SECULYZE

Built in Denmark | Delivered from the EU | Made for Microsoft Sentinel

AI-driven Security Operations

Seculyze is a Danish cybersecurity SaaS company helping organizations optimize Microsoft Sentinel with AI-driven capabilities that reduce noise, improve detection quality, and strengthen operational control.

Modern **security operations** are under pressure from growing alert volumes, limited specialist capacity, and increasing demands for efficiency and resilience.

Still, attackers increasingly move with automation, AI and machine-speed tactics.

Seculyze helps organizations get **more value from Microsoft Sentinel** by making security operations more **precise, more scalable**, and easier to manage.

Operational Value
Reduce noise and cost, improve quality, and increase control

Made for Sentinel
Optimizing security operations Microsoft

Danish/European
Built in Denmark and delivered from the EU

Turn Microsoft Sentinel into a more efficient, intelligent, and scalable security operations platform

BOOK DEMO

seculyze.com/request-demo

Security Operations are becoming too expensive, too complex and too manual

Organizations using Microsoft Sentinel face rising costs, increasing complexity, alert fatigue. With a global shortage of cybersecurity professionals, no solution is found there. The result is growing pressure on already stretched teams to do more, respond faster and optimize continuously.

Expensive

Microsoft Sentinel is powerful, but pricing can be **difficult to understand, explain, and optimize**. Ingestion, and retention often create costs that lack transparency.

10 - 30% cost reduction potential

Complex

Fine-tuning detections, automating workflows, and maintaining a strong setup requires **deep expertise** and continuous effort. It is hard to know whether the system is **truly optimized**.

+65% MITRE coverage potential

Burn-out

False positives consume analyst time and **create fatigue**. When teams are overwhelmed, valuable alerts may be **delayed, ignored, or deprioritized**.

32 minutes per false positive

Talent Shortage

Security teams are expected to **do more with fewer** specialists. ISC2 estimates a global gap of **4.8 million** cybersecurity professionals, making it harder to scale internal operations.

27% of alerts ignored due to fatigue

The challenge is *not* having a SIEM. It is making it *efficient*, *manageable* and *effective*.

SECULYZE

One Platform. Four Core Modules

Seculyze brings together configuration quality, alert tuning, cost control, and multi-tenant operations in one platform built for Microsoft Sentinel.

Calibrate
Best practice setup

- Best-practice configuration
- Automatic update of outdated rules
- Change log and configuration tracking
- Your score and benchmark for setup quality
- Recommendations for alert rules, log sources and settings

Tune
AI-driven alert tuning

- Threat intelligence enrichment from multiple CTI sources
- Dynamic risk-based prioritization
- ML classification of FP, TP and undetermined
- 1-click & auto-close of false positives
- Focus most risky alerts

Cost
Visibility & optimization

- AI-based anomaly detection on log ingestion and cost
- SKU-level optimization
- Data Collection Rule tooling
- Removal of unnecessary ingestion
- Low-cost storage moves

Unify
Multi-tenancy

- Single pane of glass across MSSP clients or business units
- Cross-tenant visibility and priority
- Noise reduction on all or selected tenants
- Presets for deployment models
- Notifications and ITSM integration

Enterprise add-on

- Customer Managed Keys
- Single Sign-On
- Segregated Infrastructure

Platform Foundation

- Two-way data sync
- Online support
- In-app onboarding
- Personalized URL
- Multiple user privilege levels

