PRESENTED BY LCC CYBER DEFENSE TEAM

DIGITAL ARMOR: DEFENSIVE SOFTWARE TOOLS

WWW.LSU.EDU/CYBERCLINIC

43% OF CYBERATTACKS TARGET SMALL BUSINESSES

VIA: ACCENTURE'S 2019 COST OF CYBERCRIME STUDY

4,000 RANSOMWARE ATTACKS PER DAY

VIA: FBI

WHAT IS DEFENSIVE SOFTWARE?

- Software that attempts to keep your assets safe
- Some alert on attack attempts
- Keep you and your team informed about what is going on on your systems and network.

WHAT ARE YOU DEFENDING?

- Confidentiality
- Integrity
- Availability

WHAT THREATS ARE YOU DEFENDING FROM?

- Ransomware
- Phishing
- Denial of Service

DEFENSIVE TOOL TYPES

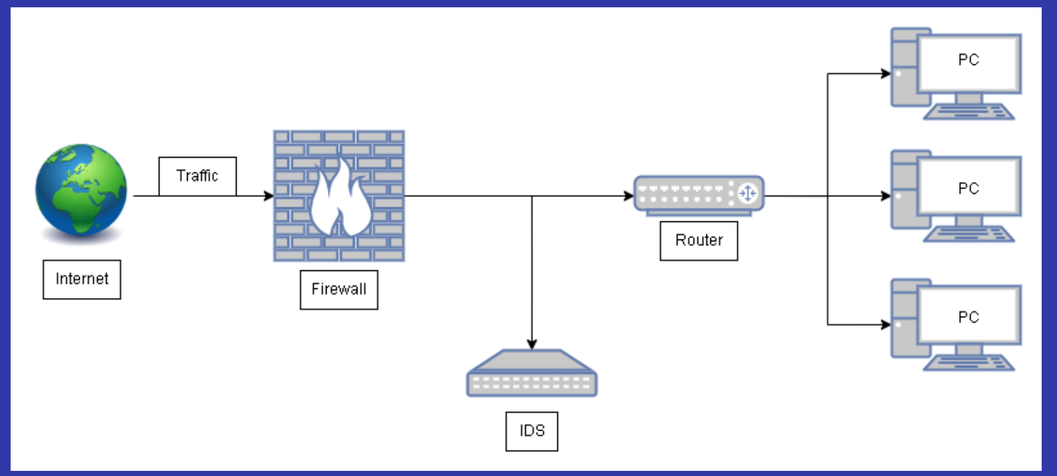
- Firewall
- Intrusion Detection System (IDS)
- Intrusion Prevention System (IPS)
- Endpoint Detection and Response (EDR)
    - Antivirus
- Security Information and Event Management (SIEM)

FIREWALLS

- A barrier between a trusted internal network and untrusted external networks
- Monitor and control incoming and outgoing traffic
- Behavior is based on preset rules configured by the network manager

INTRUSION DETECTION SYSTEM

- Reactive counterpart to Firewalls
- Focus on detecting and alerting security incidents after they occur
- Can catch threats that bypass a firewall



INTRUSION PREVENTION SYSTEM

- Build upon the capabilities of an IDS
- Actively block or prevent identified threats in real-time
- Can enforce security policies at various points within the network

END POINT DETECTION AND RESPONSE

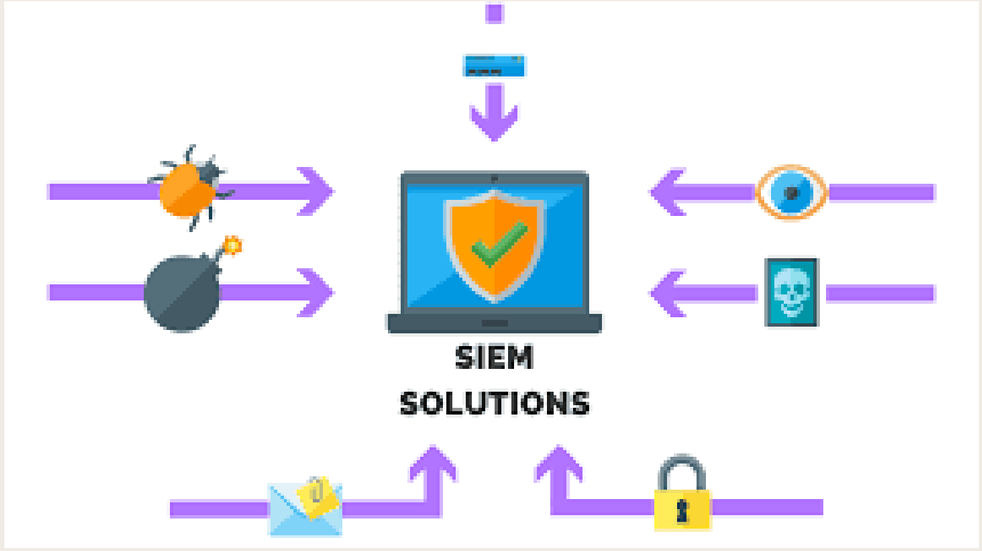
- Monitor and respond to cybersecurity threats on endpoints (laptops, desktops, servers) in real-time
- Provide advanced threat detection and incident response capabilities.

