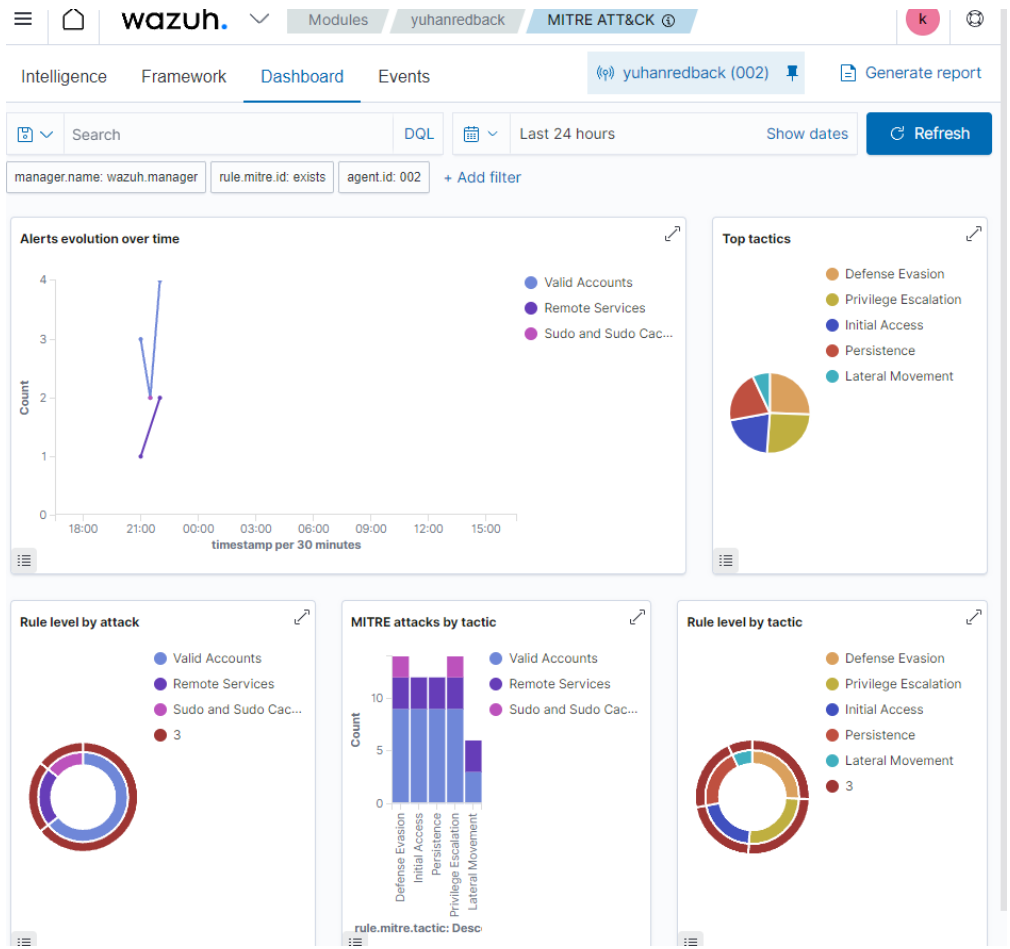
- Wazuh explores the vulnerabilities within linked agents.
- The tool explains what these vulnerabilities and how we can mitigate them.
- This is done so attackers have greater difficulty enumerating the user and exploiting them.



MODULE 2 – WHAT CAN WE LEARN FROM WAZUH?

MITRE ATT&CK FRAMEWORK

- An important framework to learn and understand to be aware of what is happening.
- Users can learn about various categories that certain attacks belong to and users can learn about these individual attacks.
- Wazuh provides intel on the specific MITRE techniques that can be applied to exploit various vulnerabilities located.
- Each attack has a unique tag which allows for the user to discover the attack type and learn about what the particular attack is.



