SUCCESS STORY

Estonian health and welfare organization cuts MTTR by 40% with Elastic

Region
Estonia

Industry
Public sector

Solution
Elastic Security,
Elastic Observability,
Elastic Cloud Enterprise

Lowers MTTR by 40%

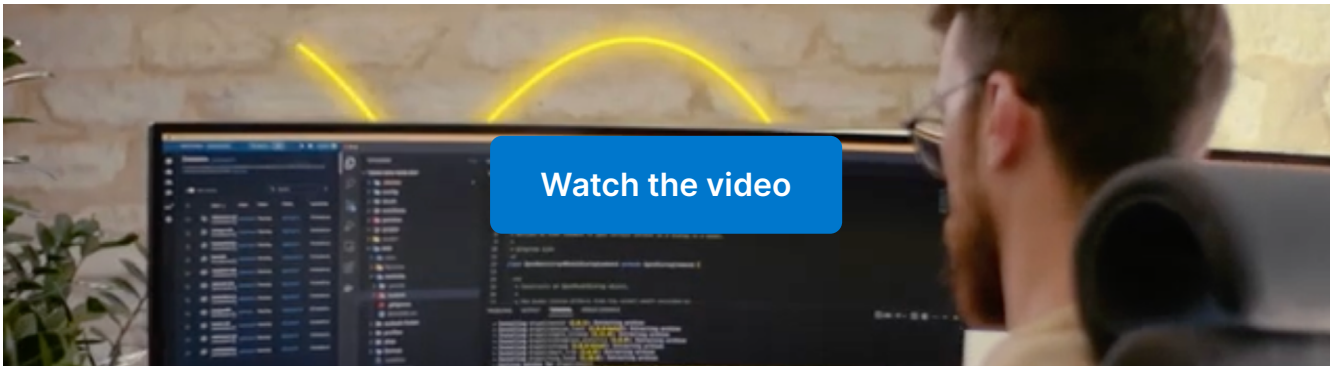
With Elastic, TEHIK expects to streamline incident management, cutting mean time to resolution (MTTR) by 40%.

Shortens control and audit processes from days to minutes

Multiple teams within TEHIK, including the control and audit departments, have cut the time of common processes from days to just minutes.

Establishes a roadmap to generative AI

With its existing Elastic license, TEHIK can deploy Elastic AI Assistant, guiding analyst workflows and broadening adoption of existing security tools..

