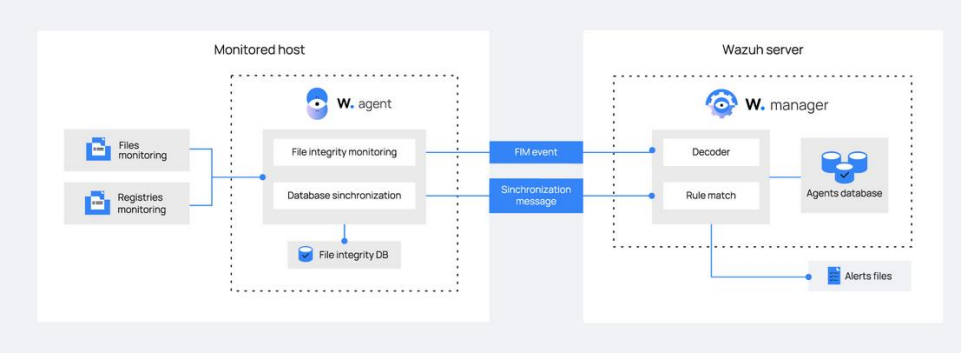
1. File integrity Monitoring and how to implement it

Wazuh File integrity monitoring (FIM) system watches selected files and triggers alerts when these files are modified. The component responsible for this task is called `syscheck`. This component stores the cryptographic checksum and other attributes of files or Windows registry keys and regularly compares them with the current files being used by the system, watching for changes.

The FIM module is located in the Wazuh agent, where it runs periodic scans of the system and stores the checksums and attributes of the monitored files and Windows registry keys in a local FIM database. The module looks for the modifications by comparing the new files' checksums to the old checksums. All detected changes are reported to the Wazuh manager.




The new FIM synchronization mechanism ensures the file inventory in the Wazuh manager is always updated with respect to the Wazuh agent, allowing for servicing of FIM-related API queries regarding the Wazuh agents. The FIM synchronization is based on periodic calculations of integrity between the Wazuh agent and the Wazuh manager databases, updating in the Wazuh manager only those files that are outdated, optimizing the data transfer of FIM.

2. Core functionality of Wazuh

The Wazuh platform helps organizations and individuals protect their data assets through threat prevention, detection, and response. Besides, Wazuh is also employed to meet regulatory compliance requirements, such as PCI DSS or HIPAA, and configuration standards like CIS hardening guides. Moreover, Wazuh is also a solution for users of IaaS (Amazon AWS, Azure, or Google Cloud) to monitor virtual machines and cloud instances. This is done at a system level utilizing the Wazuh security agent and at an infrastructure level pulling data directly from the cloud provider API.

3. Spear Phishing and control against Spear Phishing

A spear-phishing attack is a type of cybercrime where attackers send emails that appear to be from a known or trusted sender. The email is designed to convince an individual to share sensitive information or take action that allows attackers to steal data or money, to access accounts or to download malware. While a phishing attack is directed at a broad number of people, a spear-phishing attack is highly targeted to one or more individuals.

Control

- A request to download a file or to provide sensitive information that is not typically shared via email.
- A sender email address that does not match the domain name of the company the sender claims to be from.
- An email format that is different than the emails typically received from the person or company the sender claims to be.
- A link within the email that, upon inspection, would take the user to a fraudulent website rather than the website listed in the text of the email.
- Suspicious files or unexpected invoices attached to the email.
- Content within the email is unusual or out of character for the sender.

4. Integrating firewall logs in Wazuh

following configuration block to the `/var/ossec/etc/ossec.conf` file of your `wazuh-manager` (replacing `PORT`, `PROTOCOL` and `X.X.X.X/X` with your corresponding information).

```
 <remote>
    <connection>syslog</connection>
    <port>PORT</port>
    <protocol>PROTOCOL</protocol>
    <allowed-ips>X.X.X.X/X</allowed-ips>
  </remote>
After this, you will have to restart the wazuh-manager.
systemctl restart wazuh-manager
```