Redback Operations

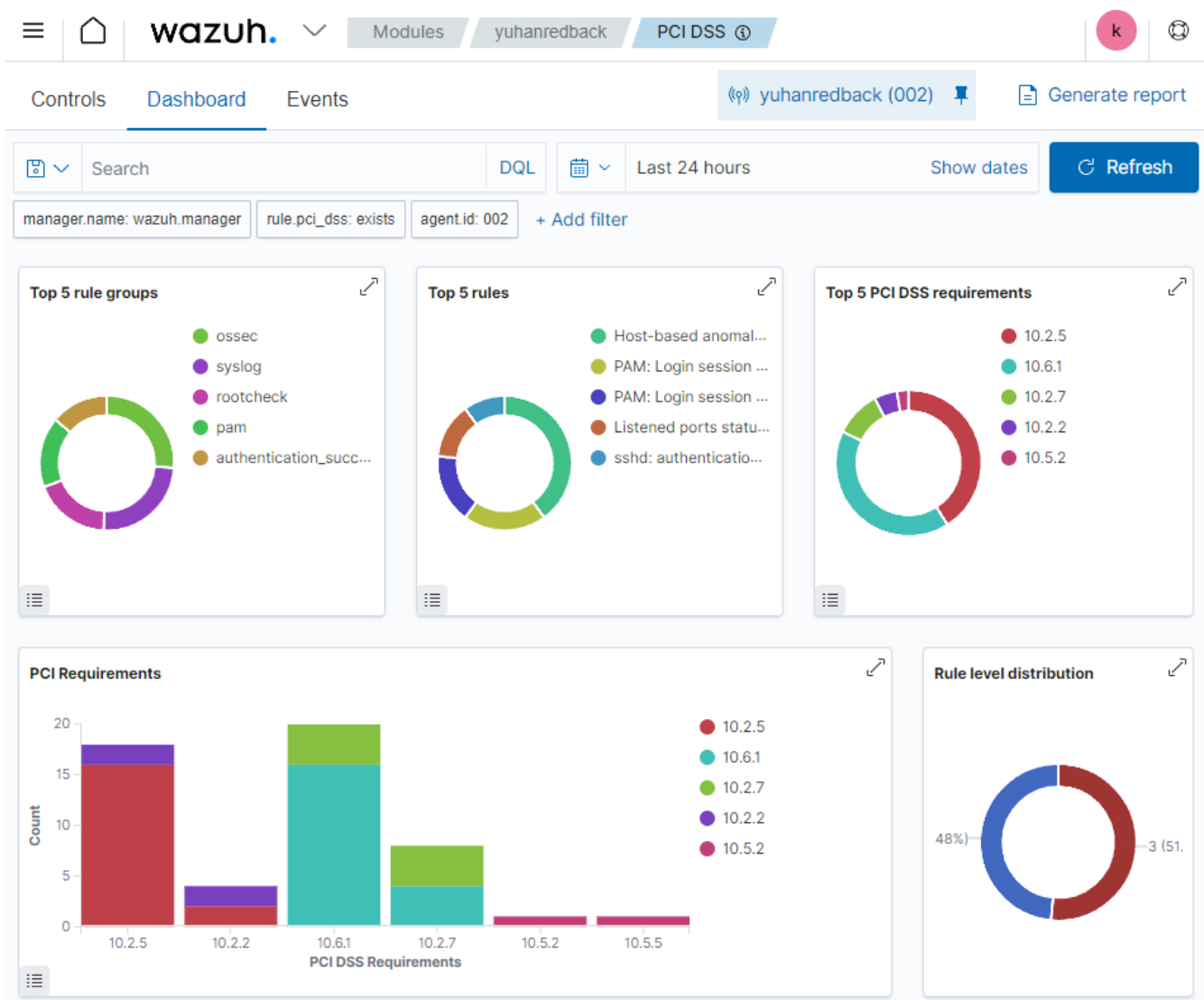
wazuh.

MODULE 2 – WHAT CAN WE LEARN FROM WAZUH?

COMPLIANCE STANDARDS

- Users can learn about compliance standards including constant securing of devices and rules associated.
- Other compliance standards involve mitigating vulnerabilities which include security configurations.

Note: Compliance standards vary from company to company. Wazuh simply explains more common standards adopted across many companies along with various compliance standards.



Note: This compliance follows PCI DSS Standards and there are various other compliance standards that you can also track

