SECULYZE

Seculyze Software White Paper

www.seculyze.com

SECULYZE

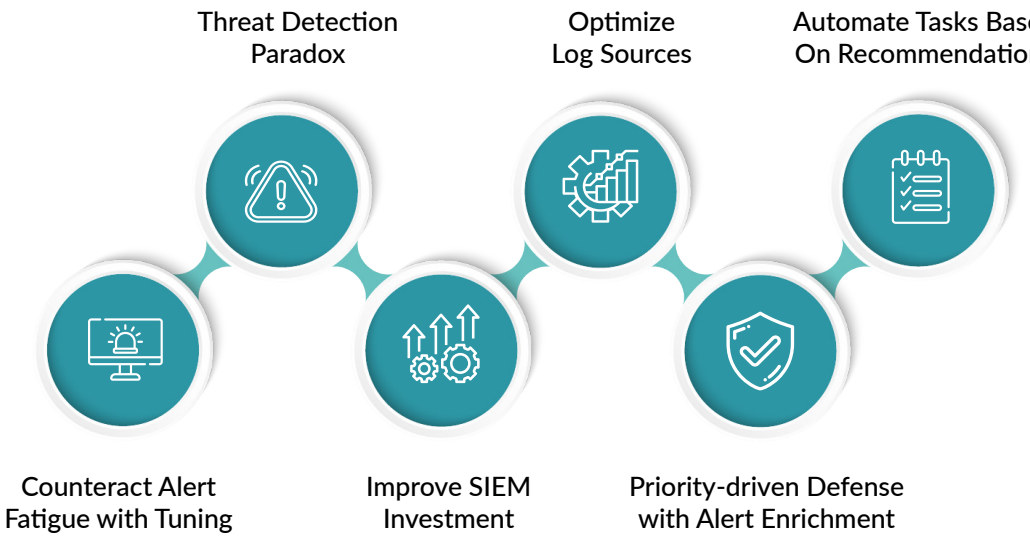
Table of Contents

1. Introduction: Navigating the Cybersecurity Frontier

In our rapidly evolving digital age, cybersecurity isn't just an IT concern—it's a business imperative. With rising cyber threats, companies are constantly seeking ways to fortify their defenses and stay ahead of potential vulnerabilities. Enter SaaS solutions: these cloud-based tools are reshaping how we approach and bolster our cybersecurity measures.

In this white paper, we'll delve into the challenges modern organizations face and introduce Seculyze, a standout SaaS solution that redefines threat detection and response. You'll discover the unique value propositions that set Seculyze apart and learn how it directly addresses the complex issues in today's cybersecurity landscape.

Key Concepts:



SECULYZE

2. Landscape: Balancing Resource Scarcity with the Surge in Cyberattacks

In the evolving digital realm, CISOs grapple with three pivotal challenges in cybersecurity. This white paper illuminates each, from escalating cyberattacks to intricate system inefficiencies, highlighting how Seculyze SaaS offers a formidable countermeasure.

2.1 The Rising Tide of Cyberattacks

Cyberattacks persist as a significant threat, increasing annually by +125%[1]. Resulting damages are €5½ trillion per year, costing organizations an average of €8 million per attack. Given an average of 130 security breaches annually per organization, the financial implications are staggering[2]. As cyberattacks increase, so do the alerts security analysts receive, leading to immense pressure on their resources and escalating the risk of "alert fatigue". This fatigue, combined with scarce resources, impedes the capacity of organizations to adequately safeguard themselves.

What does +125% imply: Being seduced by the compound function

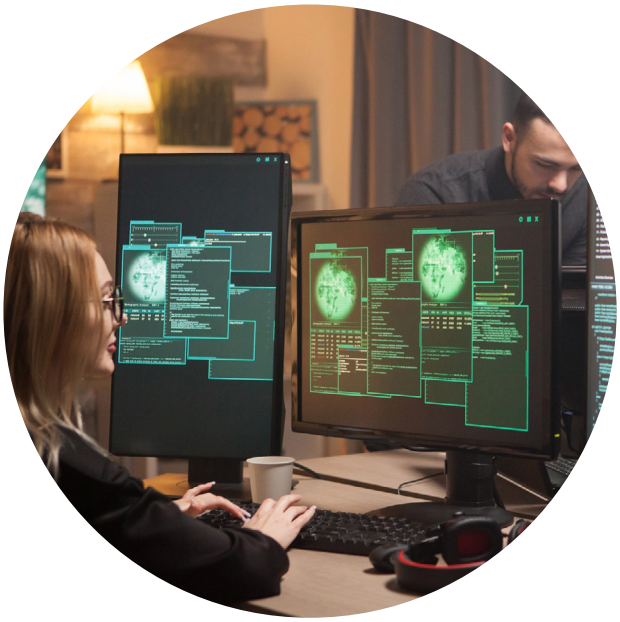
Imagine you invest €100 at a whopping compound growth rate of 125%. By the end of the first year, you'd have €225. By the end of the second year, that amount would grow to €506.25 without adding a single cent more.

Projecting this onto the digital landscape: if we took the initial number of cyberattacks as our €100, they would more than double in a year and then further escalate exponentially. It paints a dire picture of how swiftly cyber threats can proliferate under a compound growth model.