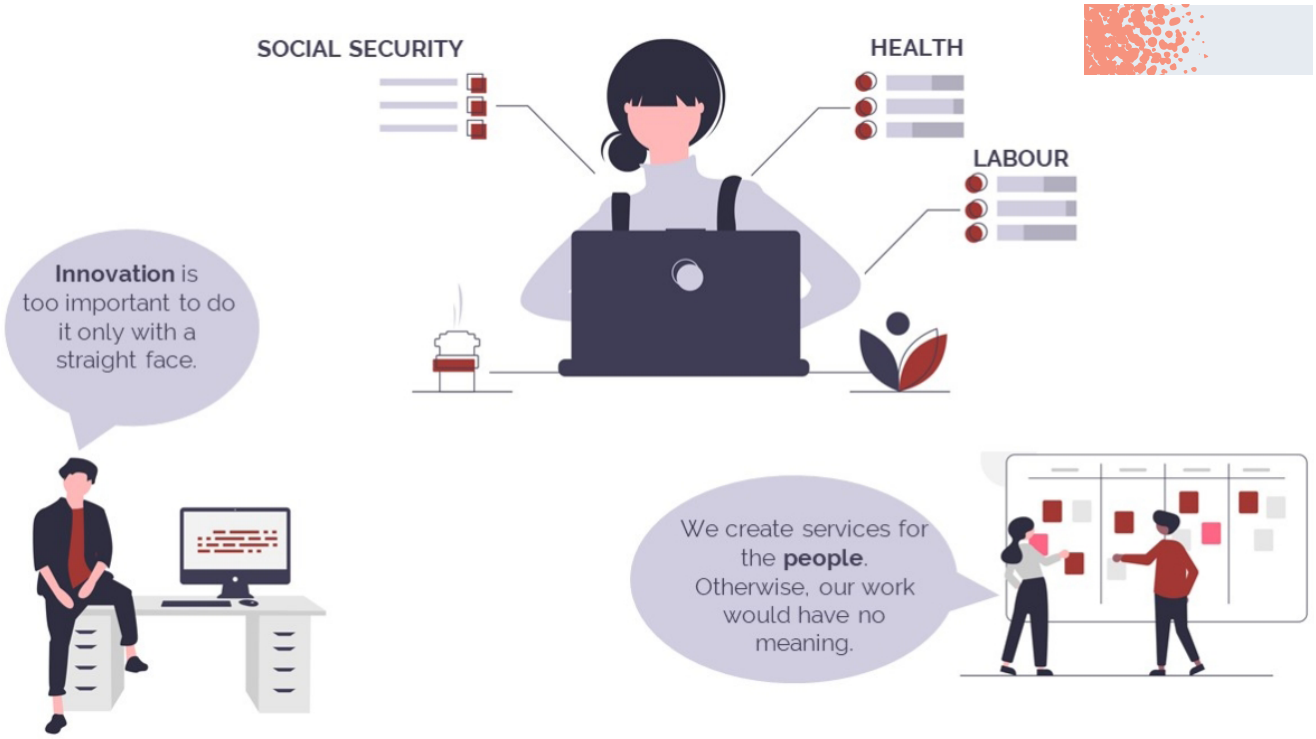


TEHIK strengthens citizen data protection and accelerates root cause detection and resolution with Elastic

In the heart of Tallinn, Estonia, The Health and Welfare Information Systems Centre (TEHIK) serves as a cornerstone in the digital transformation of the country's public services, including health, social security, and labor. One of its key responsibilities is providing these organizations with a secure environment for the storage and sharing of citizen data between various stakeholders such as health professionals and social care workers.

Anto Kallas, Information Security Specialist, TEHIK, stresses the complexity of working across several organizations and software ecosystems. "The technological demands of managing legacy software and the constant need for event data collection and monitoring require significant resources. We've always been proactive when seeking out solutions that enable us to gather, analyze, and respond to security and telemetry data across our software systems."

Estonia's stringent legal framework, which restricts public cloud usage is another challenge. This applies particularly to sensitive data handling, where national regulations govern processing and privacy. As a result, Estonian government institutions such as TEHIK must explore options such as private clouds or hybrid solutions that provide cloud computing benefits while respecting legal boundaries.



(TEHIK – the competence centre for the e-services in the fields of health, social security and labour was created in 2017 in the governance of the Ministry of Social Affairs.)

Reducing time for critical business processes from days to minutes

This journey began in 2014 when Kallas and his team first started working with a free and open version of Elastic. Since then, the team upgraded to a commercial license, introducing Elastic Security and Elastic Observability which provide a comprehensive, compliant toolset for sensitive operations. The country's regulatory restraints on public cloud usage brought TEHIK to choose the Elastic Platform deployed on containers in their own datacenter, which enables it to provision, manage, and monitor Elasticsearch and Kibana on-premises with all the advantages of a private cloud platform.

The collaboration with Elastic transformed TEHIK's approach to data analysis and system management. Elastic features such as correlation and GeoShape analysis, coupled with user-friendly machine learning tools, significantly enhanced its ability to spot data misuse. "The efficiency of this process is remarkable. By utilizing the Kibana discovery view, we are able to locate all user activities in the information system within seconds," says Kallas.

The internal control and audit departments have expressed exceptional satisfaction with the solution. Procedures that previously took days to accomplish can now be completed in minutes. Instead of focusing on data collection and processing, Kallas and his team can dedicate time to formulating and testing new hypotheses to thwart sophisticated adversaries.

Making machine learning available to all

Detecting and triaging suspected attacks quickly is a key challenge for most organizations. Most security operations teams spend more time ruling out false positives than chasing cybercriminals on the cusp of inflicting damage.

TEHIK is flipping this ratio with Elastic Security. "Machine learning, which once seemed like state-of-the-art technology, has become a daily tool for administrators at TEHIK," he says. Improved system transparency also plays a key role. "Elastic Observability is a vital addition to our institution, enhancing our toolkit for faster and more expert incident resolution," adds Kallas.

> Elastic's machine learning and other advanced capabilities have made these once complex concepts practical for regular users.

