Roadmap to zero-trust

A pragmatic approach to a better security posture

Your Challenge

A transformation to the cloud will bring new challenges to keep you safe from cyber threats. Misconfigurations or inadequate controls can expose your data which could lead to loss of intellectual property or personal information. This can have a large impact on your brand and trust of your customers and partners.

It is a complex exercise to build an appropriate security architecture in a cloud environment. While many organizations only think about a lift-and-shift approach of their existing IT-stack, security cannot be replicated asis to a cloud environment.

The shared security responsibility with cloud service providers demands a specific approach to build your security posture. When working to build or improve your organization’s security posture in the cloud, there are several best practices that you can implement to help identify gaps in security controls and quantify risk. But which of these advisories are absolutely necessary to reduce your risks and which of these are nice to have and help and support your business goals.

Devoteam can help you to identify the gaps and define security controls that are the right solution for your specific needs. As such, we will support you to develop a sound security posture that allows you to maintain continuous visibility on your current security state and desired goals. This guarantees that your cloud transformation and operations are fully secure in line with your specifications.

Benefits

This exercise allows you to improve your security posture and supports to maintain it while your cloud infrastructure is evolving through:

- An improved security posture
- Compliancy towards pre-defined security controls
- Visibility of security gaps in your current cloud environment
- Immediately Detect gaps in newly deployed cloud services
- Reporting providing insight in your current security compliancy
- a solid basis for further development such as automated security controls and automated incident management.

Roadmap to zero-trust

A pragmatic approach to a better security posture

Our Offer

Devoteam offers a cloud security posture improvement exercise that allows you to verify your environment continuously on a set of pre-defined security controls. The goal is to validate the compliancy to these controls and to evaluate the gaps through a dashboard.

Step 1 – Kick-off: Devoteam will align with all stakeholders to explain the goals and the approach of the exercise. Our Security consultant will present an overview of Zero-trust to ensure common understanding of the methodology. In this workshop we're also interested to get feedback about your business goals and needs in order to maximize the value of the outcome of the assessment. The result of the workshop is to agree on the overall scope and expectations of all parties involved.

Step 2 – Discovery & Gap Analysis: During the discovery phase, we review the environment based on architectural documents, policies, processes as well as interviews with several key IT staff within your organization. The goal is to identify which assets are critical and to review the current technical setup. After the discovery, a deep dive comparison aligned with the Zero-trust strategy will bring up a list of gaps and areas of improvement

Day 3 – Compliance definition: After analysing the collected data, we provide you relevant and contextualized recommendations and an action plan to improve your security posture, leveraging as much as possible the existing tools and technologies. We also help you to identify the key benefits which can be communicated to your management to support the migration to the zero-trust model.

The outcome will be a roadmap with a list of immediate activities and quick wins; a list of activities to cover critical risks, planned for execution within 5 months and a list of activities to improve ©