# Defending against badness

**CSC 8: Malware Defenses**


Open Source HIDS


Nessus Agents on Endpoints

http://www.cisecurity.org/controls/

# What is the profile of running services?

## CSC 9: Limitation and Control of Network Ports, Protocols, and Services

| **Limitation and Control of Network Ports, Protocols, and Services**<br><br>**Manage (track/control/correct) the ongoing operational use of ports, protocols, and services on networked devices in order to minimize windows of vulnerability available to attackers.** | |
|---|---|
| Associate Active Ports, Services, and Protocols to Asset Inventory | Associate active ports, services, and protocols to the hardware assets in the asset inventory. |
| Ensure Only Approved Ports, Protocols, and Services Are Running | Ensure that only network ports, protocols, and services listening on a system with validated business needs are running on each system. |
| Perform Regular Automated Port Scans | Perform automated port scans on a regular basis against all systems and alert if unauthorized ports are detected on a system. |
| Apply Host-Based Firewalls or Port-Filtering | Apply host-based firewalls or port-filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed. |
| Implement Application Firewalls | Place application firewalls in front of any critical servers to verify and validate the traffic going to the server. Any unauthorized traffic should be blocked and logged. |

http://www.cisecurity.org/controls/