

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/>

Defending against direct download damage

CSC 7: Email and Web Browser Protections

Email and Web Browser Protections

Minimize the attack surface and the opportunities for attackers to manipulate human behavior through their interaction with web browsers and email systems.

Ensure Use of Only Fully Supported Browsers and Email Clients	Ensure that only fully supported web browsers and email clients are allowed to execute in the organization, ideally only using the latest version of the browsers and email clients provided by the vendor.
Disable Unnecessary or Unauthorized Browser or Email Client Plugins	Uninstall or disable any unauthorized browser or email client plugins or add-on applications.
Limit Use of Scripting Languages in Web Browsers and Email Clients	Ensure that only authorized scripting languages are able to run in all web browsers and email clients.
Maintain and Enforce Network-Based URL Filters	Enforce network-based URL filters that limit a system's ability to connect to websites not approved by the organization. This filtering shall be enforced for each of the organization's systems, whether they are physically at an organization's facilities or not.
Subscribe to URL-Categorization Service	Subscribe to URL-categorization services to ensure that they are up-to-date with the most recent website category definitions available. Uncategorized sites shall be blocked by default.
Log All URL requester	Log all URL requests from each of the organization's systems, whether on-site or a mobile device, in order to identify potentially malicious activity and assist incident handlers with identifying potentially compromised systems.
Use of DNS Filtering Services	Use Domain Name System (DNS) filtering services to help block access to known malicious domains.
Implement DMARC and Enable Receiver-Side Verification	To lower the chance of spoofed or modified emails from valid domains, implement Domain-based Message Authentication, Reporting and Conformance (DMARC) policy and verification, starting by implementing the Sender Policy Framework (SPF) and the DomainKeys Identified Mail (DKIM) standards.

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