SOC as service – Microsoft Sentinel

INFORMATIKA

Microsoft Sentinel- the cloud native SIEM solution

Challenges

Data is growing at an exponential pace, and traditional SIEM solutions simply cannot keep up. Many SOC teams are using outdated solutions for monitoring and responding to security incidents. These, one-size-fits all legacy tools are not able to provide business context, threat intelligence and analytics capabilities to uncover new threats hidden in the large volumes of data.

Ideal Solution

By using Microsoft Sentinel - Cloud-native SIEM Solution, we help our clients build the best foundation to move from reacting to incidents to applying analytics to proactively manage cyber threats. Our Security Operations Center (SOC) is an external center for monitoring and analysis of our clients' IT infrastructure and systems, which provides the people, technology, and experience to help you get the most out of your Microsoft Sentinel deployment.

Who are we?

We are a future-focused organization, with an accent on helping our clients build a foundation of proactive security to address evolving threats.

The Informatika team includes highly qualified experts with over 20 years of experience in data security, threat and vulnerability assessments, design, implementation and management of security solutions, and cyber security consulting.

Informatika’s Security operations center (SOC)

- Building your own SOC presents an organizational challenge that requires enormous resources and time to develop internal competencies. It can take many years, which you may not want to spend, to reach the desired level of maturity because cyber attackers will not wait for you to be ready before start threatening your business. We are here to help!

- The Informatika’s Security Operations Center (SOC) is a purpose built, external center for 24/7 monitoring and analysis of our clients’ IT infrastructure and systems through Microsoft Sentinel.

- Our team of security analysts and defense specialists will support you every step of the way - from preliminary assessments to expert-led SOC training.

Informatika’s Security operations center (SOC)

ENTERPRISE CLASS SECURITY

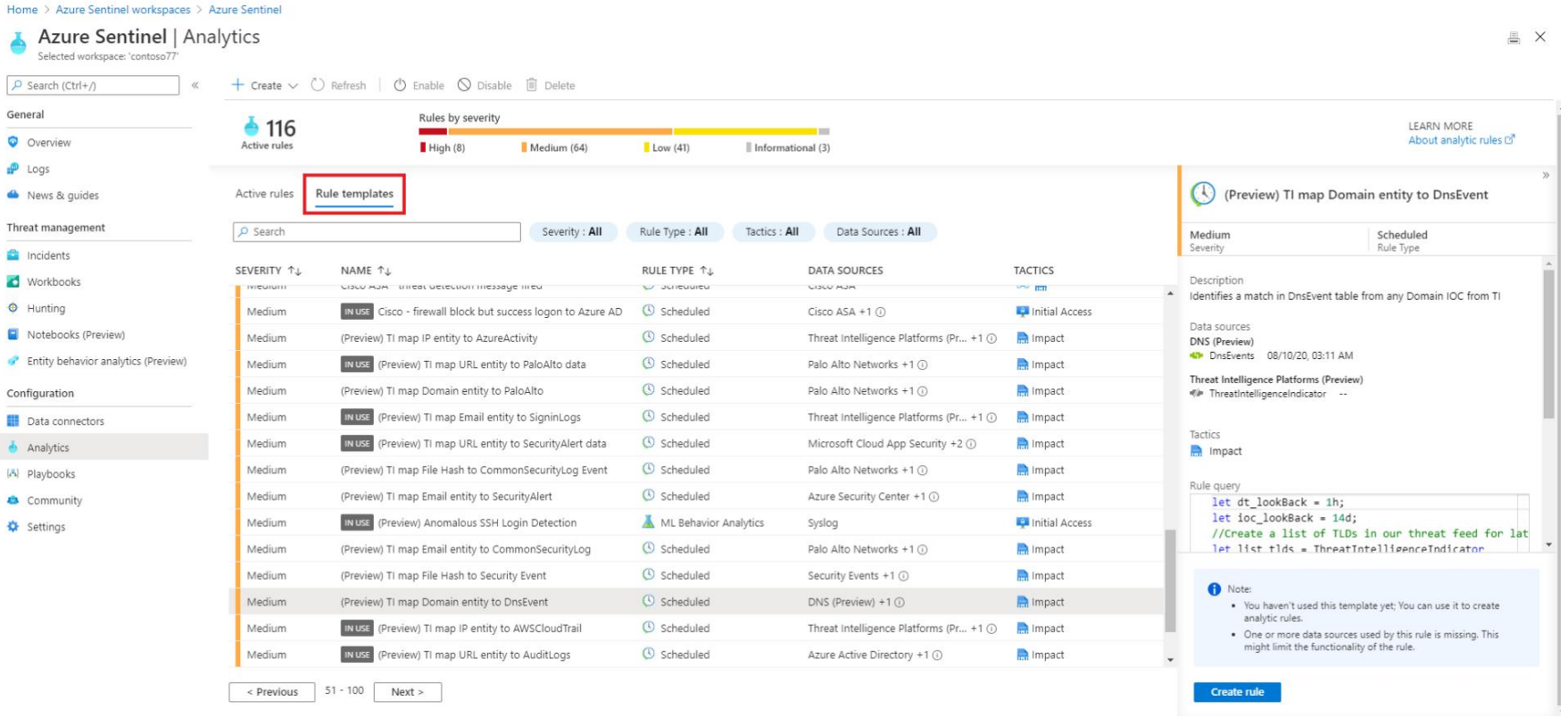
A variety of services to suit all the needs of enterprises, governments and public sector organiza-tions, underpinned by 24/7 support and tight SLAs.

