Collegiate Cyber Defense Competitions

Inject Name	Configure End-Point Protection Software
Inject ID	SVRA12T

Description

Configure end-point protection software on each Linux and Windows server. Follow the steps outlined below:

1.) Deploy Wazuh Manager Dashboard on one Linux host to provide centralized management.

Example:

curl -sO https://packages.wazuh.com/4.7/wazuh-install.sh
sudo bash wazuh-install.sh —wazuh-dashboard

2.) Install ClamAV on Windows, set to run hourly and on-access scanning.

Example:

msiexec /i clamav-1.4.3.win.x64.msi ADDLOCAL="ClamAV,FreshClam" /qn

3.) Load the Wazuh agent on Windows, and enable the modules in Gossec.conf

Example (Install):

```
msiexec /i wazuh-agent-4.7.3.msi WAZUH_MANAGER="10.0.0.5" \
    WAZUH_REGISTRATION_PASSWORD="MyStrongKey" /qn
```

Example (Enable Modules):

```
<syscollector><enabled>yes</enabled></syscollector>
<fim><enabled>yes</enabled><directories realtime="yes">C:\Users</directories></fim>
<windows_event_channels>
    <channel>Security</channel>
    <channel>Microsoft-Windows-Sysmon/Operational</channel>
</windows_event_channels>
```

— Don't forget to restart —

4.) Install ClamAV on Linux, schedule with timer and enable real-time scanning. Install Wazuh agent and enable modules.

Example (Install):

```
sudo apt update && sudo apt install clamav clamav-daemon
sudo systemctl stop clamav-freshclam
sudo freshclam          # initial DB pull
sudo systemctl enable --now clamav-freshclam clamav-daemon

curl -sO https://packages.wazuh.com/4.7/wazuh-agent_4.7.3-1_amd64.deb
sudo WAZUH_MANAGER="10.0.0.5" apt install ./wazuh-agent_4.7.3-1_amd64.deb
sudo systemctl enable --now wazuh-agent
```

Deliverables	Respond with a business memo that documents the successful install of the Wazuh dashboard. Use a screen shot of the dashboard showing each of the agents for the other servers are green. Provide similar evidence that ClamAV is operating on each node. Consider the following commands: *# Linux* *sudo ss -ltnp | grep :3310 # clamd default TCP socket* *# Windows (PowerShell)* *Get-Service "ClamAV*" | Select Status,Name,DisplayName*