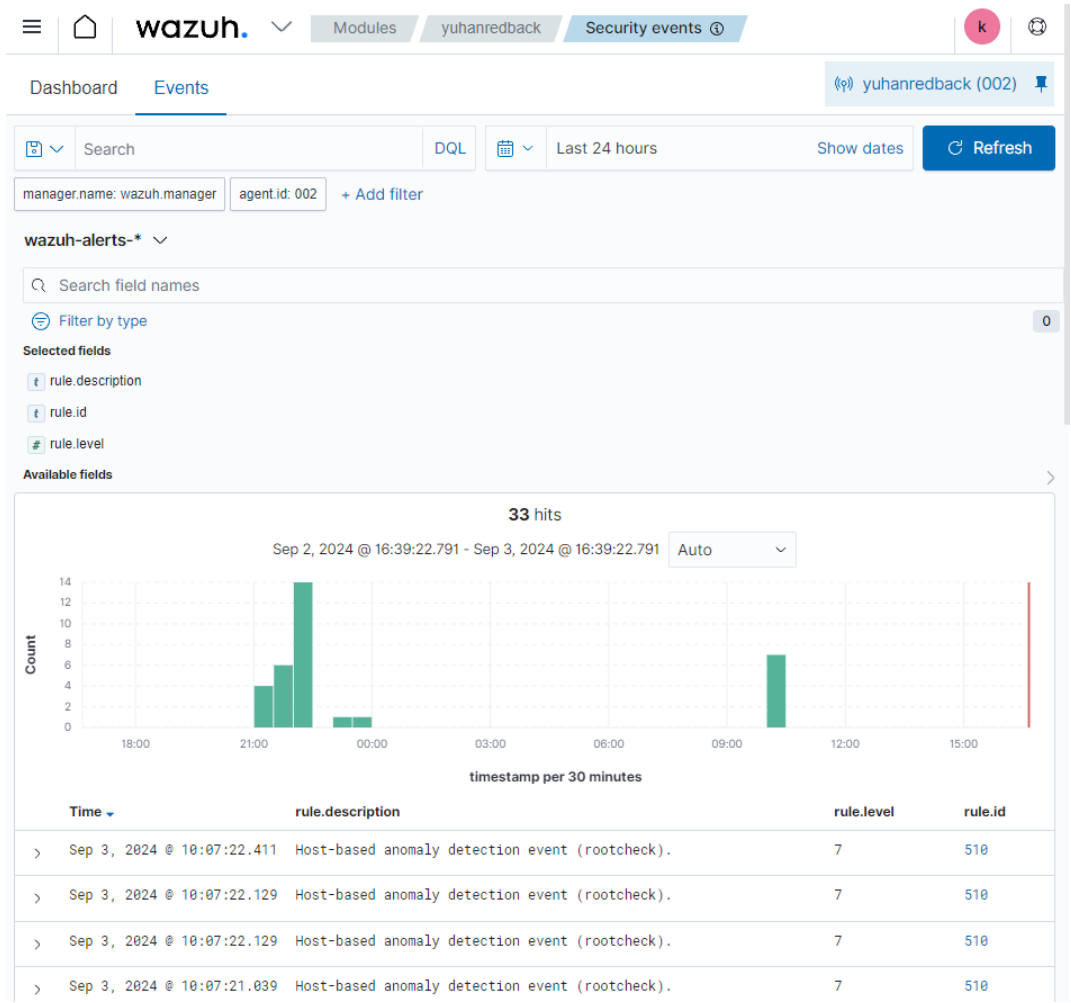
Redback Operations

wazuh.

MODULE 2 – WHAT CAN WE LEARN FROM WAZUH?

⚠CYBER ATTACKS

- There are constant new cyber-threats evolving in the world with constant new types of attacks being discovered.
- Wazuh can detect incoming brute force attacks and allow for you to respond to the attack. (Block IP address for example.)
- Wazuh also provides intel on various security events which serves as a method to developing safer agents and reduce compromises.



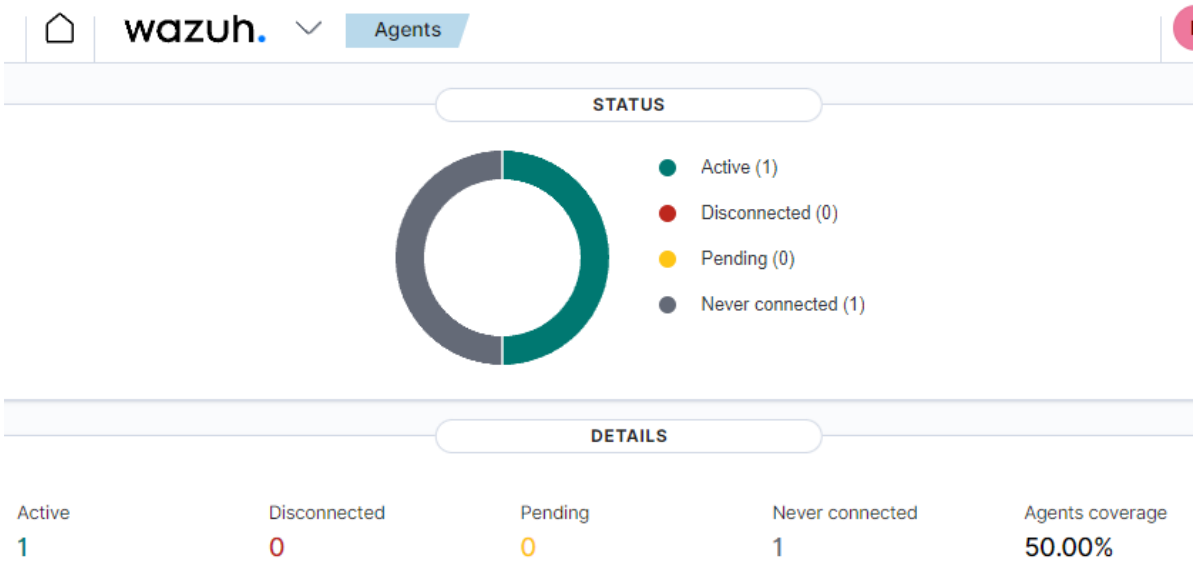
Redback Operations

wazuh.

MODULE 2 – WHAT CAN WE LEARN FROM WAZUH?

LINKED AGENTS

- We can learn a lot from our linked agents depending on what operating software (OS) we are utilizing.
- Wazuh supports many OS (MacOS, Windows, Ubuntu, Debian)
- Provides security configurations for the various agents.
- Wazuh allows for learning of specific OS capabilities and configurations in which we may not have had any experience with and also how to utilize our OS more effectively.



Redback Operations

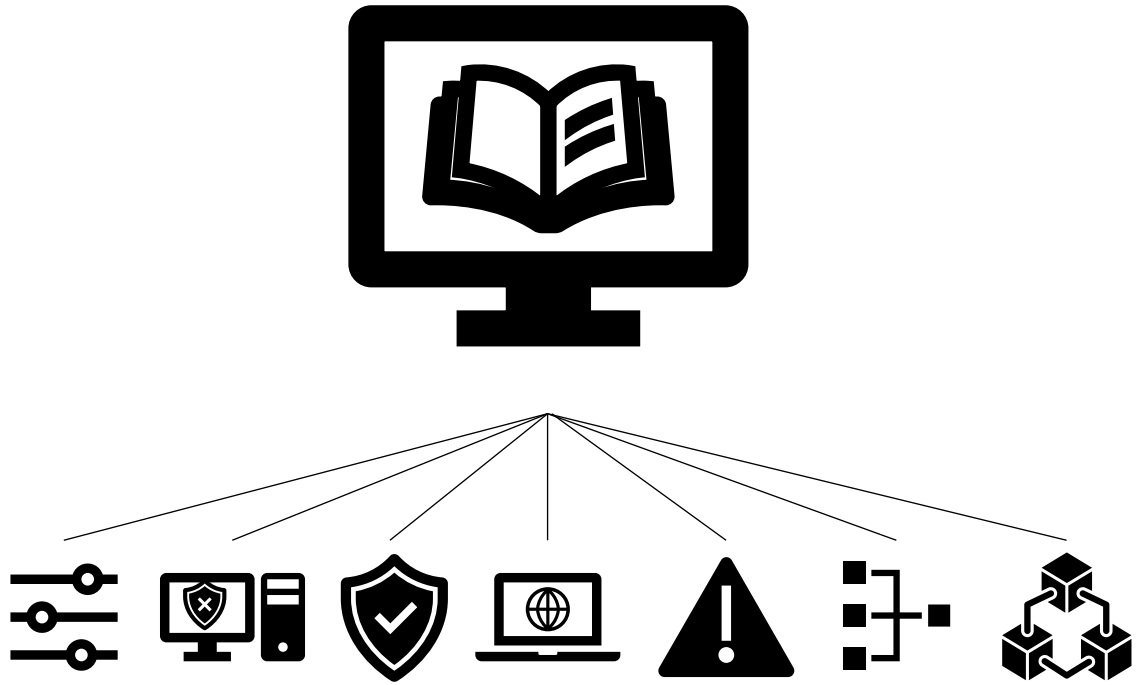
wazuh.

