**AU-4(1):**

**Control Implementation/Test Results**

The Windows Log Collector And Parser (WLCAP) PowerShell script is used to collect audit records from each system on the network and off-loads them onto a designated sub-system of the Information System for storage and analysis. This process is done at least weekly.

**AU-4(1) – CCI(s):**

|  |  |  |  |
| --- | --- | --- | --- |
| AU-4 (1) | AU-4 (1) | CCI-001851 | The Windows Log Collector And Parser (WLCAP) PowerShell script is used to collect audit records from each system on the network and off-loads them onto a designated sub-system of the Information System for storage and analysis. This process is done at the frequency defined in CCI-001850. |
| AU-4 (1) | AU-4 (1) | CCI-001850 | The frequency on which the information system off-loads audit records onto a different system or media than the system being audited is at least weekly. |

**AU-6:**

**Control Implementation/Test Results**

1. The Windows Log Collector And Parser (WLCAP) PowerShell script is used to generate reduced audit reports IAW audit categories defined below. These event categories will be reviewed on a weekly basis:

Logons – Success (off-hours logons and group account logons)

Logons – Fail

Logoffs – Success (off-hours logoffs and group account logoffs)

User/Group Management – Success/Fail (User/Group add, delete, modify, disable, lock)

Security Relevant File/Objects – Fail (Create, Delete, Modify, Permissions, Ownership)

Exports/Imports To/From Digital Media (Connections to Removable Media Devices) – Success

Configuration/Policy Changes – Success

Privileged/Role Escalation – Success

System Reboot/Shutdown – Success

Printing – Success

The event categories listed above are a subset of event categories identified for AU-2 in the DAAPM Appendix A. [Organization Name] has determined that the event categories listed above provide adequate information to detect anomalous activity and support after-the-fact investigations. All audit data identified in AU-2 is generated (if capable) and used as a supplement to the list above when needed.

1. The ISSO is responsible for conducting weekly auditing of the IS and reports anomalous activity to the ISSM. When appropriate, the ISSM reports the findings to the ISO and FSO. The ISSO documents the occurrence of weekly auditing in the Maintenance Log.

**AU-6 - CCI(s)**

|  |  |  |  |
| --- | --- | --- | --- |
| AU-6 | AU-6 (a) | CCI-000148 | The ISSO reviews and analyzes IS audit records for indications of inappropriate or unusual activity as defined in CCI-001862 and at the frequency defined in CCI-000151. |
| AU-6 | AU-6 (a) | CCI-000151 | DSS has defined the frequency for the review and analysis of IS audit records as weekly. |
| AU-6 | AU-6 (a) | CCI-001862 | The Windows Log Collector And Parser (WLCAP) PowerShell script is used to generate reduced audit reports IAW audit categories defined below. These event categories will be reviewed on a weekly basis:  Logons – Success (off-hours logons and group account logons)  Logons – Fail  Logoffs – Success (off-hours logoffs and group account logoffs)  User/Group Management – Success/Fail (User/Group add, delete, modify, disable, lock)  Security Relevant File/Objects – Fail (Create, Delete, Modify, Permissions, Ownership)  Exports/Imports To/From Digital Media (Connections to Removable Media Devices) – Success  Configuration/Policy Changes – Success  Privileged/Role Escalation – Success  System Reboot/Shutdown – Success  Printing – Success  The event categories listed above are a subset of event categories identified for AU-2 in the DAAPM Appendix A. [Organization Name] has determined that the event categories listed above provide adequate information to detect anomalous activity and support after-the-fact investigations. All audit data identified in AU-2 is generated (if capable) and used as a supplement to the list above when needed. |
| AU-6 | AU-6 (b) | CCI-000149 | The ISSO reports anomalous activity to the ISSM. When appropriate, the ISSM reports the findings to the ISO and FSO. |
| AU-6 | AU-6 (b) | CCI-001863 | The ISSM receives reports of inappropriate or unusual activity. When appropriate, the ISSM reports the findings to the ISO and FSO. |

**AU-6(4):**

**Control Implementation/Test Results**

The Windows Log Collector And Parser (WLCAP) PowerShell script provides the capability to centrally review and analyze audit records from multiple components within the Information System. Reference AU-4(1) and AU-6.

