Case Study

DTIT Security Incident Remediation API

In cooperation with

aws PARTNER Premier Tier Services

Executive summary

When security incidents occur, it's vital to contain them quickly before the damage spreads. In case of a breach, every second matters, but time is already precious for overstretched IT and security teams. As a consequence, it makes sense to automate security controls wherever possible, such as for isolating breached resources to limit the potential impact as well as unintended exposure of data or to prevent further propagation and unauthorized access.

T-Systems developed a security remediation API that codified most common manual steps and made it easier for incident responders to invoke the API to remediate issues, without any other dependencies. The solution focused on isolating IAM users and EC2 instances in AWS accounts, while using a standard deployment workflow for managing the infrastructure resources as code with automation in mind.

About the customer

DTIT is the internal IT service provider of Deutsche Telekom AG. DTIT is responsible for the design, development and operation of all its owned and transferred IT systems supporting business processes at Deutsche Telekom AG. DTIT creates user-friendly web portals with intelligent self-service functions as a basis for an integrated, cross-channel customer experience with the Telekom Magenta brand. DT IT is in the middle of a large-scale transformation program, adopting cloud as well as agile methods such as the Scaled Agile Framework.

As quoted by Andreas Proff, responsible as a Product Owner for DTIT's Security Monitoring - "The API developed by T-Systems allows us quick reactions on certain critical security incidents that might affect accounts in our AWS landing zone. Through the automated process, the reaction is executed in a predictable and timely manner, allowing forensics activities later on."

The challenge

In AWS Cloud, security incidents can be categorized on a high level as:

Infrastructure domain incidents – These incidents typically include network related or application's data related activities such as, the processes running on or traffic to Amazon EC2 instances within a VPC. The potential consequences resulting out of infrastructure domain incidents include compliance breaches, data theft incidents and operational downtime.

Service domain incidents – These incidents are typically handled through AWS APIs. While API's add value for millions of customers, these can get abused in case hijackers get unauthorized access to root credentials or IAM account. The most significant impact of service domain incident can be the inconvenience caused to end-users and uncalled interruptions to vital services, which often lead to reputational damage.

The process for addressing such security incidents for DTIT was long and time-consuming. Although Amazon GuardDuty findings, reported as security incidents, have been continuously monitored by the DTIT Cyber Defense Center (CDC), any incident response has been a manual effort: Based on an initial analysis, the incident is forwarded to a Lead Incident Manager (LIM) and delegated to the corresponding application support team for remediation.

Moreover, the long wait-time and risk of errors arising due to manual work, could lead to reputational as well as financial damage.

Solution architecture

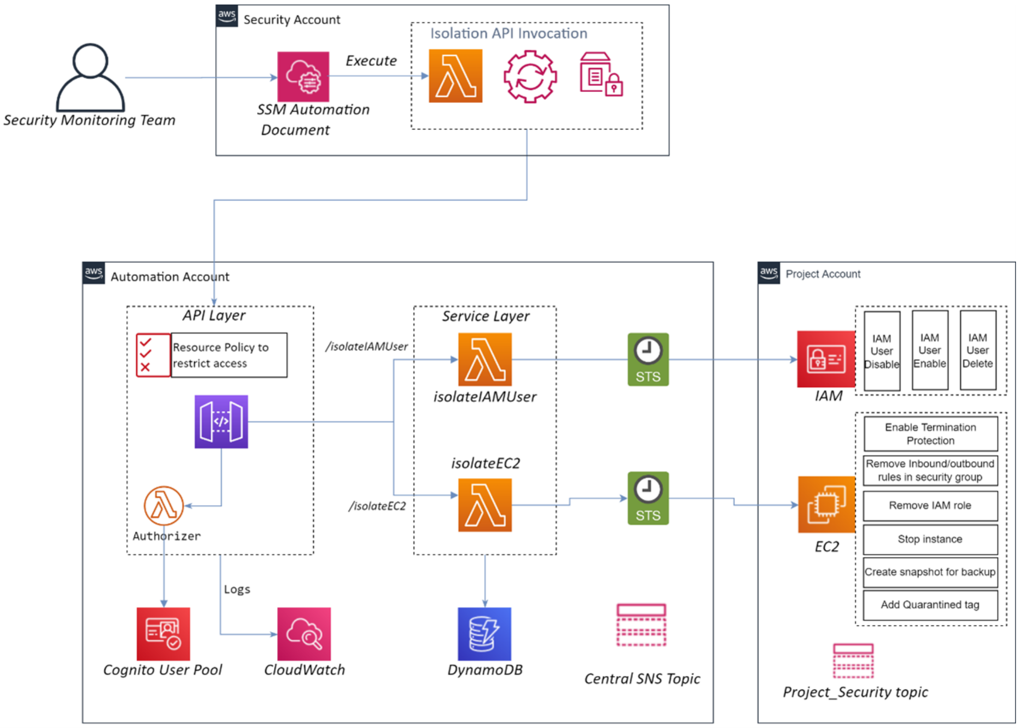
In order to save efforts and time on incident response, T-Systems was brought in to develop a security remediation API, codifying the most common manual steps. Incident responders now can invoke the API to remediate issues without any other dependencies.