1 Research paper from Accenture. 2 White paper from Critical Start.

2.2 Alert Fatigue & Resource Scarcity: A Threat Multiplier

A bulk of alerts, estimated between 25-75%, are false positives. In extreme cases, this reaches 99%[3]. False positives bury genuine threats, redirecting focus from vital incidents to insignificant alerts. The cybersecurity industry faces a global shortage of 3.4 million professionals, with 70% of existing analysts highlighting inefficiencies due to staff shortages.[4] The result? Longer investigation times and a rise in manual tasks, with 64% of analysts dedicating over half their time on tasks that could be automated.[5] Such inefficiencies and fatigue compromise security postures, leading to increased vulnerability and organizational risks.



2.3 The Threat Detection Paradox: More Coverage, Less Clarity

As security teams seek more threat coverage due to the rise in attacks, they face a clear problem: more coverage often leads to a flood of false alerts, making it hard to spot real threats. This is where Seculyze steps in, helping teams cut down on false alerts while still widening their threat detection. Adding to the challenge, the running costs of SIEMs are high, often reaching 3-4 times the initial setup cost.[6]

Free Trial

3 Research paper from Oxford University.
4 Work force study by ISC2
5 Research from the no-code firm Tines
6 Research from Exabeam

SECULYZE

3. Key Values: Unlocking Cybersecurity Excellence with Seculyze

Seculyze, a groundbreaking SaaS solution, amplifies the power of Microsoft Sentinel, revolutionizing your threat detection and response strategy. Let's address the core challenges that keep CISOs awake at night and see how Seculyze becomes your unparalleled ally.

> **Value proposition: Reduce cyberattacks by removing irrelevant alerts and prioritizing the remainder.**

How Seculyze Transforms Cybersecurity:

Combatting the Threat Detection Paradox:

The increasing wave of cyber threats has often led to more coverage but less clarity, drowning teams in false positives. Seculyze changes this narrative, dramatically reducing false positives by 83-98%. For a company with 6,600 employees, this translates to over 9,960 fewer alerts and a liberation of 318,720 minutes. Now, focus on genuine threats, not noise.

Optimizing Investments Amidst the Rising Tide of Cyberattacks:

The value of SIEM goes beyond its price tag. With SIEM operational costs skyrocketing, it's vital that every euro amplifies your defense. Seculyze ensures this, streamlining configurations, rules, and log sources, transforming your SIEM from a cost center to a fortified cybersecurity bastion.

Rising Above Alert Fatigue & Resource Scarcity:

With the modern-day flood of alerts, discerning the critical from the trivial becomes daunting. Seculyze brings clarity and purpose to your defense, enabling swift identification and mitigation of the most significant threats. Drive your team's energy where it matters most.

Set against the backdrop of an ever-evolving cyber landscape, Seculyze's dedication to directly mitigating these formidable challenges is unparalleled. Dive into our subsequent chapter for a granular look at how Seculyze rises to the occasion, every time.

7 Research done by IDC

SECULYZE

4. Solution: Enhancing SIEM with Seculyze's Pioneering Approach

The software Seculyze provides is a meticulously crafted SaaS platform designed to seamlessly integrate with Microsoft Sentinel. Distinct from other offerings, Seculyze provides a paradigm shift in SIEM by harnessing cutting-edge technologies and innovative approaches to tackle contemporary cyber challenges head-on.

How Seculyze works

Seculyze's design seamlessly bolsters Microsoft Sentinel's capabilities. With a simple integration of a service principal, organizations can swiftly begin data extraction. Seculyze then fetches, normalizes, and enhances data for both Defender and Sentinel alerts.

Our architecture features three core modules:

Health:

Optimizes the alerting and logging environment. It reviews the alert rules, data sources, and Sentinel's setup, providing solutions for any inefficienciess, keeping the system up to date to ensure your SIEM operates at peak efficiency.

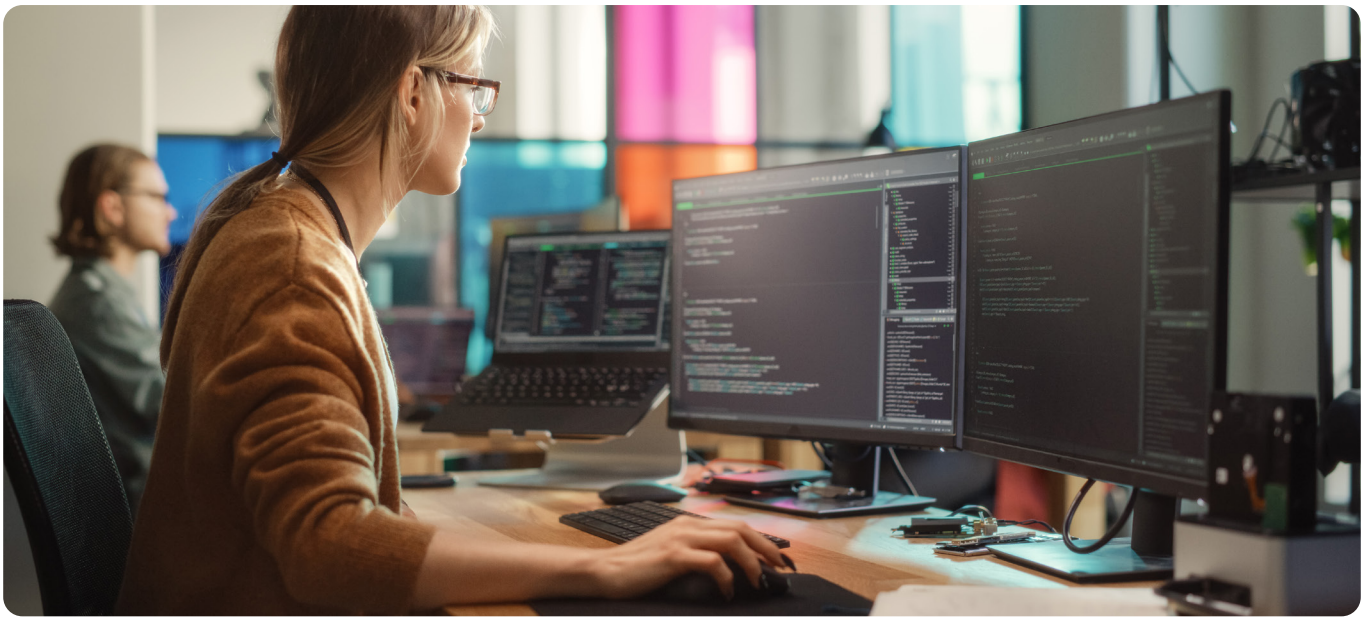
Tune:

Powered by AI, this component categorizes alerts by similarity and plays a crucial role in alleviating alert fatigue. By grouping alike alerts, Seculyze identifies patterns, reducing noise and redundant alerts.

Enrich:

Boosts alert usefulness by layering them with crucial threat intelligence, deepening understanding of each alert's significance. By providing insights into the nature and severity of each alert, it empowers teams to react faster and with precision.

These features are available in the Seculyze portal, an intuitive interface enhancing Sentinel's SOC functions. Our unique alert rules further refine the system's capabilities.



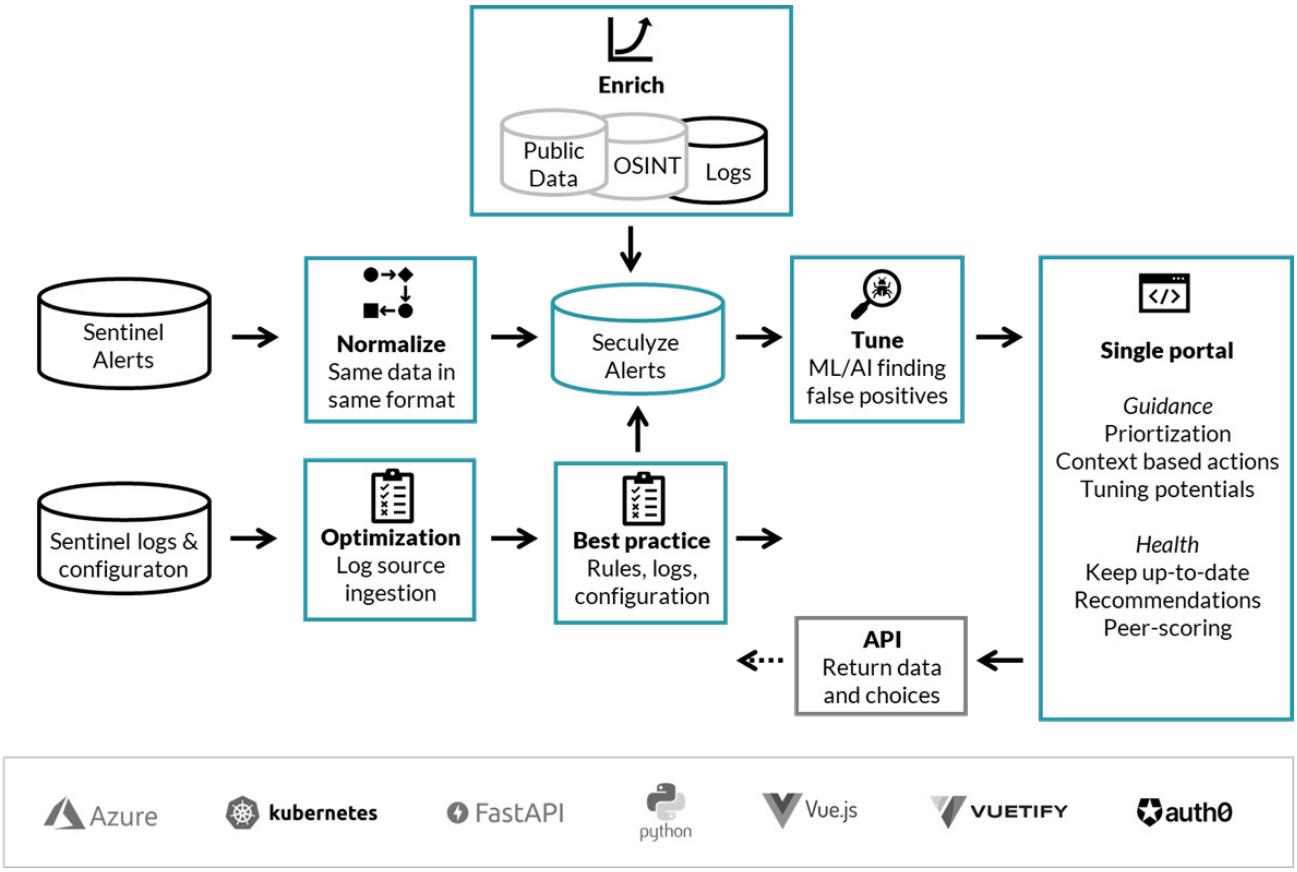


Figure 1: Architecture of Seculyze. Fetching data from Sentinel and returning data and choices through APIs