WHAT ELSE DOES WAZUH INFORM US ABOUT?

- There are various valuable pieces of information Wazuh can inform us about which include:
- Tracking of Windows Registry (if applicable).
- Changes in directories.
- Authentication failures.
- Top Alerts (Security alert list).
- Malware detected, executed and severity.
- File monitoring (modified, deleted).
- Informs the user how to secure their vulnerabilities and protect themselves.
- Monitoring for abnormal behaviour.

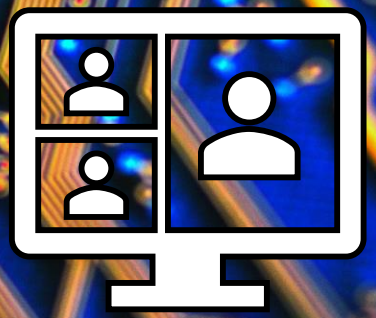
SUMMARISING MODULE:

- In this module we covered:
- The main areas in which we can enhance our learning and security of our devices.
- Other useful information that we can learn from utilizing Wazuh's services.



MODULE 3:

WHY SHOULD WE UTILIZE THIS TOOL AT REDBACK OPERATIONS?



MAIN AREAS

Security awareness

Incident response

Securing devices

Safety

Accessibility

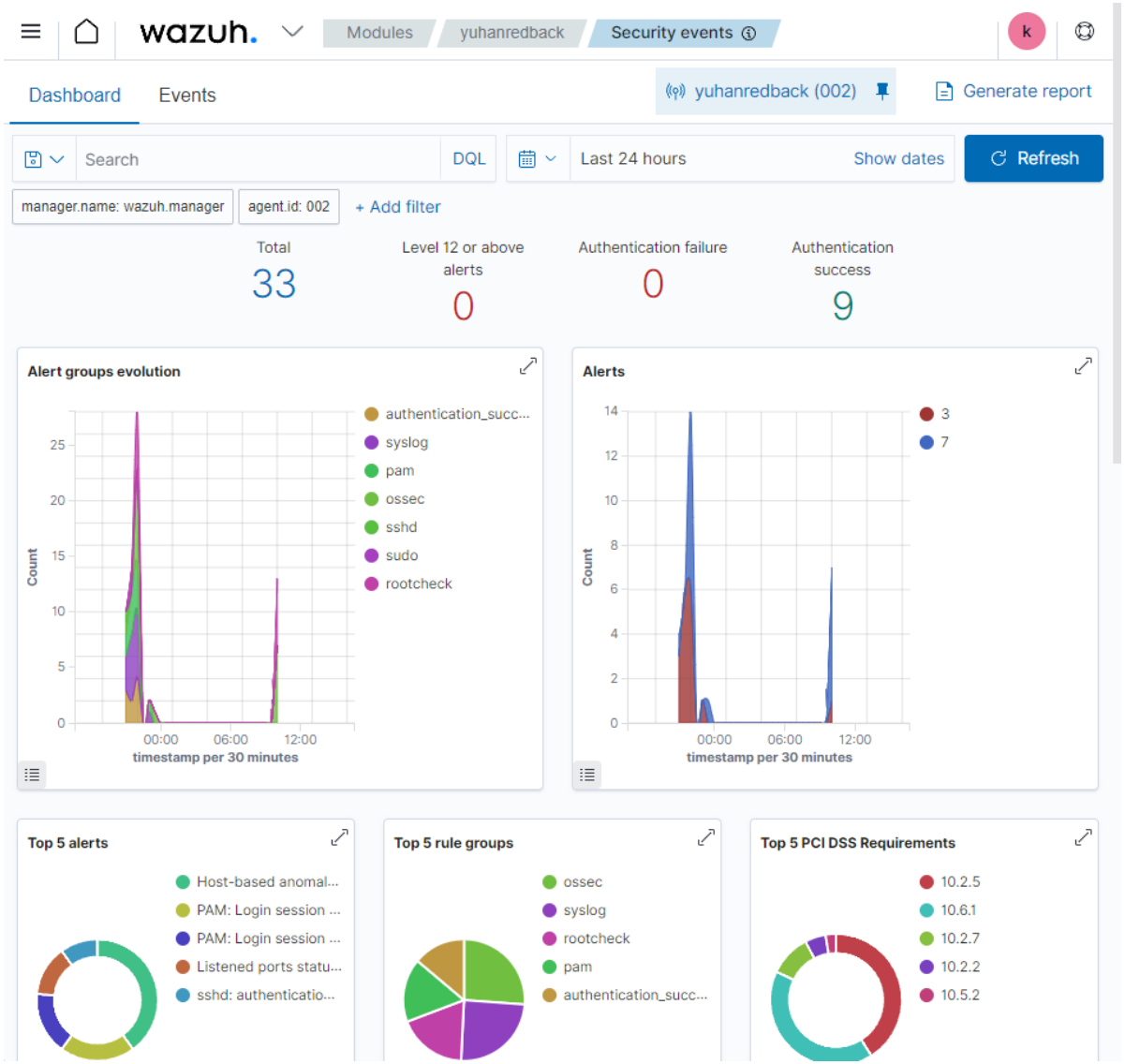
Compliance

It is important to also not solely rely on this one tool and ignore all other tools. There are also many other great defensive tools to utilize alongside Wazuh.

MODULE 3 – WHY SHOULD WE UTILIZE THIS TOOL?

SECURITY AWARENESS:

- Provides members knowledge of potential vulnerabilities and how to further secure devices to reduce the risk of a compromised device.
- Plenty of learning opportunities to become more aware of constant security threats.



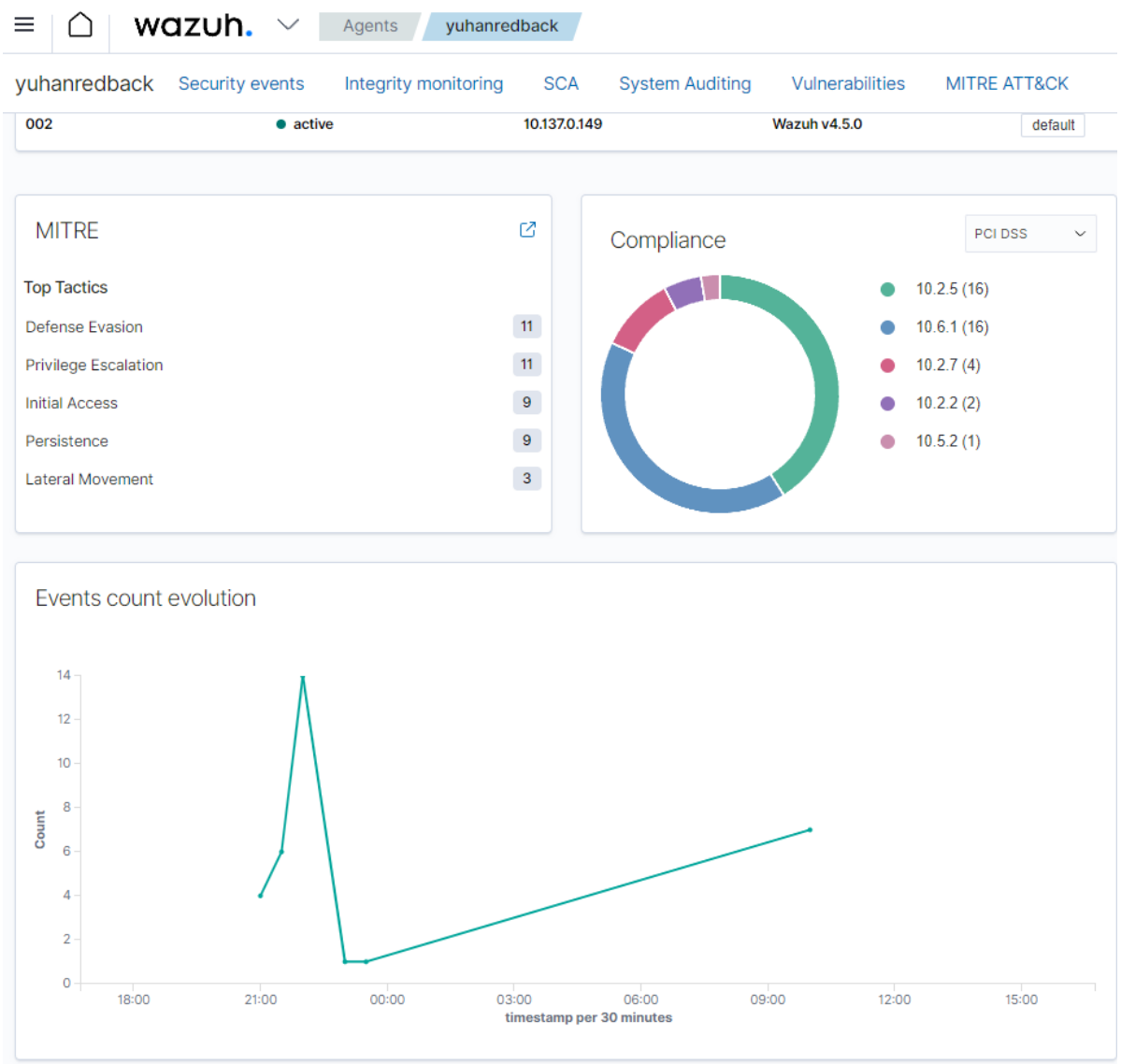
Redback Operations

wazuh.

MODULE 3 – WHY SHOULD WE UTILIZE THIS TOOL?

