

# SIEM-Integrations-Service für Cloud-verwaltete LANCOM R&S®Unified Firewalls



**Insbesondere für größere Unternehmen und Managed Service Provider (MSPs) ist ein robustes Sicherheitsmanagement unerlässlich. Ein zentrales Security Information and Event Management (SIEM)-System hilft Unternehmen, Sicherheitsbedrohungen schnell zu erkennen, zu analysieren und darauf zu reagieren, um Schäden am Geschäftsbetrieb zu verhindern.**

**Wir laden Sie ein, Ihr SIEM mit unserem Integrations-Service für Cloud-verwaltete LANCOM R&S®Unified Firewalls zu erweitern, um eine umfassende Erkennung von Angriffen auf Ihre Netzwerkinfrastruktur zu gewährleisten.**

## **Konformität mit marktführenden SIEM-Systemen**

Unsere Lösung vereinfacht die Integration mit gängigen SIEM-Systemen wie Microsoft Azure Sentinel, Splunk, Enginsight, Wazuh und Logpoint entscheidend. Die LANCOM Management Cloud (LMC) sammelt Ereignisprotokolle von allen verwalteten Unified Firewalls in einem Netzwerk und bietet einen einzigen Endpunkt für SIEM-Systeme, um alle Logs im Standard-JSON-Format abzurufen. Dieses Setup gewährleistet eine schnelle Sichtbarkeit von Angriffen auf die Netzwerkinfrastruktur und ermöglicht eine schnelle Reaktion auf Bedrohungen wie Viren, Malware und DDoS-Angriffe.

## Einfache Einrichtung mit dem LANCOM SIEM-Integrations-Service

Unser erfahrenes Support-Team unterstützt Sie bei einer unkomplizierten Integration:

- 1. Erstellen Sie ein Ticket beim LANCOM Support:** Eröffnen Sie ein Support-Ticket und stellen somit die Anfrage für den SIEM-Integrations-Service.
- 2. LANCOM Support meldet sich bei Ihnen:** Unser Team bereitet die notwendigen Konfigurationen für die Unified Firewalls und die LANCOM Management Cloud vor.
- 3. Sicherheits-Token erhalten:** Nach der Einrichtung erhalten Sie ein Sicherheits-Token für die sichere Kommunikation zwischen der LMC und Ihrem SIEM-System.
- 4. Rollout der Konfiguration:** Zu einem Zeitpunkt Ihrer Wahl rollen Sie die Konfiguration Ihrer Unified Firewalls über die LMC aus und aktualisieren bei Bedarf deren Firmware.
- 5. Konfigurieren Sie die Schnittstelle in Ihrem SIEM:** Wir stellen Ihnen bei Bedarf alle notwendigen Informationen zum Abrufen und Analysieren der Logs zur Verfügung.

## Technische Voraussetzungen

- Ihre LANCOM R&S®Unified Firewalls (alle Modelle) werden in der LANCOM Management Cloud (LMC) verwaltet.
- Mindest-Firmware-Version:
  - LCOS FX 10.13.6566 (REL) oder höher
  - LCOS FX-I 1.0 oder höher
- Die Firewalls sind einem Standort zugewiesen und als Gateway konfiguriert
- Sie haben Ihre Cloud-ID oder UUID zur Hand
- Sie haben Zugang zur LMC, um die Firewalls zu aktualisieren und die Konfigurationen auszurollen.

Durch die Integration von Cloud-verwalteten Unified Firewalls in Ihr SIEM können Sie Ihre Sicherheitsprozesse optimieren und Ihre IT-Infrastruktur schützen. Unser Integrations-Service sorgt für einen reibungslosen Rollout.

**Nehmen Sie noch heute Kontakt mit uns auf!**