Anto Kallas
Information Security Specialist, TEHIK

Reducing MTTR by 40%

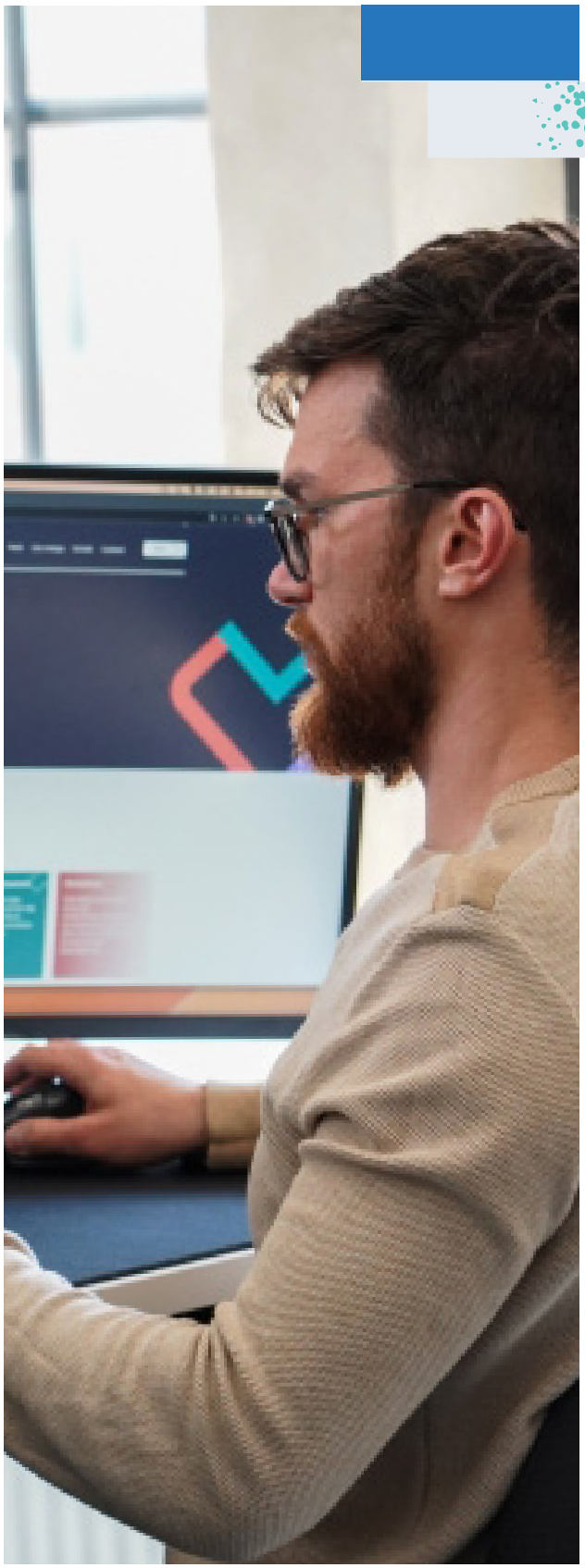
TEHIK has seen a significant reduction in response times and root cause identification. “Previously it was difficult to spot and rectify faults, adding to the cost of maintaining our software,” says Kallas. “But with Elastic we can spot issues at a very early stage, significantly decreasing the number of system interruptions.”

In the coming year, TEHIK anticipates a substantial improvement in mean time to resolution (MTTR), expecting it to decrease by at least 40%. This can be attributed to several factors, including the implementation of tools such as application performance monitoring (APM). These enhance visibility into system operations, enabling TEHIK to identify and address the root causes of operational incidents faster. “The ability to involve smaller, more agile teams in incident response, enabled by these tools, also contributes to more efficient operations,” says Kallas.

Reducing pressure on resources

More effective mitigation processes have also reduced the pressure on Kallas and his team. “With Elastic we can discover the real reason for a problem quickly and more precisely. You can manage your systems with a smaller team and free up resources to deliver more value to the business.”

On top of its advanced security and observability features, Kallas also values the Elastic team for their guidance and support. “The people at Elastic not only understand our business, they are also proactive when suggesting ways that we can improve our deployment. We have a hotline to a local Elastic expert who can resolve issues in hours or less.”



(TEHIK uses manages over 40 databases, creating essential e-services for almost 1.3 million people, using state-of-the-art and secure infotechnological solutions)

elastic

Fast forward to generative AI

Looking to the future, Kallas sees immense potential for the deployment of Elastic AI Assistant, a generative AI tool powered by Elasticsearch Relevance Engine (ESRE). This enables users to interact with Elastic Security and Observability for tasks such as alert investigation, incident response, and query generation using natural language.

“Elastic AI Assistant enables you to distribute security analysis to other areas of the business, not just the InfoSec department. This potential shift not only enhances resource efficiency, but also contributes to the sustainable development of talent within the organization,” he says.

> By enabling a wider range of staff to engage with complex data processes, the Elastic AI Assistant is not just a tool—it is a catalyst for fostering a collaborative and empowered workforce.

Anto Kallas
Information Security Specialist, TEHIK