INCIDENT RESPONSE:

- Allows for response to incidents occurring from up-to-date event management as well as any compromises including changes to files/registry.
- You can respond directly by blocking/blacklisiting suspicious IP addresses or acting upon the generated security alerts.



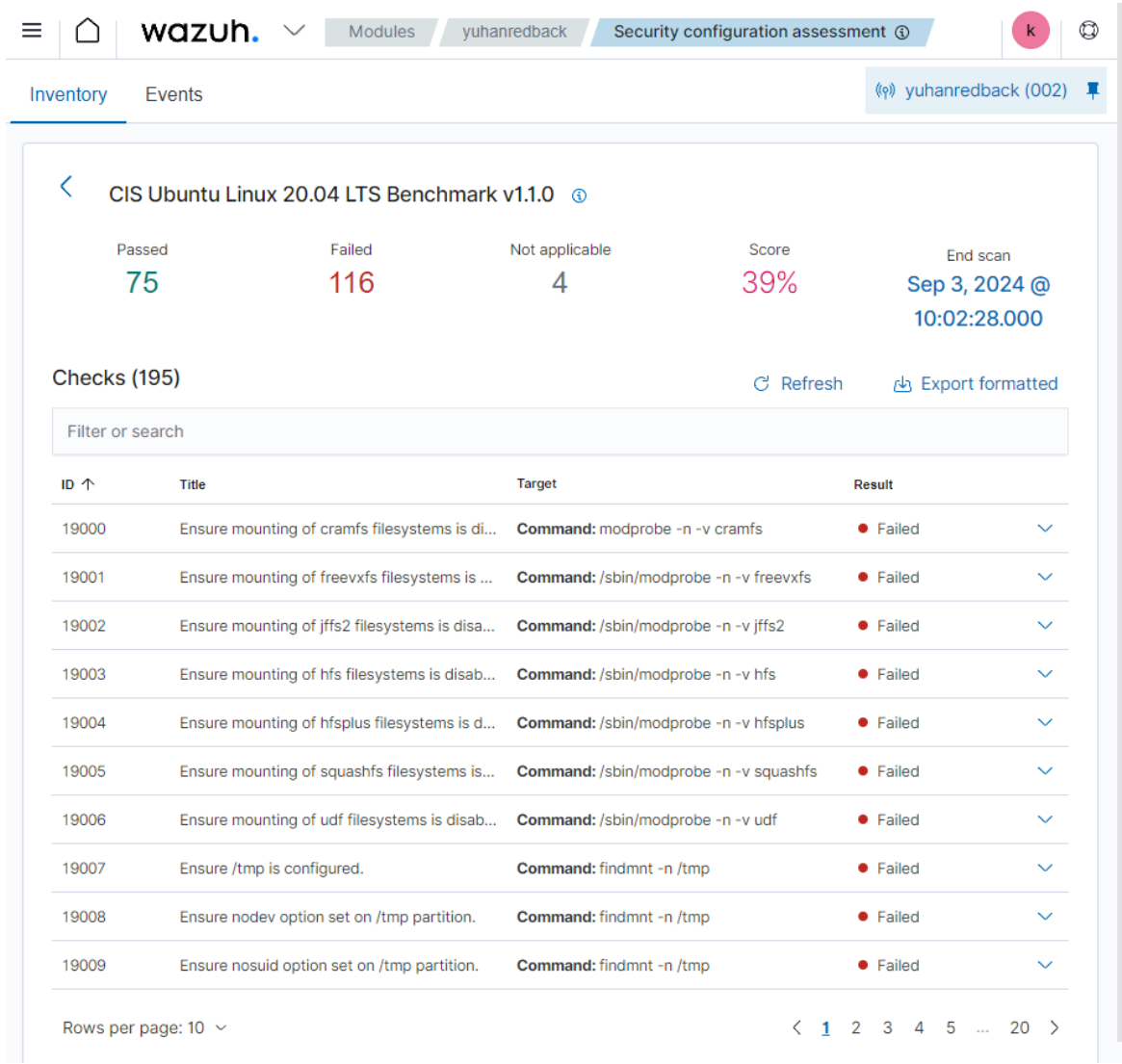
Redback Operations

wazuh.

MODULE 3 – WHY SHOULD WE UTILIZE THIS TOOL?

SECURING DEVICES:

- Constantly evolving threats allow the Wazuh tool to adapt and inform the user of new threats by creating awareness of new exploits/vulnerabilities being detected and how to further mitigate these risks.
- This allows for users to secure their devices further by adjusting their configurations and making appropriate changes to their devices in which the alerts are coming from.