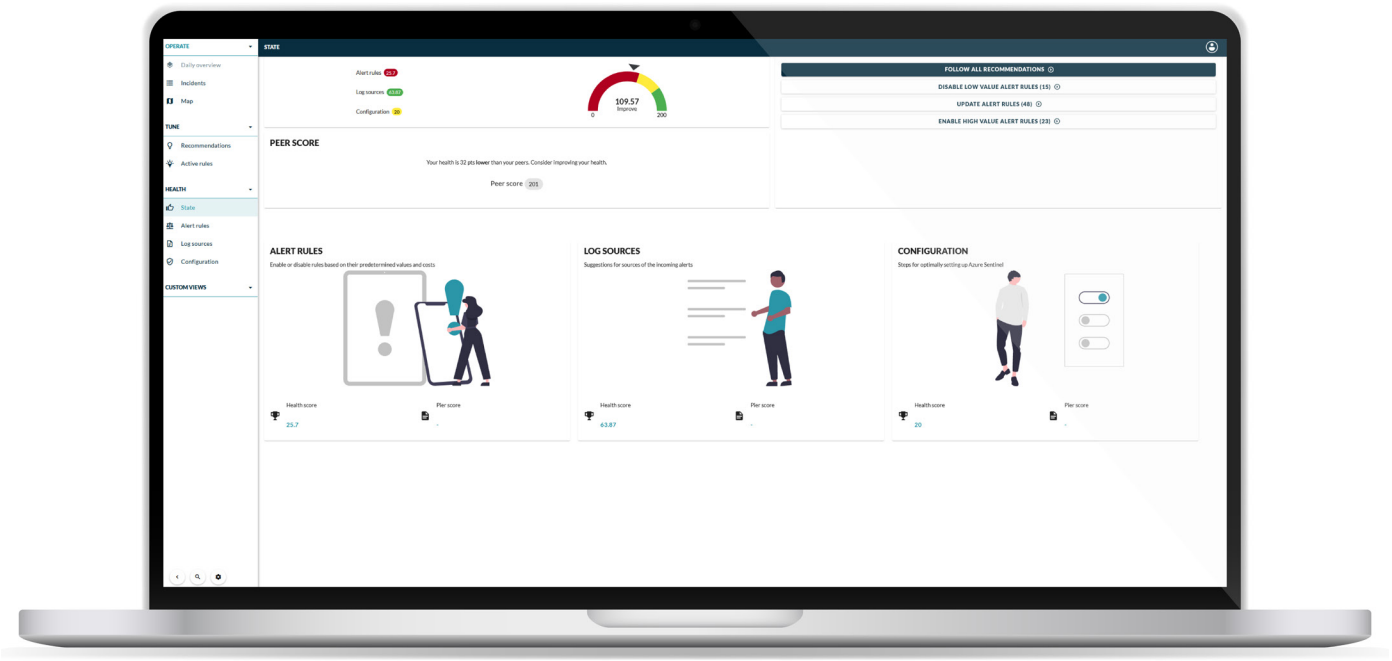
SECULYZE

5. Features & Benefits: A Closer Look at Seculyze's Key Modules

5.1 Health

Health operates at the crossroads of automation and expert knowledge, granting analysts an edge in navigating the dynamic threat environment and ensuring an optimal Sentinel setup. Alert rules, log sources and configurations are automatically and continuously assessed towards best practice to provide easy one-click recommendations. It's sophisticated scoring based provides a metric that quantifies the value of each recommendation. As a result, analysts can better navigate and optimize their Sentinel environment and the business will have a platform that continuously is setup after best practice without having to use consultants.

> **Health Check score = alert rule score + log source score + configuration**



Alert Rule Score:
Efficient Alert Rule Management

Confidence in your enabled alert rules is paramount because it provides detection coverage. Using a value-driven alert model, alert rules with high value—detecting anomalies without burdening you with false positives—and recommendations deactivate less efficient ones. The efficacy of your alert rules determines how efficiently you can respond to potential threats. With an abundance of alerts, it becomes crucial to distinguish high-value alerts that signal genuine threats from low-value ones that may contribute to noise.