The solution focuses on isolating IAM users and EC2 instances in AWS accounts. It uses highly secured REST APIs that integrate standard notifications to operations teams and account and application owners. The solution uses a standard deployment workflow and manages the infrastructure resources as code with automation in mind.

Resource isolation: The steps

On receiving an incident for resource isolation:

- Authorized user in security team logs in to security account and executes IAM user or EC2 instance isolation using SSM automation document.
- Rest API validates the user data and authenticity of the request and invokes the appropriate service securely.
- Isolation logic is implemented in the service layer using serverless AWS lambda functions.
- The respective lambda functions will assume permission to access the account to isolate the specified vulnerable IAM user or EC2 instance.
- On the target account, the vulnerable IAM user or EC2 instance is isolated.
- Resource isolation details are stored in DynamoDB for future reference.



The above diagram shows that several AWS services are used to set up the resource isolation API solution. These resources are provisioned and managed using Terraform as Infrastructure as a Code (IaC). We define a standard CICD approach with different environments for development, testing, and production use. All code developed and reviewed in the development environment is merged correctly and deployed to the test environment to validate the solution with functional test cases. After successful testing, deployment is performed to the production environment to enable the self-service security incident response API.

The benefits

Through codifying incident response runbooks and giving authorized access of the API to security team, DTIT was able to realize the following benefits:

- Preparedness – be ready for any eventuality, regardless of available human resources and expertise
- Consistency – a uniform approach to incident response, which can also support later investigations or forensic analyses
- Integrations – the API can also be used across non-AWS applications and systems

Why Amazon Web Services

AWS delivers even more scalability, better reliability, faster speed to market, and the power to drive innovation. Built by developers for developers to deploy quickly and seamlessly scalable secured infrastructure. These features allow developers and businesses to focus on improving and innovating their applications, rather than worrying about building and running identity.

AWS takes security as job zero and provides built-in services for security as well as best practices around cloud security in the AWS CAF, AWS Security Incidence Response Guide, and Well-Architected Framework. Automated procedures for security incident response are one of the recommended practices and should be in place in well-architected environments. Same for testing processes and security game days as preparatory measures for decreasing the time it takes to respond to critical security incidents.

About the partner

With a footprint in more than 20 countries, T-Systems is one of the world‘s leading vendor-independent providers of digital services headquartered in Europe. The Deutsche Telekom subsidiary offers one-stop shopping: from secure operation of legacy systems and classical ICT services, transition to cloud-based services as well as new business models and innovation projects in the Internet of Things. T-Systems also is an accredited AWS managed service provider and premier consulting partner with more than 500 experts on AWS and a growing list of competencies such as migration, SAP and well-architected.

In cooperation with

aws PARTNER Premier Tier Services

Contact

T-Systems International GmbH
Hahnstraße 43d
60528 Frankfurt am Main, Germany
Tel: 00800 33 090300
E-Mail: info@t-systems.com
Internet: www.t-systems.com

Published by

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

T Systems

Let’s power
higher performance

Last update: 04/2022 | Designed by: Creative Factory, TSIN