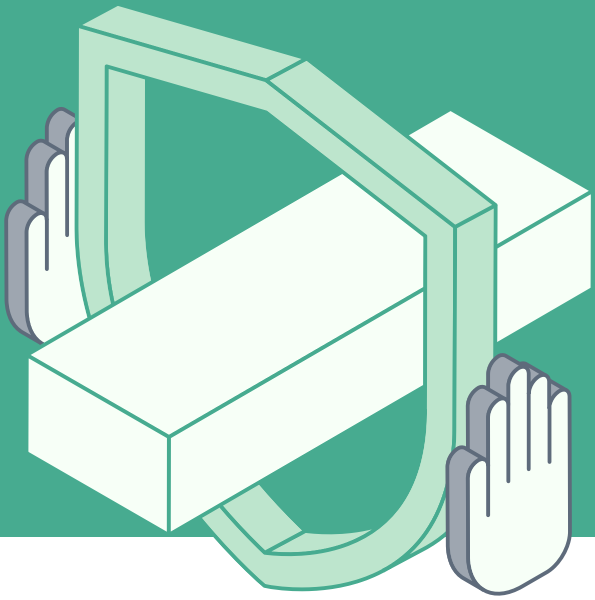
CLOUDYRION

Big Data Security in the Tech Industry

A tech company with a focus on telecommunications wanted to transfer large amounts of customer-related data from different resources to a central environment as cost-effectively as possible. An IT security concept was required for the migration and subsequent access. The tech provider entrusted Cloudyrion's experts for holistic IT security and an implementation in accordance with the security-by-design approach.



STARTING POSITION

Nowadays, both private and enterprise customers of telecommunications providers expect tariffs to be tailored to their individual needs as cost-effectively as possible. In order to offer its existing customers rate adjustments based on business intelligence (BI) analysis and to capture and evaluate the performance of individual customers, the tech company decided to establish advanced Big Data analytics and machine learning processes. The goal: to create a foundation for analytics that included benefits for both customers and the vendor.

A major challenge was to establish a centralized data repository that would meet the stringent requirements for the security of critical data. Which cloud provider would be the right one? Which met all of the criteria in terms of privacy as well as security and offered the infrastructure to properly implement the desired architecture? To answer these security-related questions while maintaining the applicable compliance requirements, the tech company went in search of a qualified IT security partner. The company learned of Cloudyrion through recommendations from its network and contacted the IT security specialists. The major plus points of Düsseldorf security experts' market presence included comprehensive consulting, technological expertise and solution-oriented, pragmatic assistance from a single source.

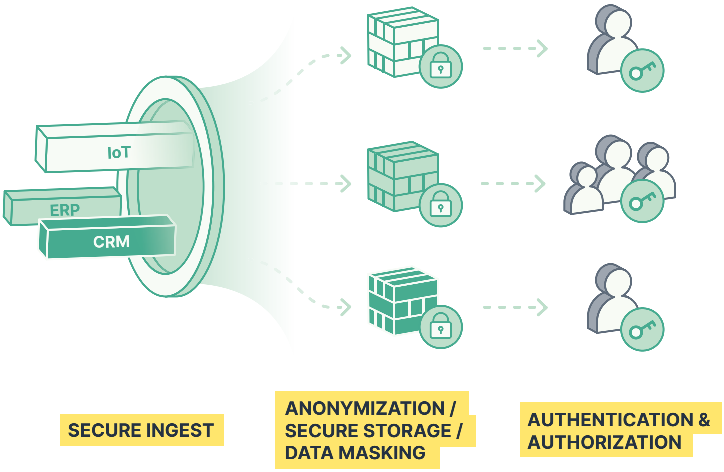
CHALLENGE

Although the company had already chosen a Big Data environment, it had not yet been put to the test in terms of security. A systematic reverse engineering approach was needed to ensure that the three key security-relevant areas in the Big Data Analytics segment were effectively addressed and covered:

- **Minimization of attack surfaces through configuration and vulnerability analysis**
- **Secure data transmission (data-in-transit encryption)**
- **Secure data storage (data-at-rest encryption)**