5. Proxy servers, and its role to protect computer Network

A proxy server acts as a gateway between you and the internet. It's an intermediary server separating end users from the websites they browse. Proxy servers provide varying levels of functionality, security, and privacy depending on your use case, needs, or company policy.
A proxy server is basically a computer on the internet with its own IP address that your computer knows. When you send a web request, your request goes to the proxy server first. The proxy server then makes your web request on your behalf, collects the response from the web server, and forwards you the web page data so you can see the page in your browser.
When the proxy server forwards your web requests, it can make changes to the data you send and still get you the information that you expect to see. A proxy server can change your IP address, so the web server doesn't know exactly where you are in the world. It can encrypt your data, so your data is unreadable in transit. And lastly, a proxy server can block access to certain web pages, based on IP address.
Role
**To control internet usage of employees and children**
**Bandwidth savings and improved speeds**
**Privacy benefits**
**Improved security**
**Get access to blocked resources**

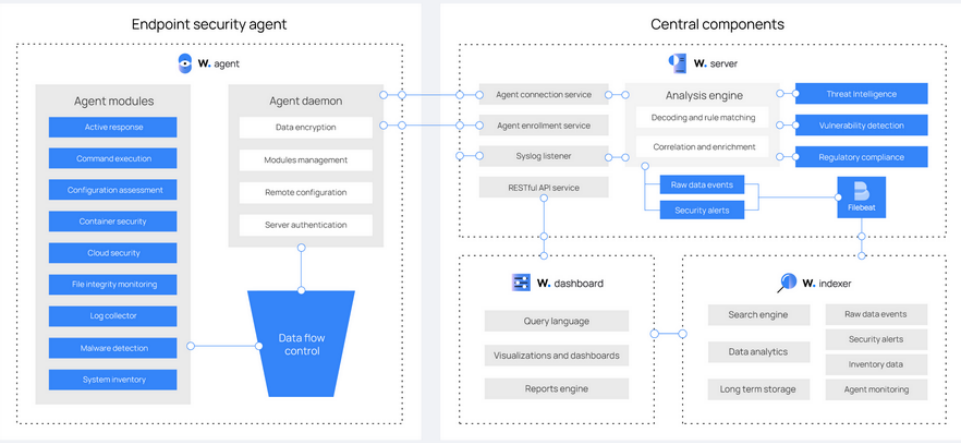
6. Connection establishment of End user (PC/Laptop) in Wazuh

7. Components in Wazuh

The Wazuh platform provides XDR and SIEM features to protect your cloud, container, and server workloads. These include log data analysis, intrusion and malware detection, file integrity monitoring, configuration assessment, vulnerability detection, and support for regulatory compliance.
The Wazuh solution is based on the Wazuh agent, which is deployed on the monitored endpoints, and on three central components: the Wazuh server, the Wazuh indexer, and the Wazuh dashboard.

- The Wazuh indexer is a highly scalable, full-text search and analytics engine. This central component indexes and stores alerts generated by the Wazuh server.
- The Wazuh server analyzes data received from the agents. It processes it through decoders and rules, using threat intelligence to look for well-known indicators of compromise (IOCs). A single server can analyze data from hundreds or thousands of agents, and scale horizontally when set up as a cluster. This central component is also used to manage the agents, configuring and upgrading them remotely when necessary.
- The Wazuh dashboard is the web user interface for data visualization and analysis. It includes out-of-the-box dashboards for security events, regulatory compliance (e.g., PCI DSS, GDPR, CIS, HIPAA, NIST 800-53), detected vulnerable applications, file integrity monitoring data, configuration assessment results, cloud infrastructure monitoring events, and others. It is also used to manage Wazuh configuration and to monitor its status.

| Index | Description |
|---|---|
| wazuh-alerts | Stores alerts generated by the Wazuh server. These are created each time an event trips a rule with a high enough priority (this threshold is configurable). |
| wazuh-archives | Stores all events (archive data) received by the Wazuh server, whether or not they trip a rule. |
| wazuh-monitoring | Stores data related to the Wazuh agent status over time. It is used by the web interface to represent when individual agents are or have been `Active`, `Disconnected`, or `Never connected`. |
| wazuh-statistics | Stores data related to the Wazuh server performance. It is used by the web interface to represent the performance statistics. |