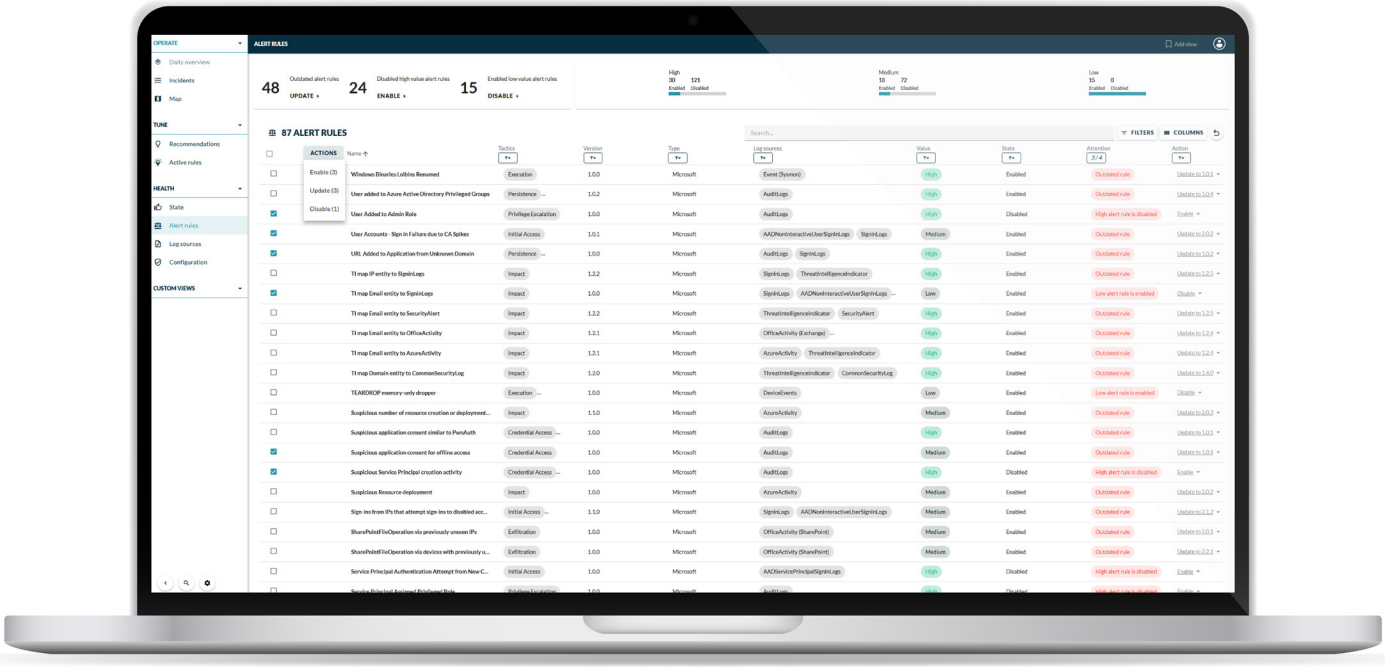


Figure 2: Alert Rule Management Interface

Seculyze offers an intelligent approach to alert rule management through the unique attention and action columns:

- Get a quick overview of your alert rules
- Enable High-Value Alert Rules that are disabled and vice versa
- Update out-of-date Alert Rule templates

Seculyze's alert rule management ensures that every decision is data-driven ensuring a tighter security posture and a more streamlined operational flow.

Log source score:
Strategic Resource Allocation Based on Data and Analysis

Health systematically evaluates log sources by juxtaposing their actual incurred cost against the associated gain from the alert rules linked to each log source. The utility of each log source is analyzed based on the number of mapped alert rules, and its intrinsic value in incident response and investigative contexts.

Comprehensive explanations are given for every log source. Seculyze provides a detailed breakdown of its gain and cost, empowering users with a clear understanding of the rationale behind each recommendation.

- Optimize your log cost
- Get a quick overview of your log sources
- Enable High-Value log sources that are disabled and vice versa

In essence, Health for log sources refines Microsoft Sentinel's setup through a nuanced, data-driven approach, ensuring that resources are effectively channeled for optimal cybersecurity outcomes.

Configuration score: Optimizing the Sentinel Workspace in Pursuit for Excellence

In the dynamic landscape of cybersecurity, effectively utilizing the Sentinel workspace requires consistent adaptation. It is not solely about the initial configuration, but also ensuring its evolution aligns with prevailing best practices. You might think it is best practice out-of-the-box, but Seculyze's Health module offers pivotal guidance with some non-exhaustive examples of recommendations:

- Retention Practices: Maintaining an optimal data retention period is essential. This not only ensures thorough incident and threat analysis but also fosters strategic baselining.
- Normalization Functions: The talent of Sentinel lies in assimilating data from varied sources. Implementing a uniform data model across these sources enhances efficiency and analytical precision.
- Resource Allocation: With continuous advancements in functionalities, periodic assessments are crucial to determine the most fitting Log Analytics and Sentinel tier, impacting both cost-effectiveness and threat detection prowess.

Remember, Sentinel's configuration is not static. As Microsoft introduces new features, staying updated is imperative to harness the platform's full potential.

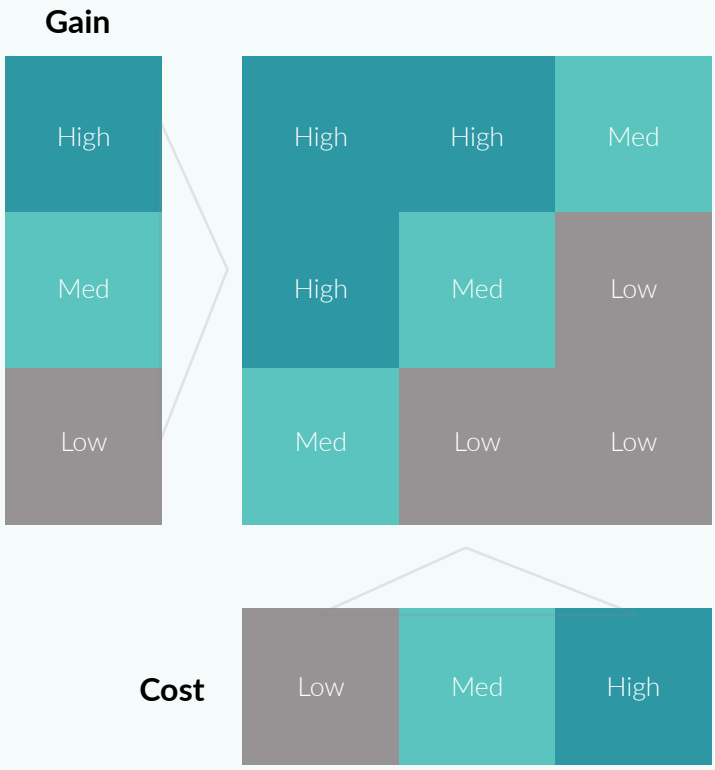


Figure 3: Value assessments. For Alert Rules, Gain is a measure of the certainty of the alert and Cost is a measure of time used. For Log Sources, Cost is your actual, estimated monetary cost and Gain is the amount of alert rules covered.

