HIPAA integrity controls

In a healthcare organization, you must implement policies and procedures to ensure that electronic protected health information (e-PHI) is not improperly altered or destroyed. These searches show users with a large number of modification events so their activity can be monitored easily and they can be traced back quickly if any suspicious events are detected.

Required data

- Endpoint data
- Medical device data
- Database data

To optimize the searches shown below, you should specify an index and a time range. These sample searches use Cerner audit logs. You can swap out this data source for ones in use at your organization, changing field names as necessary.

Record actions

To count the number of events recorded your patient record system, run the following search.

    sourcetype="cerner_audit_log" | stats count BY EventName

Modification events

To see the details of healthcare records that have been modified, run the following search.

    sourcetype=cerner_audit_log
    EventName="Write/Update Results" OR EventName="Add" OR EventName="Sign" OR EventName="Modify" OR EventName="Modify Details" OR EventName="Add/Modify and Review"
    | convert ctime(_time)
    | table _time, EventName, UserName, PrsnlName, Role, EventName, NetworkAccID
    | rename _time AS "Date/Time", UserName AS "User ID", PrsnlName AS "Name", EventName AS "Event Type",
    EventName AS "Event Name", NetworkAccID AS "Workstation"

To see the modifications in a timeline, change the search to the following:

    sourcetype=cerner_audit_log
    EventName="Write/Update Results" OR EventName="Add" OR EventName="Sign" OR EventName="Modify" OR EventName="Modify Details" OR EventName="Add/Modify and Review"
    | timechart count(UserName) BY EventType
Abnormal modifications events during a two-minute period

To calculate when a higher number of modifications than normal occurred, run the following search. In this case, an abnormal value is considered as 1.5 standard deviations from the average. You can change that value in the `where` command to fit your needs. You can also change the `time_window` to a value other than two minutes.

```
sourcetype=Cerner_Audit_Log (EventType=Modify OR EventType=View* OR EventType=Security) ParticipantName=* UserName=* | streamstats time_window=2min count AS Mod BY EventName UserName ParticipantName | table EventName UserName ParticipantName Mod | eventstats avg(Mod) AS avg stdev(Mod) AS stdev BY UserName | where Mod > avg+(1.5*stdev) | stats values(EventName) AS actions count BY UserName | rename UserName AS user | sort - count
```

Next steps

After running these access controls and taking appropriate action, you may want to look into other HIPAA controls:

- Access controls
- Audit controls
- Person or entity authentication
- Transmission security

The information provided in Splunk Lantern is intended for informational and educational purposes only. All information is provided in good faith, however, Splunk disclaims any and all representations and warranties, express and implied, regarding the information provided, including without limitation any warranties and representations regarding the completeness, adequacy or accuracy of the information. You agree to take full responsibility for the results arising from the use of the information provided.