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 badness

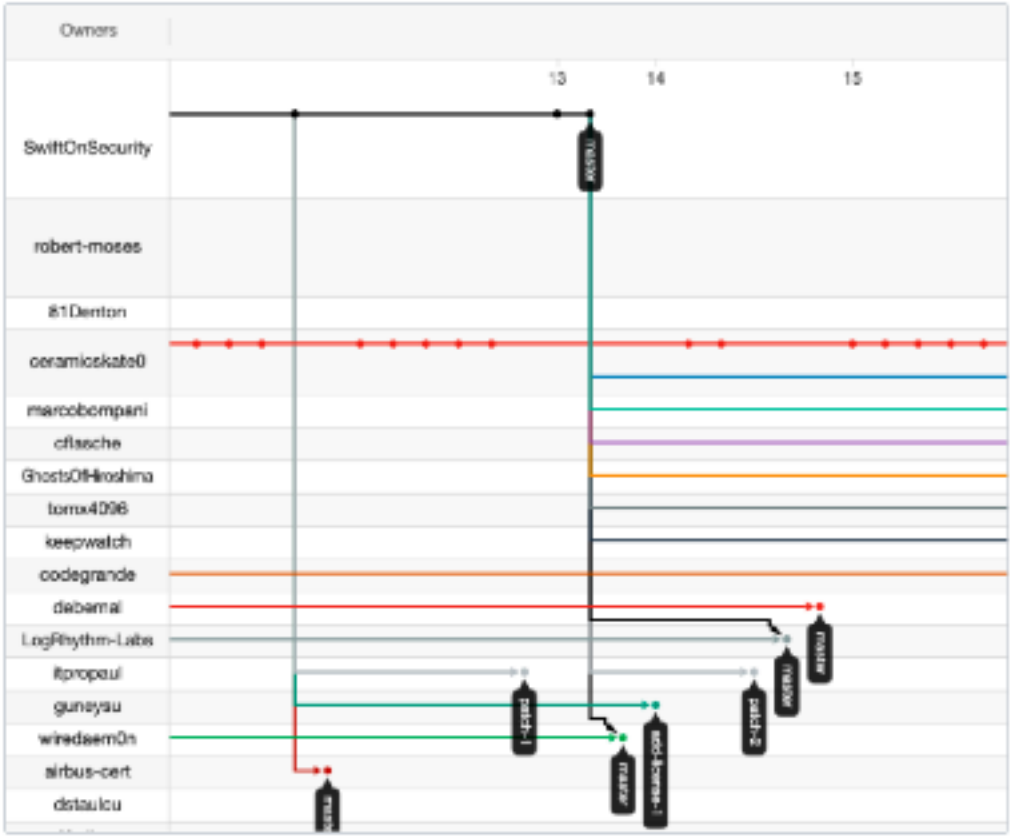
CSC 6: Maintenance, Monitoring and Analysis of Audit Logs

Microsoft

Sysmon v10.2

System Monitor (Sysmon) is a Windows system service and device driver that, once installed on a system, remains resident across system reboots to monitor and log system activity to the Windows event log. It provides detailed information about process creations, network connections, and changes to file creation time. By collecting the events it generates using Windows Event Collection or SIEM agents and subsequently analyzing them, you can identify malicious or anomalous activity and understand how intruders and malware operate on your network.

Sysmon configuration file template with default high-quality event tracing



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