Published Report: Acme HIPAA Compli | Print

Date **Sep 10 12:00:00 AM** to **Sep 10 11:59:59 PM**

This report is based on guidance from the HIPAA. For security logs to be useful in the defense of information assets, they must be monitored and analyzed. To generate this report, EventTracker receives, processes, alerts and summarizes log data from all sources in scope as described in this solution brief. Review this report regularly to satisfy the Log Monitoring requirements of HIPAA. If you would like to get more information or have questions regarding HIPAA, email us at essentials-support@eventtracker.com

Section 164.308(a)(1)(ii)(D)

Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.

Windows Audit Log Cleared.

Description: Below listed audit log clear activities were observed.

Recommendation: Review the audit log clear activities listed below and confirm if they are legitimate.

2 INCIDENTS: SHOW

Section 164.308(a)(4) and 164.312(a)(2)

Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicable requirements of subpart E of this part.

Windows Administrative Activity.

Description: Below listed windows administrative activity were observed.

Recommendation: Review the windows administrative activity listed below and confirm if they are legitimate.

7 INCIDENTS: SHOW

Section 164.308(a)(4)(ii)(B)

Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism.

Windows Identification and Authentication Mechanism Activity.

Description: Below listed user activities were observed.

Recommendation: Review the user activities listed below and confirm if they are legitimate.

2 INCIDENTS: SHOW

Section 164.308(a)(4)(ii)(C)

Implement policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.

Windows Elevation Privilege Activity.

Description: Below listed privilege elevation activities were observed.

Recommendation: Review the privilege elevation activities listed below and confirm if they are legitimate.

2 INCIDENTS: SHOW

Section 164.308(a)(5)(ii)(C)

Procedures for monitoring log-in attempts and reporting discrepancies.

Windows User Logon or Logoff Success.

Description: Below listed user activities were observed.

Recommendation: Review the user activities listed below and confirm if they are legitimate.

4 INCIDENTS: SHOW

Windows Security User Pre-Authentication Failed.

Description: Below listed user logon failures were observed.

Recommendation: Review the user logon failures listed below and confirm if they are legitimate.

1 INCIDENTS: SHOW

Fortinet User Authentication Success or Failed.

Description: Below listed user activities were observed.

Recommendation: Review the user activities listed below and confirm if they are legitimate.

4 INCIDENTS: SHOW

Fortinet Administrator Logon Success or Failed.

Description: Below listed admin activities were observed.

Recommendation: Review the admin activities listed below and confirm if they are legitimate.

0 INCIDENTS: SHOW

Fortinet VPN User Logon Success or Failed.

Description: Below listed VPN activities were observed.

Recommendation: Review the VPN activities listed below and confirm if they are legitimate.

1 INCIDENTS: SHOW

Section 164.308(a)(6)(ii)

Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity; and document security incidents and their outcomes.

Fortinet Attack Detected on System.

Description: Below listed attacks were observed.

Recommendation: Review the attacks listed below and take the necessary actions.

2 INCIDENTS: SHOW

Fortinet Data Leak Detected on System.

Description: Below listed data leaks were observed.

Recommendation: Review the data leaks listed below and take the necessary actions.

2 INCIDENTS: SHOW

Fortinet All Suspicious Web Content Detected Report.

Description: Below listed All Suspicious Web Content Detected were observed.

Recommendation: Review the windows administrative activity listed below and confirm if they are legitimate.

1 INCIDENTS: SHOW

Fortinet All Suspicious E-mail Content Detected Report.

Description: Below listed All Suspicious E-mail Content Detected were observed.

Recommendation: Review the windows administrative activity listed below and confirm if they are legitimate.

1 INCIDENTS: SHOW

Section 164.312(c)(2)

Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.

Windows System Level Object Created or Deleted.

Description: Below listed system level object activities were observed.

Recommendation: Review the system level object activities listed below and confirm if they are legitimate.

2 INCIDENTS: SHOW