ANTIVIRUS

- Downloaded on an endpoint in a network
- Detect and removes all types of malware if possible
- Not all are created equal

SECURITY INFORMATION AND EVENT MANAGEMENT

- Collect, analyze, and correlate security events
- Some can create alerts and notifications about high priority events
- Some can integrate smoothly with other tools.



HOW TO CHOOSE THE RIGHT TOOL FOR YOU

- Budget
- Compatibility with existing hardware
- Needs of business
- Ease of use and ability to learn

TIPS FOR IMPLEMENTATION

Employee training and awareness of tools

Regular updates and maintenance

Monitor and react to incidents and events

TAKEAWAYS

01. What is a defensive tool

02. How to choose the tool for you

03. How to best implement these tools

Installing the Wazuh agent

The Wazuh agent is a single and lightweight monitoring software. It is a multi-platform component that can be deployed to laptops, desktops, servers, cloud instances, containers, or virtual machines. It provides visibility into the endpoint's security by collecting critical system and application records, inventory data, and detecting anomalies.

If the Wazuh central components are already installed in your environment, select your operating system below and follow the installation steps to deploy the agent on the endpoints.




```
aya@aya-virtual-machine:~/wazuh$ curl -sO https://packages.wazuh.com/4.7/wazuh-install.sh && sudo bash ./wazuh-install.sh -a
[sudo] password for aya:
10/05/2024 05:41:52 INFO: Starting Wazuh installation assistant. Wazuh version: 4.7.4
10/05/2024 05:41:52 INFO: Verbose logging redirected to /var/log/wazuh-install.log
10/05/2024 05:41:58 INFO: --- Dependencies ----
10/05/2024 05:41:58 INFO: Installing gawk.
10/05/2024 05:42:00 INFO: Wazuh web interface port will be 443.
10/05/2024 05:42:02 INFO: --- Dependencies ----
10/05/2024 05:42:02 INFO: Installing apt-transport-https.
10/05/2024 05:42:05 INFO: Wazuh repository added.
10/05/2024 05:42:05 INFO: --- Configuration files ---
10/05/2024 05:42:05 INFO: Generating configuration files.
10/05/2024 05:42:05 INFO: Created wazuh-install-files.tar. It contains the Wazuh cluster key, certificates, and passwords necessary for
installation.
10/05/2024 05:42:05 INFO: --- Wazuh indexer ---
10/05/2024 05:42:06 INFO: Starting Wazuh indexer installation.
10/05/2024 05:42:41 INFO: Wazuh indexer installation finished.
10/05/2024 05:42:41 INFO: Wazuh indexer post-install configuration finished.
10/05/2024 05:42:41 INFO: Starting service wazuh-indexer.
10/05/2024 05:42:48 INFO: wazuh-indexer service started.
10/05/2024 05:42:48 INFO: Initializing Wazuh indexer cluster security settings.
10/05/2024 05:42:58 INFO: Wazuh indexer cluster initialized.
10/05/2024 05:42:58 INFO: --- Wazuh server ---
10/05/2024 05:42:58 INFO: Starting the Wazuh manager installation.
10/05/2024 05:43:23 INFO: Wazuh manager installation finished.
10/05/2024 05:43:23 INFO: Starting service wazuh-manager.
10/05/2024 05:43:37 INFO: wazuh-manager service started.
10/05/2024 05:43:37 INFO: Starting Filebeat installation.
10/05/2024 05:43:41 INFO: Filebeat installation finished.
10/05/2024 05:43:42 INFO: Filebeat post-install configuration finished.
10/05/2024 05:43:42 INFO: Starting service filebeat.
10/05/2024 05:43:43 INFO: filebeat service started.
10/05/2024 05:43:43 INFO: --- Wazuh dashboard ---
10/05/2024 05:43:43 INFO: Starting Wazuh dashboard installation.
10/05/2024 05:44:03 INFO: Wazuh dashboard installation finished.
10/05/2024 05:44:03 INFO: Wazuh dashboard post-install configuration finished.
10/05/2024 05:44:03 INFO: Starting service wazuh-dashboard.
10/05/2024 05:44:03 INFO: wazuh-dashboard service started.
10/05/2024 05:44:18 INFO: Initializing Wazuh dashboard web application.
10/05/2024 05:44:18 INFO: Wazuh dashboard web application initialized.
10/05/2024 05:44:18 INFO: --- Summary ---
10/05/2024 05:44:18 INFO: You can access the web interface https://<wazuh-dashboard-ip>:443
    User: admin
    Password: u+lF19xZCSiI*tFhkZZEQ5ej9Zo7CdjE
10/05/2024 05:44:18 INFO: --- Dependencies ----
10/05/2024 05:44:18 INFO: Removing gawk.
10/05/2024 05:44:20 INFO: Installation finished.
aya@aya-virtual-machine:~/wazuh$
```