How is this thing configured?

CSC 5: Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers

Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers **Establish, implement, and actively manage (track, report on, correct) the security configuration of mobile devices, laptops, servers, and workstations using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.**	
Establish Secure Configurations	Maintain documented security configuration standards for all authorized operating systems and software.
Maintain Secure Images	Maintain secure images or templates for all systems in the enterprise based on the organization's approved configuration standards. Any new system deployment or existing system that becomes compromised should be imaged using one of those images or templates.
Securely Store Master Images	Store the master images and templates on securely configured servers, validated with integrity monitoring tools, to ensure that only authorized changes to the images are possible.
Deploy System Configuration Management Tools	Deploy system configuration management tools that will automatically enforce and redeploy configuration settings to systems at regularly scheduled intervals.
Implement Automated Configuration Monitoring Systems	Utilize a Security Content Automation Protocol (SCAP) compliant configuration monitoring system to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur.

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

What is this thing doing?

CSC 6: Maintenance, Monitoring and Analysis of Audit Logs

Maintenance, Monitoring and Analysis of Audit Logs **Collect, manage, and analyze audit logs of events that could help detect, understand, or recover from an attack.**	
Utilize Three Synchronized Time Sources	Use at least three synchronized time sources from which all servers and network devices retrieve time information on a regular basis so that timestamps in logs are consistent.
Activate Audit Logging	Ensure that local logging has been enabled on all systems and networking devices.
Enable Detailed Logging	Enable system logging to include detailed information such as a event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.
Ensure Adequate Storage for Logs	Ensure that all systems that store logs have adequate storage space for the logs generated.
Central Log Management	Ensure that appropriate logs are being aggregated to a central log management system for analysis and review.
Deploy SIEM or Log Analytic Tools	Deploy Security Information and Event Management (SIEM) or log analytic tool for log correlation and analysis.
Regularly Review Logs	On a regular basis, review logs to identify anomalies or abnormal events.
Regularly Tune SIEM	On a regular basis, tune your SIEM system to better identify actionable events and decrease event noise.

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