5.2 Tune

Seculyze's tuning approach revolves around constructing threat models grounded in baselining the alert output of the daily security activities of an organization. This creates accurate behavioral baselines, ensuring that alerts or incidents are continuously adjusted and validated to accurately highlight threats that warrant investigation.

Artificial Intelligence at the Heart of Seculyze Tuning

Seculyze's AI mechanism streamlines the Sentinel alert detection output specific to your organization's security needs. It constantly scans incoming alerts, grouping those with shared characteristics. Alerts are clustered based on their similar context are often indicative of false positives. This pattern recognition capability then fuels the generation of precise tuning recommendations, constantly refining your system's alert threshold.

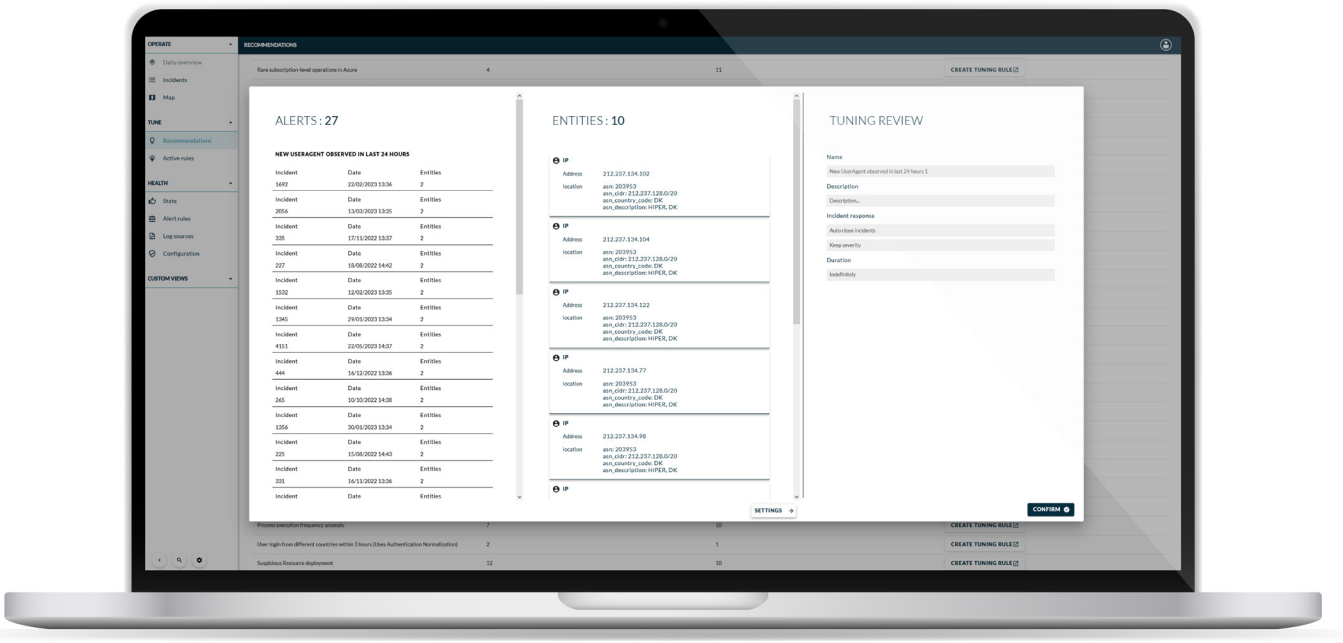


Figure 4: Example of a tuning rule suggestion for 27 alerts

In the example, the suggestion provides a commonality: the IP address is almost the same and the ASN remains consistent. This consistency underscores the user's behavior, pinpointing the shared traits amidst the diverse user agents. Through Seculyze's intelligent clustering, such nuances are brought to the forefront, assisting analysts in discerning genuine threats from benign activities.

We use a combination of supervised learning and reinforced learning models. By using historical data, the parameters can be optimized in relation to your data set. The recurring decisions on future alerts acts as a reinforced learning further optimizing the parameters.

Intuitive Rule Creation and Management: Retain Full Control

Seculyze's dynamic rule creation feature is designed for alerts with high level of commonality. While AI streamlines the detection and recommendation, analysts retain full control, deciding on rule durations, actions, and severity adjustments. This synergy of technology and human insight ensures alerts are addressed efficiently without compromising accuracy or oversight.

