devoteam

Microsoft

Cloud Enabler for **SIEM**

Streamline security operations with smart analytics

24 May 2024

Anders Kristiansen

Status: WIP

Version: 1.0

Be guided by tech natives

Cloud Enabler
by Devoteam

Azure Sentinel is the fastest security information and event management (SIEM) system

Everything you need in a battle-tested, ready-to-go package

Building a comprehensive solution for all your security needs can be painstaking work.

Microsoft's cloud-native SIEM Azure Sentinel can offer an overwhelming set of choices if you don't have a clear idea of what your enterprise needs.

To accelerate the implementation of your cloud security operation, our experts created a scalable and cost-effective framework for Azure Sentinel.

devoteam

Cloud Enabler
by Devoteam

Cloud Enabler for SIEM framework provides a cost-effective and scalable **enterprise-grade** cloud security operation tailored to your needs:

Where others use 6+ months, Cloud Enabler for SIEM is implemented in **8-12 weeks**.

We train and onboard your organization to ensure that you can **operate and adjust** your new security operation.

We enable your IT security team to work **faster and more effectively.**

Cloud Enabler for SIEM

Assessment

Through thorough analysis, we have a clear idea of what Azure Sentinel features and design an organization like your needs.

Workshops

Devoteam ensures that our customers can operate and adjust their SIEM system in-house.

Design

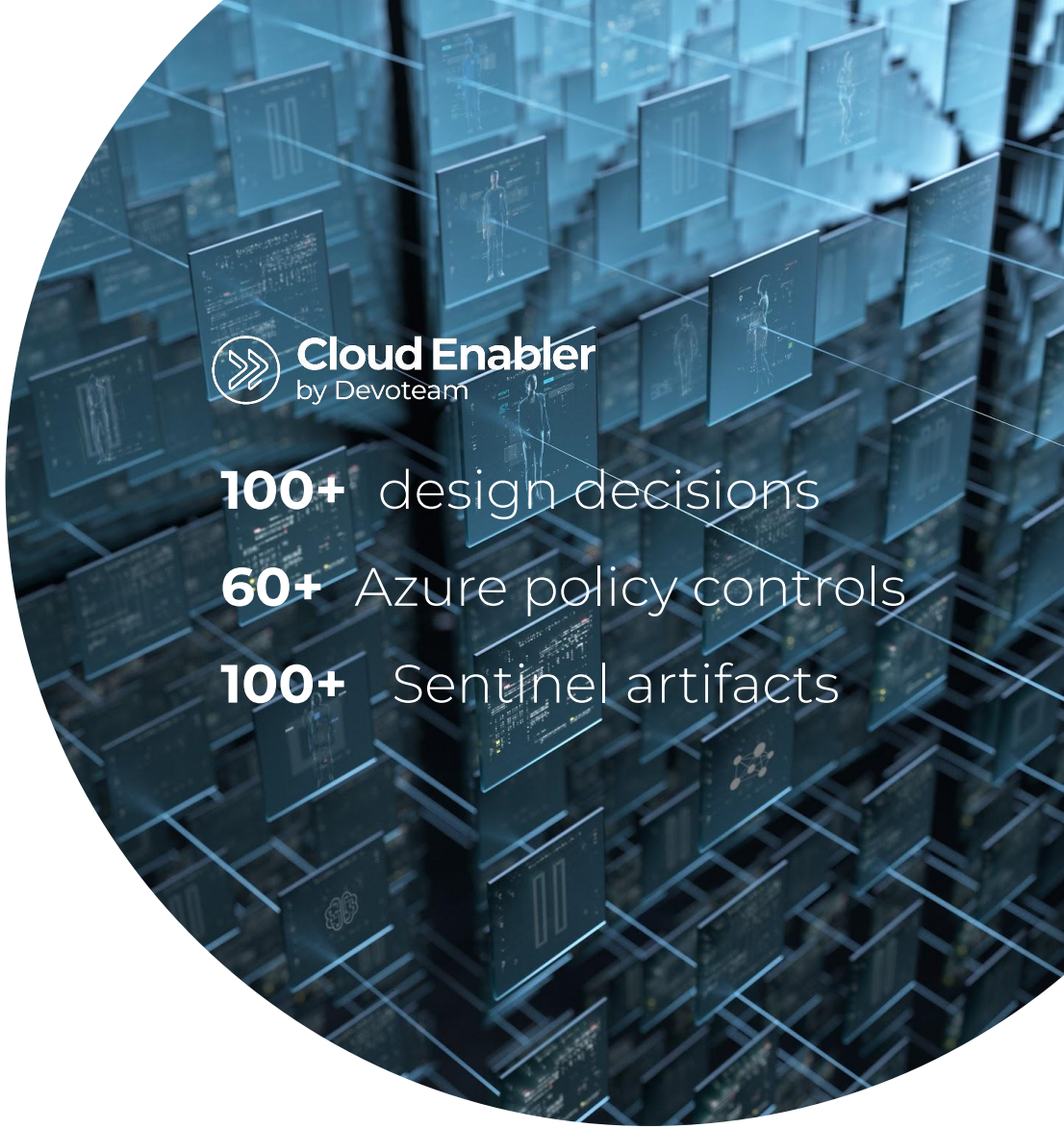
Cloud Enabler for SIEM delivers sets of readily deployable, validated designs and design decisions.

Implementation

Devoteam provides a scalable and cost-effective set of rules, workbooks and automation tasks for Azure Sentinel.

Operations

Cloud Enabler for SIEM gives analysts and security operators what they need to perform security tasks and automate security responses.



devoteam

The Cloud Enabler for SIEM Implementation Process

1

Analysis

The first step is analyzing your security requirements and priorities. All our experts are opinionated advisors. Therefore, after the analysis, we will have a clear idea of what Azure Sentinel features and designs a company like yours needs – and a clear idea of what you don't need.

2

Workshops

With Cloud Enabler for SIEM, our goal is not only to provide a state-of-the-art security operation. Through collaborative sprints and workshops, Devoteam ensures that our customers can operate and adjust their SIEM system in-house.

3

Implementation

Based on a collaborative process, Cloud Enabler for SIEM works alongside you and your IT security team to get you onboarded and operating – fast. Devoteam has created a set of readily deployable, validated designs and design decisions, saving you a lot of time and deliberation. We provide a scalable and cost-effective set of rules, workbooks, and automation tasks for Azure Sentinel.

devoteam

The Value Outcome

Acceleration

Cloud Enabler for SIEM is faster to deploy and configure than comparable solutions available on the market today. In 8 to 12 weeks, we design, deploy and adjust a cost-effective and scalable cloud security operation for your enterprise needs. Devoteam delivers great results quickly by building solutions on enterprise-ready rules, workbooks, and automation tasks.

Competence

Through sprints and workshops, we give your organization a thorough introduction to every part of your SIEM solution. We transform your digital infrastructure and strengthen the organization's digital competency, enabling you to operate securely and confidently in the cloud.

Control

With Cloud Enabler for SIEM, you can be confident that your security and compliance requirements are met. By building solutions on infrastructure as code (IaC) principles, you also reduce the risk of human errors to an absolute minimum. Maximising the system's capacity makes it easier for you to devote time, focus, and resources to running your business.

Cost

Cloud Enabler for SIEM provides cost control and helps your company cut costs. We do this by deploying ready-made, battle-tested solutions for your Azure Sentinel needs. By enabling our clients to maintain and run their systems themselves, while also developing their internal IT resources, you get an increased return on your investment.

devoteam


Thank you.
devoteam