In cooperation with

aws PARTNER Premier Tier Services

Case Study

TMNL Security Architecture

Executive Summary

T-Mobile Netherlands (TMNL), Netherlands' largest mobile phone company providing wireless data and voice communication services, was looking for a new landing zone solution securing all their existing critical systems and accounts in AWS.

T-Systems was brought in to develop a cloud-native approach to security - key success factors being maintainability, automation, extensibility and reliability as well as centralized security logging, monitoring and auditing. The objective of the project covered detailed planning, design and implementation of the secure landing zone using Infrastructure-as-Code (IaC) and integrated centralized security management across a multi-account environment.

About TMNL

T-Mobile Netherlands is the major telecommunications provider in the Netherlands with more than 5.7 million customers, focusing on delivering cost-effective and quality solutions for personal mobile and broadband communication. The company offers cell phones and plans, internet services, applications, bundled packages, as well as other related products and services.

The Challenge

Being a telecommunications provider, there were multiple requirements, that had to be taken care of while setting up the new solution:

1. Network setup to enable **secure connection** from TMNL datacentre as well as from Internet to the applications.
2. **Centralized monitoring and alerting** across the organisations: TMNL required a single pane of glass to see the security posture of the entire organisation and manage security incidents.
3. **Strict data privacy and residency requirements:** EU only.
4. **Centralized security management and deployment:** All security tools and solutions should be centrally deployed and managed.
5. **Abuse and anomaly detection through tight cost controls:** Get notified on any inconsistencies or patterns.

T · · Systems ·

Let's power higher performance

Solution Architecture

T-Systems, as AWS Premier Partner, was chosen to develop the solution, advise on AWS best practises and implement those within the project scope. T-Systems together with TMNL created a project plan, set milestones, negotiated priorities, and did the implementation and testing. T-Systems fulfilled the transition from a legacy account provisioning automation to a new fully managed secured Landing Zone. The first milestone of this journey was to build a revised Multi-Account setup, made up of different Organizational Units (OU) on which different Service Control Policies were applied according to the account type and purpose. Infrastructure is created by a fully automated continuous delivery approach. This has helped in seamless delivery of infrastructure, using Terraform as Infrastructure-as-Code Tool.

Preventive Controls

After the initial Organisation and account setups, **Service Control Policies** were deployed to meet the **Data privacy and Data residency** requirements. **Region restrictions** were applied with AWS SCP, which ensured the data and access to be only in the specified region . Also, additional restrictions for creation of resources that do not have **required tag** to control the cost and for enhanced security was deployed.

All accounts are connected to TMNL Azure AD and provide **Single Sign on** functionality so that users can interact with AWS console and CLI.

In addition to the Service Control Policies, **AWS Config** was configured to meet the Privacy and Security Assessment (PSA) requirements. Multiple rules are configured and auto remediated on non-compliance. This gives the customer a fully automated process to have a compliant architecture and proactive management of any configuration issues. As a part of compliance requirements, defined compliance rules using AWS Config and **non-compliance are remediated.**

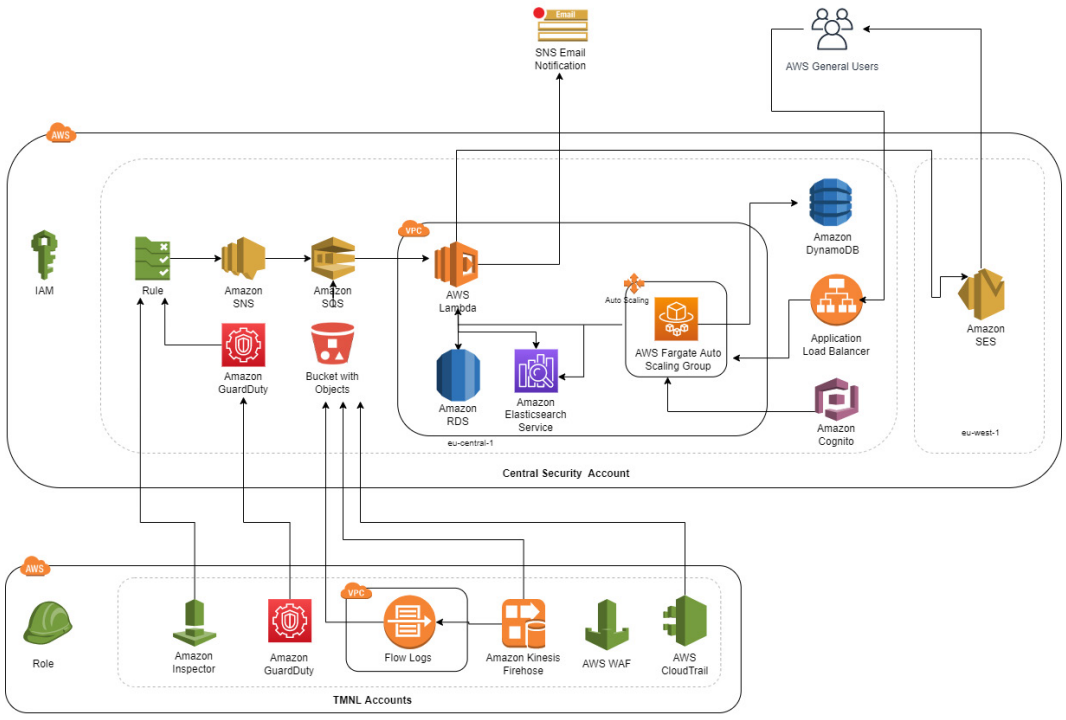
By implementing these rules, TMNL can quickly detect any deviation from their compliance state and auto-remediate most of the issues. Weekly compliance reports are sent to TMNL. Compliance status data is pushed to the central monitoring solution for TMNL to visualize and take required actions in use cases where auto-remediation is not agreed upon.

Centralised Security Analysis & Dashboard

Logs from all accounts (Cloudtrail, Config, Guard Duty, VPC Flow Logs, Inspector) are sent to a central SecDevOps account and then analysed and visualised in a **central dashboard** based on grafana. Security Incidents are managed as per TMNL incident management process and sent to the operations ticketing tool.

Technically, whenever a new log entry happens, an SQS queue is triggered, that invokes a lambda „Log- Aggregator“ function, storing logs in Elasticsearch and Aurora DB. The lambda function is also configured to capture issues right away and notify the Ops team. Similarly auto-remediation, separate Lambda function, can be triggered based on certain filters.

Centralized Security Architecture:



The Benefits

As a result of this solution, TMNL has created a centralized view on their security posture and achieved the following benefits:

Security policies and standards - tracking information security policies and standards and make sure IT systems are in compliance with policies and standards, and alert about violations in real time.

Access and authentication - monitoring account creation, change requests, and activity by users.

Network security - monitoring alerts from Cloudtrail, VPC Flowlogs, Guarduty and WAF etc, and identifying known attack patterns in network traffic.

Log monitoring - aggregating security events and alerting on invalid login attempts, port scans, privilege escalations, etc.

Segregation of duties - Using least privilege access control policies and SSO.

Improve federation by enabling seamless login using corporate credentials for corporate users.

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.

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 advanced 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

Publisher

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

T · · Systems ·

Let's power higher performance

Last update: 03/2022 | Designed by: Creative Factory, TSIN