Chad Ballay

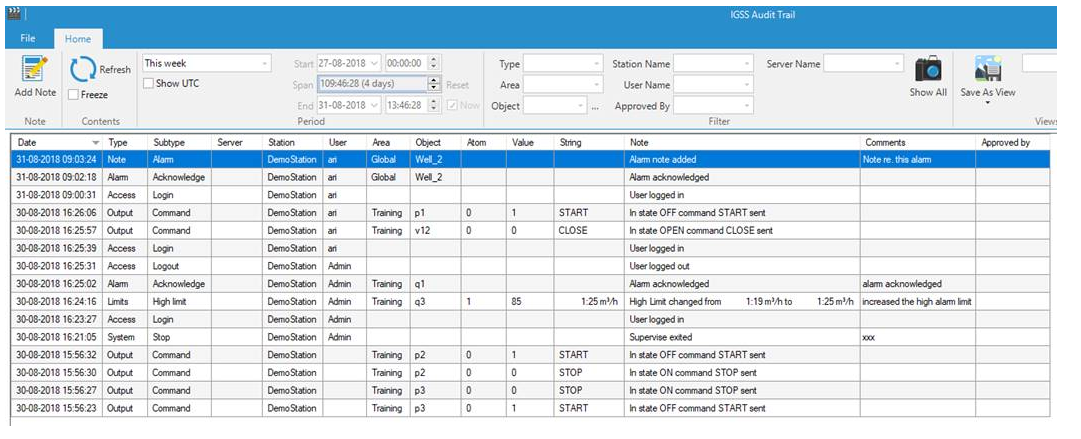
CYBR410-342

11/01/2020

Week 8 Module 1

What information is contained within an audit trail?

In the broader sense this contains all the relevant records that shows the events that occurred relative to the systems and interactions performed. Login events, file modifications, execution log files, etc., etc... The chronologically organized evidence of what occurred. Only facts though. An example would be the linked item. In it you can see how the user progressed through their session.

<https://www.igss.com/Files/Doc-Help/Webhelp/V14/AuditTrail/Audit%20Trail%20Program/What%20is%20IGSS%20Audit%20Trail.htm>

Specific to databases, audit trails will be focused on the data transformations that occurred. What queries were run? Who ran them? When did they run them? The format of these reports and the tools that generate them will vary widely based on the database technology involved. A defining need is will it pass the required legal and compliance needs. For many industries this would SOX, PCI, or HIPAA but increasingly the need for audit trails are becoming a precondition to the work rather than a nice to have.

# What are the advantages and disadvantages of using an audit trail?

The biggest advantage is the observability it provides to what is occuring on your system. At no point has anyone wished they didn’t have the data needed to troubleshoot an issue. They may wish for less data but really mean a better way to parse the data. They may wish for a more standard formatting of the data for analysis. But never has anyone said they would rather not be able to understand what happened.

The disadvantage comes with performance and cost. Data capture and storage is not free. Streams of data must traverse the network, be captured, and interpolated, get stored, etc., etc... All of these costs in person-hours, infrastructure, cloud cost, support, SLA enforcements, etc., etc... means real world dollars must be spent here on things that may never be used. There is a trade off between “nice to haves” and “must haves” that there is no single right answer. There is just a good enough answer and the need to monitor and adjust as the situation changes.