8. Configure VirusTotal in Wazuh

Wazuh can scan monitored files for malicious content in monitored files. This solution is possible through an integration with VirusTotal, which is a powerful platform that aggregates multiple antivirus products along with an online scanning engine

This is an example configuration to add on the `ossec.conf` file:

```
<integration>
  <name>virustotal</name>
  <api_key>API_KEY</api_key> <!-- Replace with your VirusTotal API key -->
  <group>syscheck</group>
  <alert_format>json</alert_format>
</integration>
```

9. Common Use cases of the wazuh platform

The Wazuh platform helps organizations and individuals protect their data assets through threat prevention, detection, and response. Besides, Wazuh is also employed to meet regulatory compliance requirements, such as PCI DSS or HIPAA, and configuration standards like CIS hardening guides. Moreover, Wazuh is also a solution for users of IaaS (Amazon AWS, Azure, or Google Cloud) to monitor virtual machines and cloud instances. This is done at a system level utilizing the Wazuh security agent and at an infrastructure level pulling data directly from the cloud provider API. Additionally, Wazuh is employed to protect containerized environments by providing cloud-native runtime security. This feature is based on an integration with the Docker engine API and the Kubernetes API. The Wazuh security agent can run on the Docker host providing a complete set of threat detection and response capabilities.

| | |
|---|---|
| Log data analysis | File integrity monitoring |
| Rootkits detection | Active response |
| Configuration assessment | System inventory |
| Vulnerability detection | Cloud security |
| Container security | Regulatory compliance |

10. Phases in Cyber Kill Chain

1. Reconnaissance

Reconnaissance is the first stage in the Cyber Kill Chain and involves researching potential targets before carrying out any penetration testing. The reconnaissance stage may include identifying potential targets, finding their vulnerabilities, discovering which third parties are connected to them (and what data they can access), and exploring existing entry points as well as finding new ones. Reconnaissance can take place both online and offline.

2. Weaponization

The weaponization stage of the Cyber Kill Chain occurs after reconnaissance has taken place and the attacker has discovered all necessary information about potential targets, such as vulnerabilities. In the weaponization stage, all of the attacker's preparatory work culminates in the creation of malware to be used against an identified target. Weaponization can include creating new types of malware or modifying existing tools to use in a cyberattack. For example, cybercriminals may make minor modifications to an existing ransomware variant to create a new Cyber Kill Chain tool.

3. Delivery

In the delivery stage, cyberweapons and other Cyber Kill Chain tools are used to infiltrate a target's network and reach users. Delivery may involve sending phishing emails containing malware attachments with subject lines that prompt users to click through. Delivery can also take the form of hacking into an organization's network and exploiting a hardware or software vulnerability to infiltrate it.

4. Exploitation

Exploitation is the stage that follows delivery and weaponization. In the exploitation step of the Cyber Kill Chain, attackers take advantage of the vulnerabilities they have discovered in previous stages to further infiltrate a target's network and achieve their objectives. In this process, cybercriminals often move laterally across a network to reach their targets. Exploitation can sometimes lead attackers to their targets if those responsible for the network have not deployed deception measures.

5. Installation

After cybercriminals have exploited their target's vulnerabilities to gain access to a network, they begin the installation stage of the Cyber Kill Chain: attempting to install malware and other cyberweapons onto the target network to take control of its systems and exfiltrate valuable data. In this step, cybercriminals may install cyberweapons and malware using Trojan horses, backdoors, or command-line interfaces.