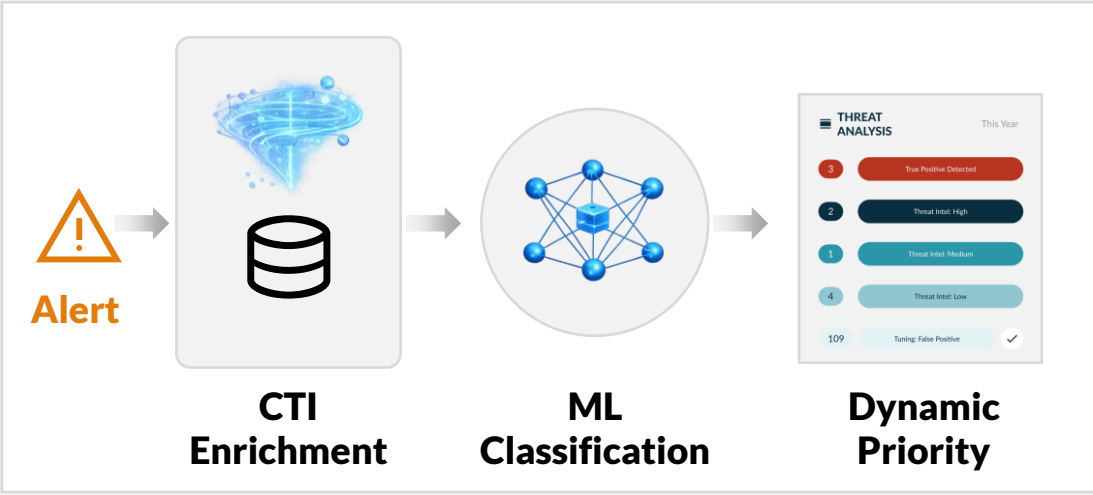
SECULYZE

Deep Dive: Tune
One of Seculyze's Core Modules

Tune combines multi-source threat intelligence (CTI) enrichment with a purpose-built neural-network model to classify alerts more accurately.

At the core of *Tune* is a technology choice: Seculyze uses custom ML built around a neural-network architecture designed for cybersecurity data patterns based on university studies.

Normalized alert data, flexible hidden layers and a variational Bayesian linear output layer are used for classification confidence. In practice, model quality depends on using the right amount of data features rather than the maximum as it reduces efficiency. During onboarding, the Seculyze SaaS selects the model setup that best fits the customer environment and then follows performance continuously confusion matrices, F1 scores, and confidence monitoring.



A key part of the data features come from CTI. Seculyze's engine evaluates IOCs across multiple open and commercial feeds, then scores them using weighted dimensions. Signals are aggregated into a single risk score to prioritize alerts based on your actual environment rather than a static severity. The result is a tuning capability that learns from your specific patterns, benefiting from historical alert data and external threat context providing lower noise, faster triage and more confident decisions.

Why ML, not LLM
Built for classification, not language processing.

Why model fit matters
Too many features reduce efficiency. The goal is an optimal feature set

How quality is monitored
Confusion matrices, F1 score, recall/precision tracking and confidence monitoring

How threat context is added
Recency, feed quality, consensus, MITRE phase and targeting context

Trusted by security teams across industries

UNIVERSITY OF COPENHAGEN · ecit · Jyske Bank · KANDA

Real Operational Value-add

AI-driven optimization that reduces false positives, lowers Sentinel cost, and improves security outcomes in day-to-day SOC operations.

Case story

In one global manufacturing environment, Seculyze helped transform alert handling in Microsoft Sentinel by removing large volumes of low-value noise and making the remaining incidents faster to assess and resolve. This allowed the SOC to spend less time on repetitive triage and more time on genuine threats and operational priorities.

The result was a false-positive auto closure rate of **71%** and a **24%** reduction in Sentinel-related cost, while MITRE ATT&CK coverage increased by **65%**. In other words, the customer improved efficiency and tune out the noise while increasing detection coverage

Up to

97%

false positive detection rate

Up to

30%

cost reduction on your Microsoft bill

At least **+65%** more MITRE coverage ○ Up to **99,7%** recall rate

> We have worked on tuning the handling of alarms in our SOC, and in this work have benefited greatly from Seculyze's software. I can definitely recommend Seculyze to anyone who needs tuning of alarms in Sentinel.

Michael Collin
CISO

AALBORG UNIVERSITET

Optimize system → Tune alerts → Remove noise → Lower costs

SECULYZE

A Practical Path to Smarter Security Operations

Seculyze is designed to help organizations improve Microsoft Sentinel in a structured and low-friction way. Whether the priority is reducing false positives, lowering Sentinel cost, or improving coverage, the starting point is practical and easy.

From automatic onboarding, value is added after only 2 hours. Follow recommendations and start tuning alerts and optimize the system. The objective is not to add another layer of complexity, but to make existing security operations more effective. That means giving security teams a clearer path from current-state challenges to measurable operational improvements, with a model that can scale over time.

ONBOARD

Get up and running in less than **2 hours**. Machine learning stabilizes within **18 hours**

IMPROVE

Follow recommendations with **one click**. Ensure Microsoft Sentinel is **properly configured**

TUNE

Start adjusting the system and setup ML-driven **auto-closure rules**

OPTIMIZE

Optimize the setup; **Sentinel costs**, automatically generate incident reports, prioritize **most risky incidents**

Let's explore how your organization reduce noise, improve coverage, and get more value from Microsoft Sentinel

Contact us

Kristian Jacobsen
Founder & CPO
+45 6179 2740
kristian@seculyze.com
linkedin.com/in/kristianjac

Alex Steninge
Founder & CEO
+45 2190 9575
alex@seculyze.com
linkedin.com/in/alexsteninge

SECULYZE