**AU-6(4) – CCI(s):**

|  |  |  |  |
| --- | --- | --- | --- |
| AU-6 (4) | AU-6 (4) | CCI-000154 | The Windows Log Collector And Parser (WLCAP) PowerShell script provides the capability to centrally review and analyze audit records from multiple components within the Information System. Reference AU-4(1) and AU-6. |

**AU-6(8):**

**Control Implementation/Test Results**

The Windows Log Collector And Parser (WLCAP) PowerShell script is used to generate reduced audit reports IAW audit categories defined in AU-6. WLCAP also provides the full-text of commands executed in the Windows Command Line Interface (CLI) and PowerShell (PSH). The audit reports are reviewed at the frequency defined in AU-6.

**AU-6(8) - CCI(s):**

|  |  |  |  |
| --- | --- | --- | --- |
| AU-6 (8) | AU-6 (8) | CCI-001870 | The Windows Log Collector And Parser (WLCAP) PowerShell script is used to generate reduced audit reports IAW audit categories defined in AU-6. WLCAP also provides the full-text of commands executed in the Windows Command Line Interface (CLI) and PowerShell (PSH). The audit reports are reviewed at the frequency defined in AU-6. |

**AU-7:**

**Control Implementation/Test Results**

The Windows Log Collector And Parser (WLCAP) PowerShell script provides an audit reduction and report generation capability (IAW AU-6) that:

1. Supports on-demand audit review, analysis, and reporting requirements and after-the-fact investigations of security incidents by offering the capability to parse audit records that have been saved to a file (see “-parseOnly” in the WLCAP README).
2. Does not alter the original content or time ordering of audit records by using FIPS 140-2 validated hashing algorithms to verify the integrity of files anytime they are moved and using a read-only PowerShell function to read from the audit record files.

**AU-7 - CCI(s):**

|  |  |  |  |
| --- | --- | --- | --- |
| AU-7 | AU-7 (a) | CCI-001875 | The Windows Log Collector And Parser (WLCAP) PowerShell script provides an audit reduction capability (IAW AU-6) that:  Supports on-demand audit review, analysis by offering the capability to parse audit records that have been saved to a file (see “-parseOnly” in the WLCAP README). |
| AU-7 | AU-7 (a) | CCI-001876 | The Windows Log Collector And Parser (WLCAP) PowerShell script provides an audit reduction capability (IAW AU-6) that:  Supports on-demand reporting requirements by offering the capability to parse audit records that have been saved to a file (see “-parseOnly” in the WLCAP README). |
| AU-7 | AU-7 (a) | CCI-001877 | The Windows Log Collector And Parser (WLCAP) PowerShell script provides an audit reduction capability (IAW AU-6) that:   1. Supports on-demand after-the-fact investigations of security incidents by offering the capability to parse audit records that have been saved to a file (see “-parseOnly” in the WLCAP README). |
| AU-7 | AU-7 (a) | CCI-001878 | The Windows Log Collector And Parser (WLCAP) PowerShell script provides a report generation capability (IAW AU-6) that:  Supports on-demand audit review, analysis by offering the capability to parse audit records that have been saved to a file (see “-parseOnly” in the WLCAP README) and generating a report based on that data. |
| AU-7 | AU-7 (a) | CCI-001879 | The Windows Log Collector And Parser (WLCAP) PowerShell script provides a report generation capability (IAW AU-6) that:  Supports on-demand reporting requirements by offering the capability to parse audit records that have been saved to a file (see “-parseOnly” in the WLCAP README) and generating a report based on that data. |
| AU-7 | AU-7 (a) | CCI-001880 | The Windows Log Collector And Parser (WLCAP) PowerShell script provides a report generation capability (IAW AU-6) that:  Supports on-demand after-the-fact investigations of security incidents by offering the capability to parse audit records that have been saved to a file (see “-parseOnly” in the WLCAP README) and generating a report based on that data. |
| AU-7 | AU-7 (b) | CCI-001881 | The Windows Log Collector And Parser (WLCAP) PowerShell script provides an audit reduction capability (IAW AU-6) that:  Does not alter the original content or time ordering of audit records by using FIPS 140-2 validated hashing algorithms to verify the integrity of files anytime they are moved and using a read-only PowerShell function to read from the audit record files. |
| AU-7 | AU-7 (b) | CCI-001882 | The Windows Log Collector And Parser (WLCAP) PowerShell script provides a report generation capability (IAW AU-6) that:  Does not alter the original content or time ordering of audit records by using FIPS 140-2 validated hashing algorithms to verify the integrity of files anytime they are moved and using a read-only PowerShell function to read from the audit record files. |