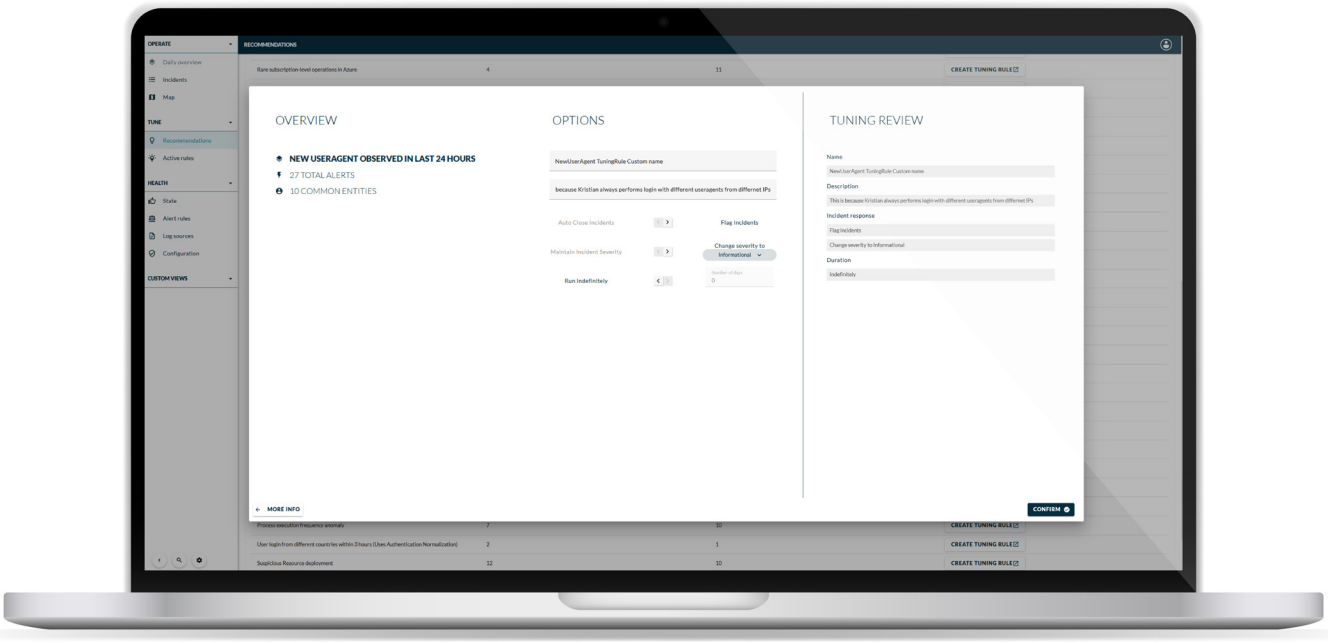


Figure 5: An example of the interface and options of creating a tuning rule based on the same suggestion for 27 alerts.

Options:

1. **Naming and describing the tuning rule**

2. **Choose: Auto-tune alerts or flag alerts with tuning recommendations**

   Remove the manual interaction totally or retain control and get recommendations when a new alert matches an existing tuning rule

3. **Choose: Run indefinitely or until a fixed time**

   If you want to test an alert before making it productive, set an ending date. You can at any time turn a rule off.

4. **Choose: Retain or change severity**

   Commercials in some MDR contracts rely on severity, so you can use it to optimize your MDR/SOC spend

Free Trial

SECULYZE

5.3 Enrich: Efficient Countermeasures to Attacks by Pinpointing the Largest Threat

Enrich automatically adds threat intelligence from advanced sources to your security alerts – and transforms security event data by integrating contextual insights derived from threat intelligence and open-source intelligence (OSINT). Tapping into public sources like websites, public databases, and geo-location data, OSINT is complemented by specific threat intelligence details, such as IP addresses or abuse scores. This depth of knowledge provides clarity on attack methods, threat actor profiles, and their motivations.

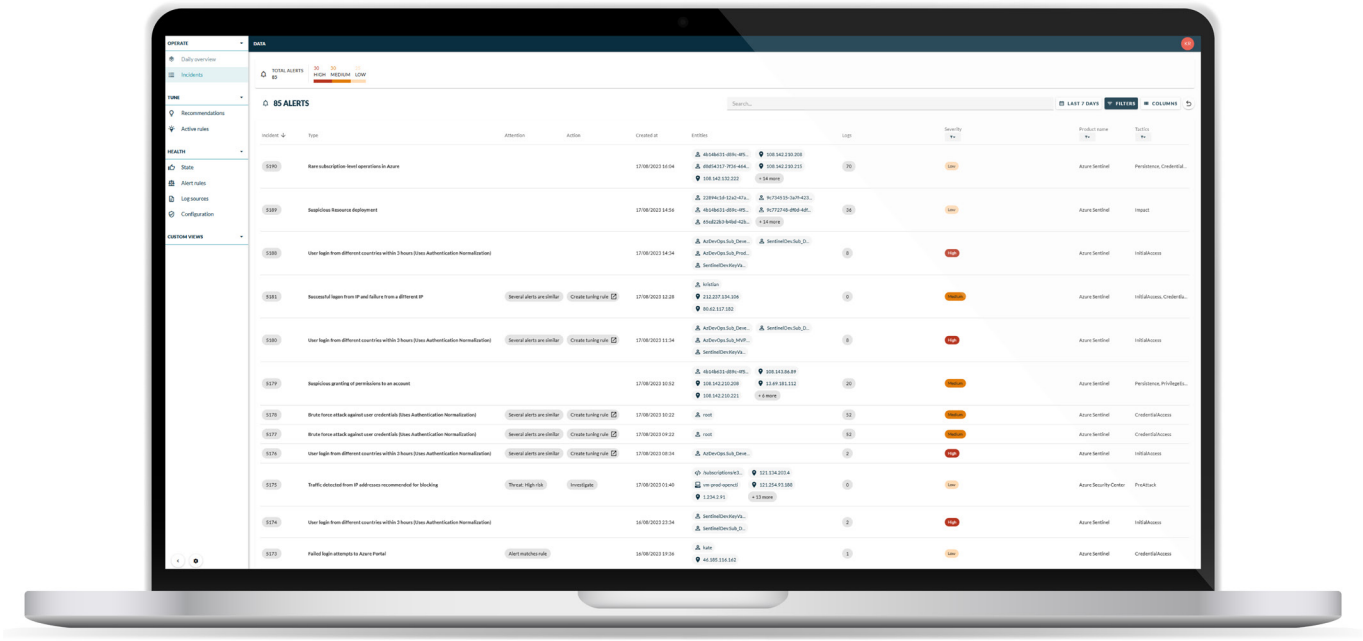


Figure 6: Enriching alerts with external provides a better context for prioritizing than the static, fixed severity level creating from the alert rule.