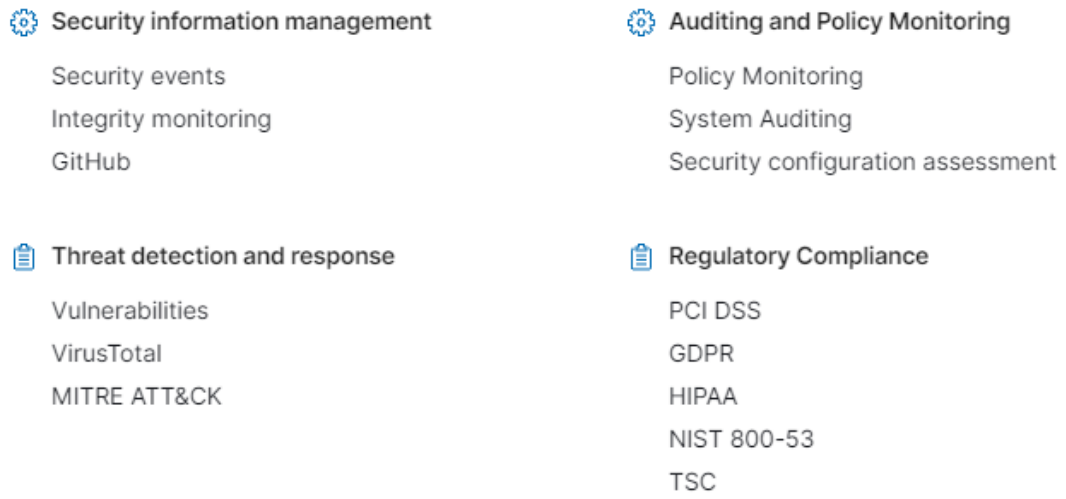
Redback Operations

wazuh.

MODULE 3 – WHY SHOULD WE UTILIZE THIS TOOL?

SAFETY:

- Protects member's machines from foreign interference/attacks which creates ease of access for company members to continue their work knowing the device they are utilizing is up to date and is protected.
- (Provided the right implementations/configurations are performed)

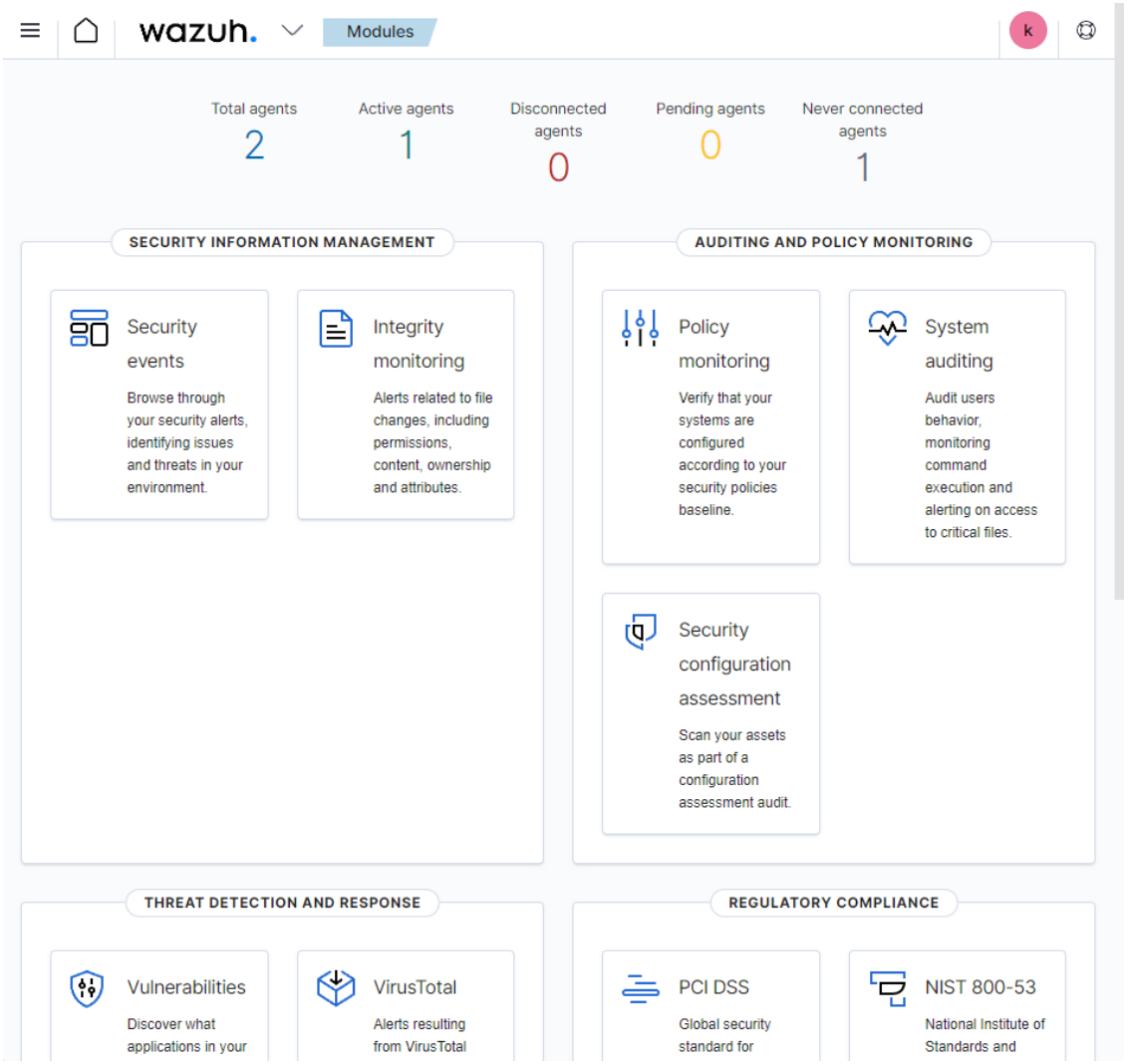


Redback Operations

wazuh.