6. Command and Control

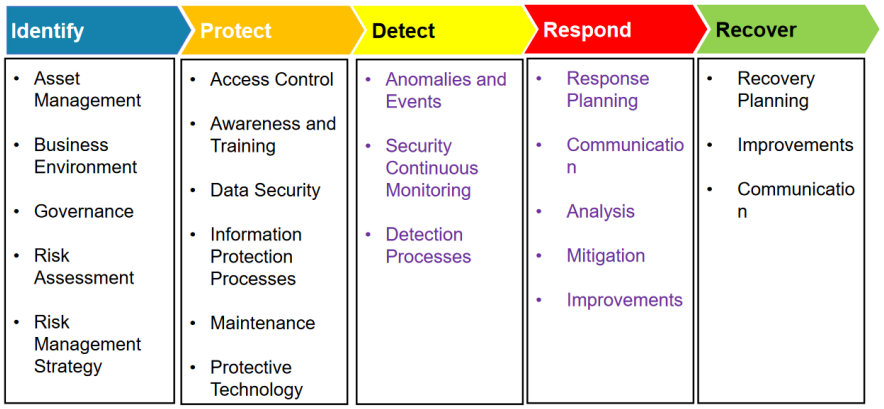
In the C2 stage of the Cyber Kill Chain, cybercriminals communicate with the malware they've installed onto a target's network to instruct cyberweapons or tools to carry out their objectives. For example, attackers may use communication channels to direct computers infected with the Mirai botnet malware to overload a website with traffic or C2 servers to instruct computers to carry out cybercrime objectives.

7. Actions on Objectives

After cybercriminals have developed cyberweapons, installed them onto a target's network, and taken control of their target's network, they begin the final stage of the Cyber Kill Chain: carrying out their cyberattack objectives. While cybercriminals' objectives vary depending on the type of cyberattack, some examples include weaponizing a botnet to interrupt services with a Distributed Denial of Service (DDoS) attack, distributing malware to steal sensitive data from a target organization, and using ransomware as a cyber extortion tool.

11. Phases in Incident Handling Life Cycle?

## NIST Cybersecurity framework



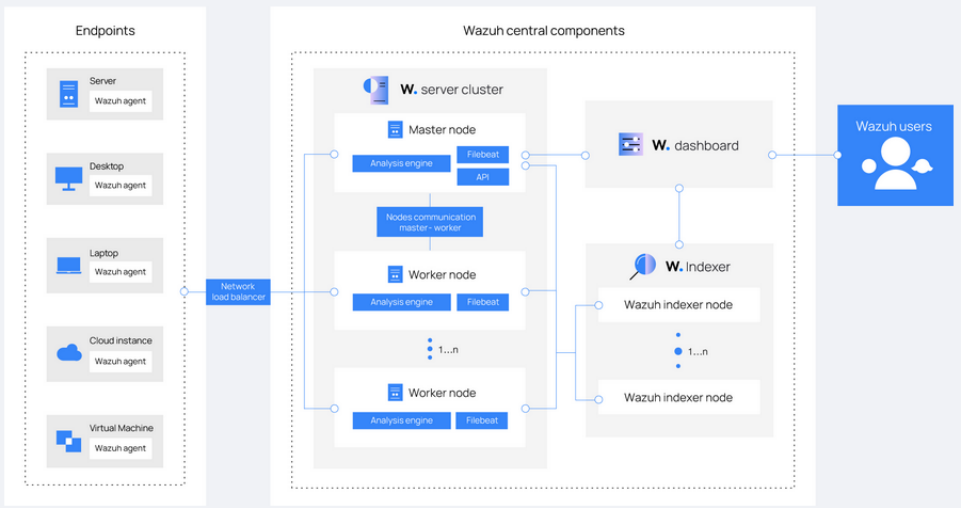

-> Preparation
-> Detection & Analysis
-> Containment Eradication & Recovery
-> Post-Incident Activity

12. Creation of sample website and integrate access logs to Wazuh Manager.

13. Steps to configure Wazuh
14. Show different Log source types
15. Setup Active Directory, configure simple group policy, capture the logs and send it to Wazuh Manager
16. steps involved in Configuring Secure remote access to AWS SIEM lab with two factor authentication, encryption & activities logs captured

17. Wazuh Architecture, Use Cases, Events Thresholds & Vulnerability Scanning

The Wazuh architecture is based on agents, running on the monitored endpoints, that forward security data to a central server. Agentless devices such as firewalls, switches, routers, and access points are supported and can actively submit log data via Syslog, SSH, or using their API. The central server decodes and analyzes the incoming information and passes the results along to the Wazuh indexer for indexing and storage.




18. Wazuh Modules: Security Events, Security Configuration, File Integrity Monitoring, Threat Intel- Virus Total, Mitre attack, & Compliance Modules.