By enhancing alerts with this enriched data, analysts are equipped to identify which alerts are tied to potential malicious activities, thus streamlining their decision-making process. The module also prioritizes alerts. Seculyze classifies alerts into defined risk tiers moving from high to unknown; the latter corresponding to lack of pertinent threat intelligence. This categorization allows for a prioritized response, ensuring critical threats are addressed first.

The result is a swifter analysis, reduced alert handling duration, and a more precise incident response, positioning analysts at the forefront of threat mitigation.

Enrich provides context-based, easy-actionable recommendations and alert insights so that you can respond faster and better, using less resources.

5.4 An overview of other features: The Glue that Brings Efficiency to Your SOC/MDR

Map your Health score towards your peers to understand your security posture

Recommendation: Attention column = clear explanations. Action = context-based, easy-implementable action

Tags are written back to your Sentinel installation, e.g. “tuned out with rule 1234”

Easy onboarding with videos, userflows and guides – and offboarding

Free 14 days trial to try out Seculyze’s features

Optimize your spend on ingested log sources by trimming your log sources and removing redundant log sources

Easily document your alerts with suggestions for “who, what, when” and reused when tuning our similar alerts

Choose 12 months data retention if you want more detection power than the standard 3 months retention

6. Data Security and Compliance: The Foundation for Reliable Software

Reliability is a core value for us which is also implemented in our data security and compliance.

6.1 Security Robustness

Our automated, uniform deployments via Terraform are realized through a mix of Azure Kubernetes, FastAPI, and Vue.js. Dependabot aids in code health, while continuous vulnerability scans for container images and Microsoft Defender on our resources help shield our application. Azure's Security Benchmarking guides our remediation strategies. Grafana and Loki amplify our Kubernetes monitoring, dovetailed by Azure Sentinel's oversight on a myriad of activities, ensuring no blind spots.

With every client data housed in isolated Kubernetes and Azure environments, coupled with separate application and database environments, we prioritize data integrity.

6.2 IAM Excellence

Relying on Auth0, we ensure tailored access based on organizational needs with three different role levels. This granular control integrates seamlessly with our APIs. Azure AD's MFA fortifies access, ensuring identity security for our employees. With the foundational principle of least privilege in our Azure IAM model, we ascertain that only the right entities access relevant data.

6.3 Data Protection

Data In Transit:

Every interaction, APIs or direct data access, is encrypted. We leverage the robust security features of FastAPI's TLS for seamless and secure API communications. In addition, our Azure-based infrastructure ensures encrypted data transfers through SSL/TLS.

Data At Rest:

Protecting data doesn't end once it's stored. Security of data at rest is done by AES-256 encryption. This provides strong protection against potential breaches or unauthorized access.

Customer-Managed Keys:

Recognizing that some data is exceptionally sensitive, we offer our clients the option to manage their encryption keys, including autonomy to implement key rotation policies. These customer-managed keys are stored securely in key vaults to provide an additional layer of security and trust.

6.4 Data Storage Technologies & GDPR Compliance

For our infrastructure, we rely on Microsoft Azure, hosted in West Europe. Authentication for our APIs is bolstered by Auth0, based in Europe, while our support framework is powered by HubSpot, situated in the EU. Each platform is meticulously chosen for its capabilities and alignment with GDPR's rigorous standards, ensuring that every facet of our operation prioritizes data integrity and user privacy.

Hubspot	Data hosting location: European Union
Auth0	Data hosting location: Europe
Azure	Data hosting location: west-europe

SECULYZE

7. About Seculyze: Pioneering Cybersecurity Evolution

Seculyze was born from a collective pursuit of a better way. With a background as cybersecurity consultants in Sentinel, we recognized the recurring patterns and challenges faced by businesses. The idea was seeded - an idea that would later manifest as Seculyze, a Software as a Service (SaaS) solution tailored to optimize cybersecurity efforts.

Established in 2021, Seculyze embodies the spirit of adaptation and client-centricity echoing the principles of the Scaled Agile Framework (SAFe). Its foundation is built upon the pillars of Reliability, Openness, and Learning. Reliability ensures that every decision is a trusted one, fostering data security and privacy. Openness fuels proactive collaboration and transparent communication, essential in the ever-changing landscape of cybersecurity. Learning is the driving force behind Seculyze's continuous growth, fueled by insights from clients and a commitment to refining cybersecurity solutions.

Seculyze is more than a solution; it's a testament to the ever-present spirit of evolution. Our dedication to excellence is echoed in our alignment with ISO27001 and ISO 9001 standards, which contribute to a seamless experience for our clients.

Alex Steninge Jacobsen
CEO
+4521909575
alex@seculyze.com

Kristian Jacobsen
CTO
+4561792740
kristian@seculyze.com

Read More

8. Would you like to know more?

Next step is our free trial or a demo

Free Trial

Call or write us

Alex Steninge Jacobsen
☎ +45 2190 9575
✉ alex@seculyze.com

Kristian Jacobsen
☎ +45 6170 2740
✉ kristian@seculyze.com

SECULYZE