Incident Overview: SafetyDetectives discovers 6.5 TB of sensitive data exposed on a Turkish-based Pegasus Airlines AWS S3 bucket. The open bucket was discovered by the cyber security team on 28 February 2022 as part of a large-scale web-mapping project.

The team subsequently contacted the airline on 1 March 2022 regarding the open S3 bucket. On 20 March the team sent a follow-up message to Pegasus and reached out to PegasusEFB. Finally, on 24 March the Safety Detective team responsibly disclosed the data exposure to Pegasus EFB after contacting the company.

Impact Assessment: Highlight the extent of the damage or disruption, such as:

Number of systems affected: UnKnown
Estimated downtime or operational impact: N/A
Financial implications: Unknown
Any sensitive or personal data that may have been compromised: **3.2 million files containing sensitive flight data.**

Cause of the Incident: A bucket is used by AWS customers to store related data and objects. The Pegasus EFB bucket's security settings were misconfigured, meaning it was left open and could be easily accessed by anyone.

Response and Mitigation Steps: The team reconfigured the AWS bucket properly by restricting access. They followed the outlined steps provided by amazon web services.

Lessons Learned: I think the biggest lesson learned from this incident is that the cloud is a shared responsibility. Even though Pegasus was using amazon web services, they needed to configure their buckets properly. This is a good lesson for the future, to always configure your security settings properly. Maybe even test the settings in an offline setting before deploying to a live environment where millions of peoples information can be freely accessed.