ACCESSIBILITY:

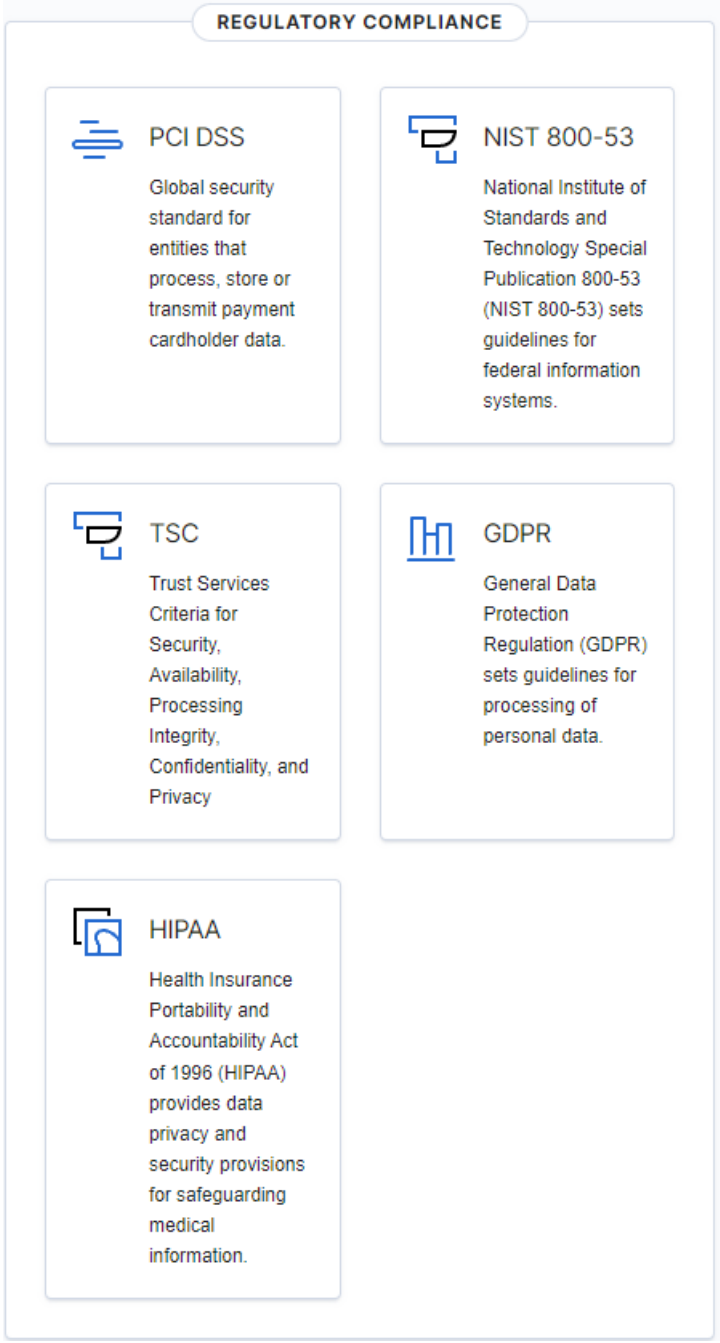
- Wazuh is an easy tool to understand, navigate and learn.
- Creates an easy and safe way of learning what is being displayed to them.
- Easily accessible User Interface (UI) assists in locating applicable vulnerabilities along with detailed information with solutions to the selected vulnerability.



MODULE 3 – WHY SHOULD WE UTILIZE THIS TOOL?

COMPLIANCE:

- The Wazuh tool also provides members opportunities to be compliant with various standards of companies to follow.
- Provides members the ability to become more Cybersafe and create a more cybersafe environment for the company.



Redback Operations

wazuh.

SUMMARISING MODULE:

- In this module we covered:
- The main areas in which provide valid reasoning into why we should use Wazuh.
- How Wazuh can benefit company members to become more cybersafe and secure.
- Why this tool is important for the company to utilize.
- Members who utilize this tool can reduce their exposure to cyber-related incidents.

EXTRA RESOURCES:

- Documentation on Redback Operations Docusaurus page: https://redback-operations.github.io/redback-documentation/docs/category/cyber-security-team
- Wazuh home page: https://wazuh.com/
- MITRE ATT&CK Framework: https://attack.mitre.org/
- Link to Security Awareness Training modules: https://classroom.google.com/c/NzAzMjgw0TI3MDIw?cjc=ppfbboc
- Link to Wazuh Documentation: https://redback-operations.github.io/redback-documentation/docs/cybersecurity/research/ids-and-wazuh/wazuh-documentation
- Link to Video Documentation: https://youtu.be/g82PwIFLYYc
- Link to Wazuh Tutorial video: https://youtu.be/3F5PPwxITWQ

Redback Operations

wazuh.

INDEX:

- Vulnerabilities: A flaw in code/design that can create a potential point of security compromise.
- User Interface (UI): A point of interaction/communication in a device.
- Open-Source: The source code is available freely for modification from a program.
- Authentication: Verifying the identity of a user. Often a prerequisite to allowing access to a system.
- SIEM (Security Information and Event Management): Assists organizations to detect, analyse and respond to security threats. Wazuh is an example of a SIEM tool.
- Mitigating: Reducing the likelihood of a severe compromise
- Linux: An open-source operating system (OS) which is supported on most major computer platforms.
- Docker: An open-source platform that handles containers which can be built, deployed, managed and updated.
- MITRE ATT&CK framework: A model for cyber attacker's behaviour, demonstrates various phases of an attacker's lifecycle and details tactics and techniques attackers utilize.
- PCI DSS Compliance: Payment Card Industry Data Security Standard – A set of policies and procedures aimed at security of financial transactions.
- Security alert: Refers to an event detected that has sent an alert out indicating suspicious behaviour.

wazuh.