Defending against badness

CSC 8: Malware Defenses

Malware Defenses **Control the installation, spread, and execution of malicious code at multiple points in the enterprise, while optimizing the use of automation to enable rapid updating of defense, data gathering, and corrective action.**	
Utilize Centrally Managed Anti-malware Software	**Utilize centrally managed anti-malware software to continuously monitor and defend each of the organization's workstations and servers.**
Ensure Anti-Malware Software and Signatures Are Updated	Ensure that the organization's anti-malware software updates its scanning engine and signature database on a regular basis.
Enable Operating System Anti-Exploitation Features/Deploy Anti-Exploit Technologies	Enable anti-exploitation features such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR) that are available in an operating system or deploy appropriate toolkits that can be configured to apply protection to a broader set of applications and executables.
Configure Anti-Malware Scanning of Removable Devices	Configure devices so that they automatically conduct an anti-malware scan of removable media when inserted or connected.
Configure Devices to Not Auto-Run Content	**Configure devices to not auto-run content from removable media.**
Enable DNS Query Logging	**Enable Domain Name System (DNS) query logging to detect hostname lookups for known malicious domains.**
Enable Command-Line Audit Logging	**Enable command-line audit logging for command shells, such as Microsoft PowerShell and Bash.**

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

Defending against badness

CSC 8: Malware Defenses

Open Source HIDS

Nessus Agents on Endpoints

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