The focus included access permissions, encrypting data as it is sent and data integration patterns that standardize what data can go in and out of where, as well as who has access to the data lakes (cold/warm storage) and BI tools. The „need to know" principle provided a practical framework for implementing secure role management. According to this principle, everyone who works operationally with the data is only given access to what they need for their specific tasks. Usually, the management of access authorizations in big data environments tends toward clutter - a thoroughly dangerous setup. Beyond the legal requirements, which are anchored in the EU Data Protection Regulation, data security is fundamentally extremely valuable. As soon as breaches, negligence and security incidents become public, the affected brand suffers image damage that is almost impossible to repair. In addition, the compromising of particularly sensitive data assets can severely damage the company's core business and, in extreme cases, even jeopardize its continued existence. With a clear focus on security and support from Cloudyrion, the company needed to create clarity around role management with a view to data security and compliance.

The set time frame for the project extended to six months. During the implementation, the high availability of data for authorized users was to be ensured at all times.


IoT
ERP
CRM
SECURE INGEST
ANONYMIZATION / SECURE STORAGE / DATA MASKING
AUTHENTICATION & AUTHORIZATION

SOLUTION

At the beginning of the project, Cloudyrion worked with the company to define the data integration patterns for the Big Data environment. At the core of this was defining the logic behind the dashboards used and who would be given the authority to change them as needed. The security experts provided advice on the following topics, among others:

- **Establishing data transparency using data asset inventory / data catalogue (missing data discovery and mapping)**
- **Data classification on four levels from C1 to C4**
- **Data protection (data leakage/loss prevention)**
- **Secure data source integration and data validation**
- **Securing of data lakes (ETL and ML pipelines)**
- **Masking or anonymization of data sets**
- **Creation of an asset inventory in the form of a data catalog**
- **Data retention**
- **Secure data backup**
- **Identity management (identity access management)**

The last point focused on questions regarding the assignment of roles to users. What roles are there? How are they assigned, revoked and released? How can the whole be audited? It was necessary to note that all processes that were reviewed and, if required, adapted in accordance with the above inventory method were compliance-relevant for the company.

In addition, the experts identified weaknesses and errors in the already-implemented live environment and corrected them iteratively. To this end, they conducted specific audits, as well as penetration tests, to find attack surfaces and close gaps. This process was carried out using reverse engineering, going backward step by step through all levels to the solution's original design. On the basis of the findings obtained up to that point, the solution was adapted in accordance with the security-by-design approach.

To ensure the long-term high availability of the data and data lakes, the Big Data solution was originally set up in a multi-cloud environment. Most common cloud service providers structurally support this, but their security tools have a relatively high rate of false positives when it comes to identifying correct data patterns. This was a challenge that the entire team learned to deal with, thanks to support from Cloudyrion.

OUTLOOK

After reaching the milestone set for six months, the company engaged Cloudyrion to continue to drive and monitor the implementation of security-by-design and compliance with the associated principles beyond the initial project period. This deepened the trusting cooperation between the teams on the client's side and the consultants. As a result, the company's general awareness of security issues increased significantly. Unannounced audits, which Cloudyrion carries out repeatedly at irregular intervals within a system environment that has continued to grow, also contribute to continuously detecting and closing vulnerabilities. In addition, Cloudyrion is available to provide support for particularly challenging issues.

BENEFITS AND EVALUATION

In practical implementation, it turned out to be a challenge to provide users with the necessary skill set to work confidently with the system. The learning that was ultimately achieved, however, shows that the effort was worthwhile. „Generally speaking, security-related errors made by employees are not intentional, but unknowingly done. However, the goal must be to ensure that these errors never reach the productive environment," explains Okay Güler, Founder & IT Security Consultant at Cloudyrion. „Our customer and its workforce therefore particularly appreciated our solution-oriented approach and flexibility in helping people on the ground develop security know-how in the Big Data context, imparting it to them and anchoring it sustainably in the processes."

Key achievements at a glance

- Secure storage and access to data
- Compliance with internal company policies
- EU-DSGVO compliance
- Implementation of „what good looks like" data integration patterns
- Much faster processes
- Validation of incoming data from a security perspective
- Increasing know-how in the workforce
- Clear assignment of tasks and roles for users

Are you looking for a reliable partner who supports your team, successfully implements ambitious and security-critical IT projects, and can guarantee long term availability?
Get in touch - we would love to help.