LOGRHYTHM & KUDELSKI SECURITY

Complete Security Protection

Secure and simplify your IT infrastructure with Kudelski Security and LogRhythm

Together, Kudelski Security and LogRhythm have helped hundreds of organizations worldwide secure their networks – everything from ICS/SCADA infrastructure to cloud and SaaS solutions.

Kudelski Security has vast experience delivering tailored, business-oriented security solutions. In 2021, the company was named LogRhythm's European Sales Partner of the Year for the second year in a row. Since 2016, Kudelski Security has integrated LogRhythm technologies to support its Cyber Fusion Centers in Switzerland and the United States.

With over 300 engineers and security professionals on hand, Kudelski Security has the capabilities to design, install, configure, and manage solutions using LogRhythm security technology for any enterprise environment. Additionally, Kudelski Security's Cyber Fusion Centers enable organizations to immediately realize the value of their investments by delivering 24x7x365 Managed Detection & Response with LogRhythm technology.

A Security-First Platform

The LogRhythm NextGen SIEM Platform empowers organizations to advance their overall security posture and operations maturity. It delivers a unified user experience that includes real-time visibility, customizable dashboards, and streamlined workflows. The platform provides capabilities needed to simplify work and decrease detection and response time. Kudelski Security supports most of the following features:
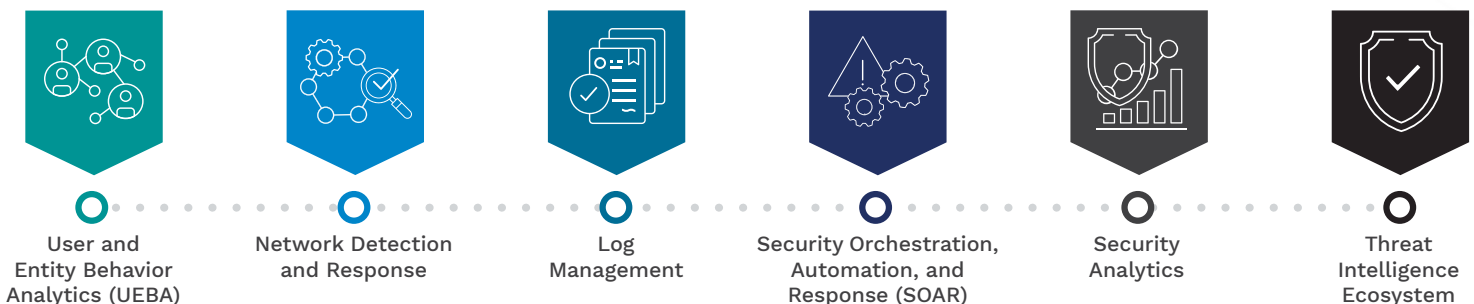
| User and Entity Behavior Analytics (UEBA) | Network Detection and Response | Log Management | Security Orchestration, Automation, and Response (SOAR) | Security Analytics | Threat Intelligence Ecosystem |

Kudelski Security

Next-Generation Managed Detection and Response (MDR)

Kudelski Security amplifies the power of the LogRhythm solution through its world class MDR offerings, providing security teams a range of additional benefits:
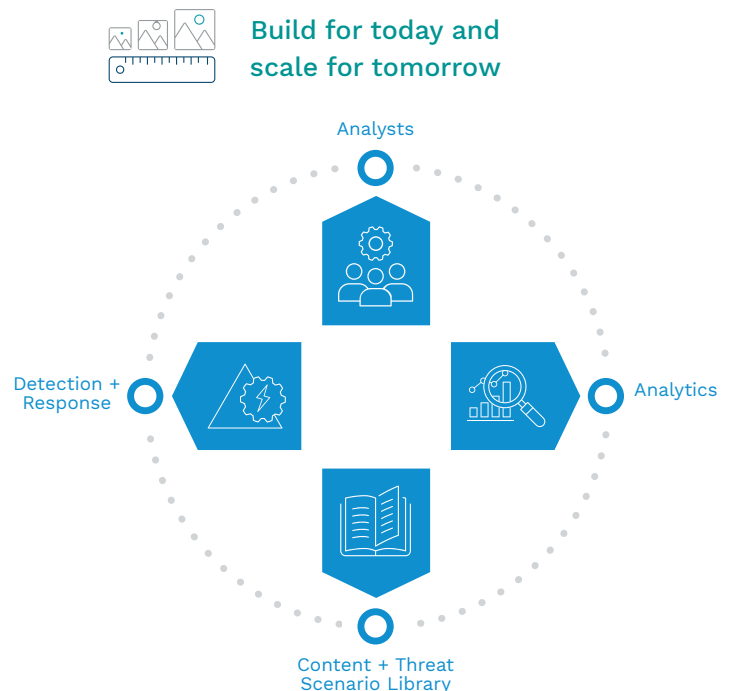
- **Prioritized security visibility based on your threat model**
  - ✓ We leverage custom-built tooling to help you build your threat model – highlighting attack techniques that are likely to target your business
  - ✓ We use the defined threat model to help prioritize which data to send to LogRhythm to make the most impact on your security visibility gaps
- **Reduce attack detection and response time**
  - ✓ We leverage rich contextualization, tailored use case scenarios, and detection rules mapped with the latest MITRE ATT&CK techniques
  - ✓ We deliver fast, effective threat analysis and thorough investigation of relevant alerts
  - ✓ Daily, human-led threat hunting detects hidden activity of an advanced attack, which would otherwise be missed
- **Adopt a streamlined response** to incidents with clear, actionable recommendations
- **Gain access to the CFC's LogRhythm detections** that are continuously updated to detect new threats and attacker technique
- **Gain broad visibility** into the state of your security visibility, through our MSS client portal
- **Easy-to-understand dashboards and monthly service reporting**

LogRhythm

Next-Generation Security Solutions

The LogRhythm NextGen SIEM Platform powers security operation centers (SOCs) and helps organizations improve security posture and operations maturity:

- **Detect threats earlier and faster** by enabling security analysts to surface threats, search through log data, make decisions, collaborate, and respond quickly to security incidents
- **Surface both known and unknown threats** as they occur through machine learning and scenario-based analytics
- **Save time writing scripts, building rules, and creating reports** using a library of updated security content and threat scenarios
- **Eliminate blind spots** with network detection and response capabilities for complete visibility

Build for today and scale for tomorrow

Analysts

Detection + Response

Analytics

Content + Threat Scenario Library

KUDELSKI SECURITY