HOW WE CAN HELP

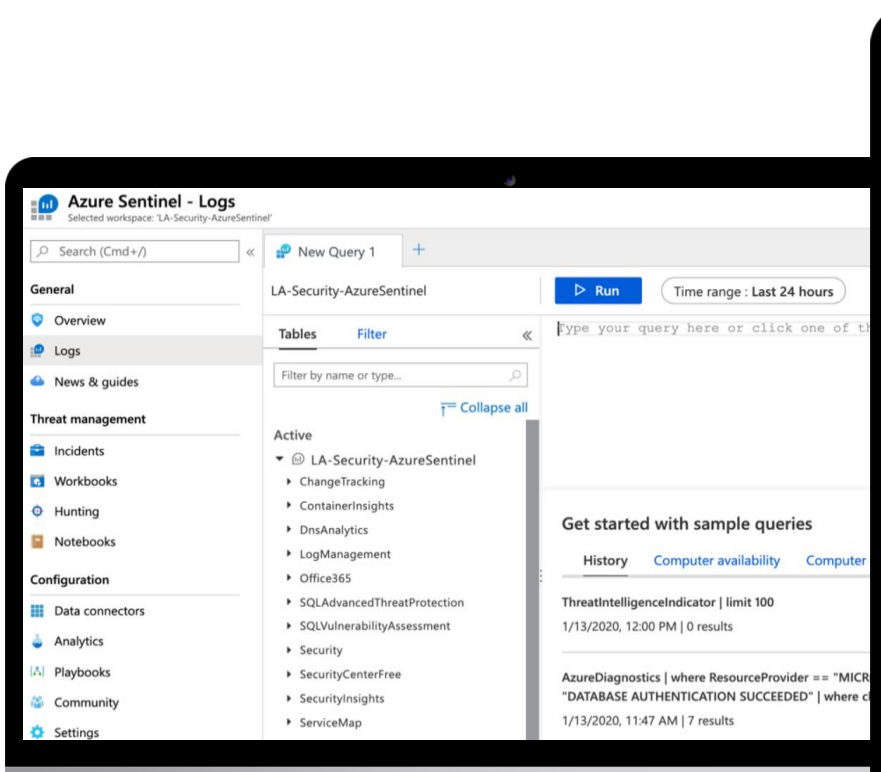
- ✓ 24/7 surveillance and alert services
- ✓ Monitoring internal and external security threats
- ✓ Digital forensics
- ✓ Real-time incident reports
- ✓ Automated Incident response services
- ✓ Professional consulting services
- ✓ Cyber security consulting and training

