

How the Cloud Protects Employees

Setting up a Threat Management Assistant (TMA) System according to AWS best practices



“With the AWS-based solution our threat management process receives a new level of efficiency. Furthermore we are able to convert the TMA into a market offer in the medium term.”

Claudia Brandkamp, Threat Management, Deutsche Telekom

While the companies are focusing on the external threats perpetrated by cyberbullying, they tend to overlook the internal threats that pose a great risk to the safety and security of their employees. According to a current study about 25 percent of German workers claim to have been victims of some form of physical or psychological violence at work in 2019. And in other countries the situation doesn't differ too much. In some cases, an ongoing bullying can even lead to suicidal ideation.

Deutsche Telekom AG is engaged for an employee-friendly workplace environment taking threats and bullying seriously. Since 2014, the company has established a threat management system to protect employees against all kinds of violence, financial and personal stress that eventually results in corporate risk. The aim of the company is to ensure that each employee is treated with dignity and respect in an effective, uncomplicated work environment. The threat management process is not only relevant in Germany, but in all local business units of Deutsche Telekom.

At a glance

The personnel security team along with the advisory council worked together with experts from the University of Berlin to avoid threats as well as to deal with all kinds of viciousness such as psychological abnormalities, radicalization and any other sort of targeted violence. To achieve this goal of mitigating threats, the threat management works ensuing three steps: recognition, assessment and defusion. The original doc- and e-mail-based process was not enough. Thus the team decided to set up a digital process based on AWS Cloud. In a first step the digital solution should optimize the threat management – with the perspective to offer the service to other companies.

- Process support improvement for threat management
- Scalable solution on AWS Cloud
- Using the best practices of the well-architected framework
- Fulfilment of high data privacy and security demands

Reference in detail

The challenge

An effective collaboration with different experts such as labor law, compliance, HR, etc. is essential for the threat management. Currently, all steps are monitored with word documents and e-mails, which is manual and cumbersome making it very difficult to manage. In order to enhance the collaboration and the documentation, a digital process-supporting system, the Threat Management Assistant (TMA), should be implemented. The new system should also incorporate scientific models to help to evaluate the respective monitored employee situation. Those scientific models will be continuously developed so the new system needs to support continuous development/continuous integration (CI/CD). As the team plans to offer the TMA to other companies, they opted for a platform that could easily scale up according to market demands: AWS Cloud. Additionally, due to the nature of the project, the new system should be built in a secure environment to store and share documents. With the business idea in mind the team searched for a partner that could take over the technical realization of the project and the ongoing management of the service. They chose T-Systems.

The solution

The T-Systems team built up the system based on the business demands and according to AWS best practice of the well-architected framework. This ensures not only scalability and CI/CD, but as well a high level of security for an efficient and sophisticated system. AWS CloudFormation provides the necessary infrastructures as code. After setting up the infrastructures, the T-Systems team introduced the security features using Key Management Service, AWS Certificate Manager and SSM parameter store for passwords and parameters. Data at rest (in Elastic Block Store and the PostgreSQL database) and in transit are encrypted accordingly. The cloud-native TMA application was established in the AWS Cloud in Frankfurt. Ruby on Rails was used as web application framework. It also introduced containerization (Docker) based on Amazon Elastic Container Service as a fully managed container orchestration service. It allows easy running of applications on a managed cluster of Amazon EC2 instances. Deployments are done with Code Pipeline. PostgreSQL is used as database. A multi-AZ setup realizes high availability and failover support. WordPress is operated for the documentation process. Monitoring is done via Amazon Cloud Watch. The future-oriented method to have an effective solution easily passed an AWS well-architected review. The application can be scaled easily and additionally fulfils all important security aspects. This project jointly developed a best practice (network & tool) solution for all units of Deutsche Telekom group.

Customer benefits

Today, threat management is an integral part of Telekom security in Germany. In fact, Deutsche Telekom AG is the first company in Europe with a professional and firmly established Threat Management Assistant system. The TMA allows clear communication and collaboration beyond different units which is important for a successful threat management within the company. Thus, the cloud solution improves the efficiency of the process. Furthermore, the solution fulfils all the various business demands of the personnel security team: flexibility, security, scalability as well as improved business continuity. The setup allows the continuous optimization of the tool with improved scientific models for a sophisticated threat management and employee support. Last, but not least the solution enables the Threat Management Assistant to be offered to the market. Research shows that there is huge demand at multi-national enterprises for such a tool. With the incorporated know-how and the ready-to-go solution Deutsche Telekom becomes a top-notch provider in this area.

Further benefits:

- Fast setup
- Better transparency
- High security and privacy level

Contact

T-Systems International GmbH
Hahnstraße 43d
60528 Frankfurt am Main, Germany
E-Mail: referenzen@t-systems.com
Internet: www.t-systems.com

Publisher

T-Systems International GmbH
Marketing
Hahnstraße 43d
60528 Frankfurt am Main
Germany