Microsoft Sentinel – Log manager, analytics & data connectors

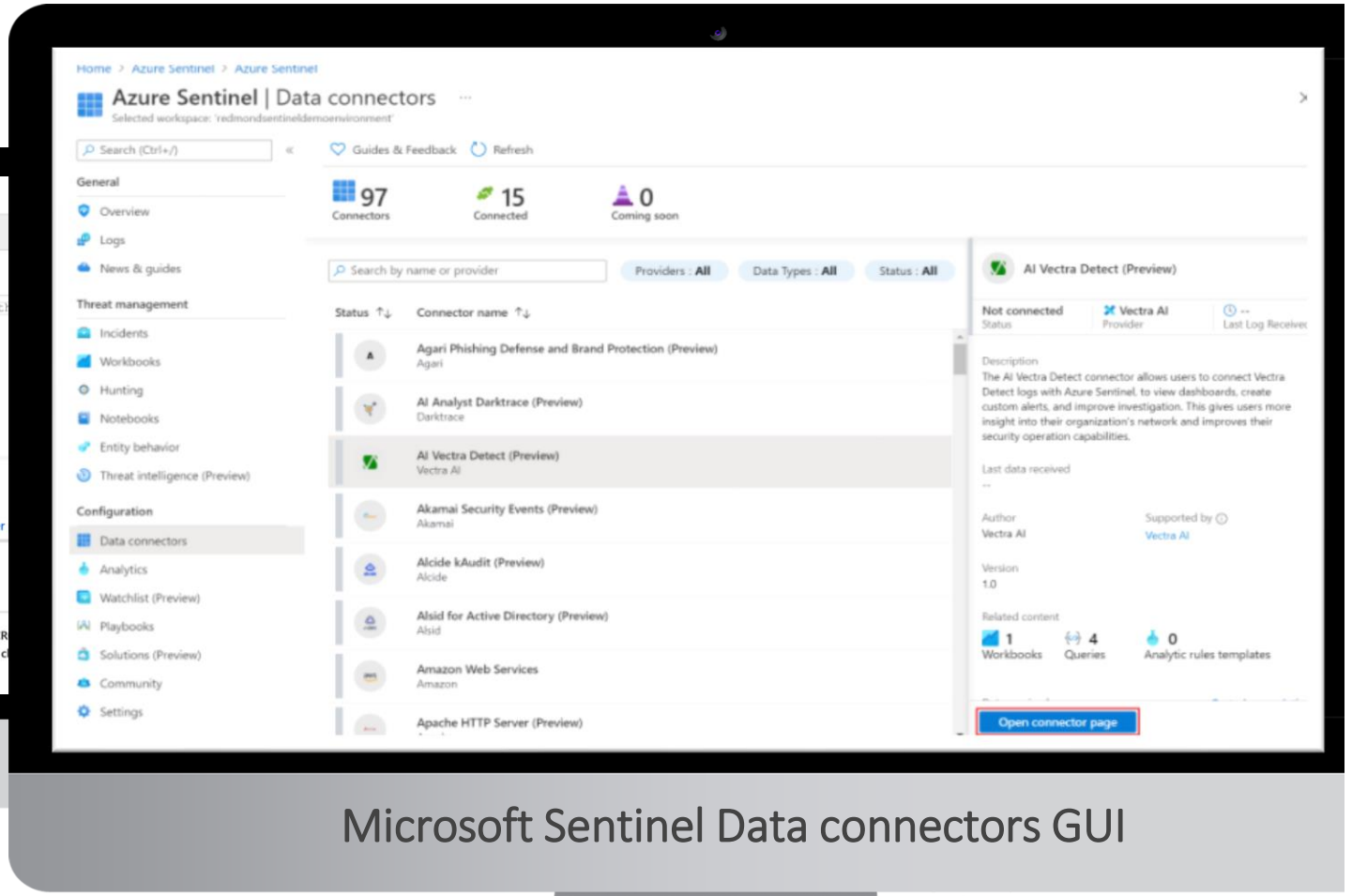
- Microsoft Sentinel Log Manager provides high event-rate processing, long-term data retention, regional data aggregation, and simple searching and reporting functionality for a broad range of applications and devices.
- Microsoft Sentinel Analytics is where you set up rules to find issues with your environment. You can create various types of rules, each with its own configuration steps and niche for the types of abnormalities you are trying to detect.
- Microsoft Sentinel Data connectors, shows the full list of connectors that Microsoft Sentinel provides, and their status in your workspace.



Microsoft Sentinel visual interface



Microsoft Sentinel Log manager



Microsoft Sentinel Data connectors GUI

Pricing

SOC AS A SERVICE - Pricing based on 4weeks POC	
Security operations center (SOC) 24x7 service - Negotiable	**EUR 25,000.00**
Realtime incident reports (Daily, Weekly, Monthly) - Negotiable	
Service Level Agreement (Response time) - Negotiable	