SIEM-INTEGRATIONS-SERVICE FÜR CLOUD-VERWALTETE R&S®LANCOM 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 R&S®LANCOM 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 R&S®LANCOM Management Cloud (R&S®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 R&S Networks and Cybersecurity SIEM-Integrations-Service

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

1. **Erstellen Sie ein Ticket beim R&S Networks and Cybersecurity Support:** Eröffnen Sie ein Support-Ticket und stellen somit die Anfrage für den SIEM-Integrations-Service.
2. **R&S Networks and Cybersecurity Support meldet sich bei Ihnen:** Unser Team bereitet die notwendigen Konfigurationen für die Unified Firewalls und die R&S®LANCOM Management Cloud vor.
3. **Sicherheits-Token erhalten:** Nach der Einrichtung erhalten Sie ein Sicherheits-Token für die sichere Kommunikation zwischen der R&S®LMC und Ihrem SIEM-System.
4. **Rollout der Konfiguration:** Zu einem Zeitpunkt Ihrer Wahl rollen Sie die Konfiguration Ihrer Unified Firewalls über die R&S®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.

VERWENDUNG VON SIEM MIT R&S®LANCOM UNIFIED FIREWALLS IN DER R&S®LANCOM MANAGEMENT CLOUD (ONELOG)

Im Folgenden wird beschrieben, wie ein SIEM-System mit R&S®LANCOM Unified Firewalls in der R&S®LMC verwendet werden kann.

Voraussetzungen

- Ihre R&S®LANCOM Unified Firewalls muss durch die R&S®LMC verwaltet werden.
- Die Unified Firewall muss einem Standort zugewiesen sein.
- Die Unified Firewall muss die Rolle ‚Gateway' haben.
- Zugang zur R&S®LMC zur Aktualisierung der Unified Firewall und Rollout der Konfiguration
- LCOS FX ab Version 10.13 Rel (download aktuelle Version)
- Bereits konfiguriertes und funktionsfähiges SIEM-System

Die SIEM-Implementierung in der R&S®LMC wurde mit den folgenden SIEM-Systemen erfolgreich getestet:

- Microsoft Sentinel
- Splunk
- Enginsight
- Wazuh
- Logpoint

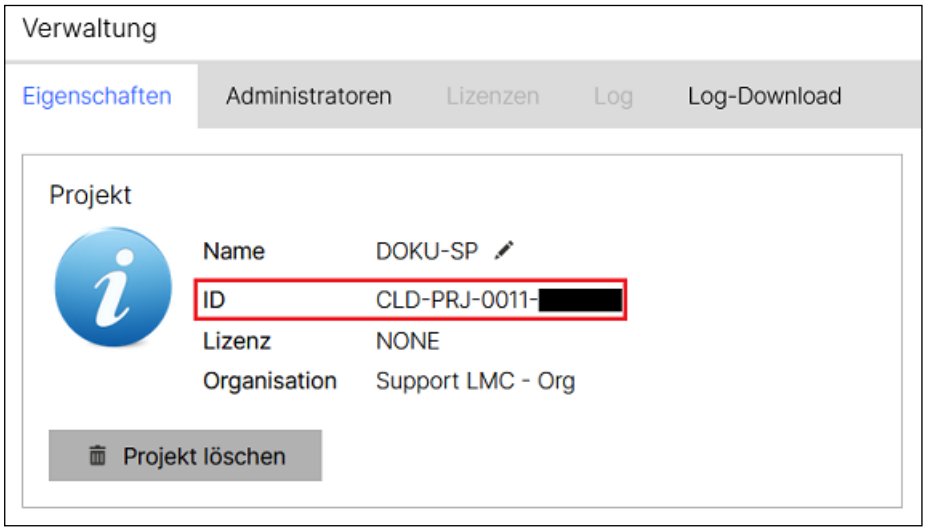
VORGEHENSWEISE

1. SIEM-Unterstützung in der R&S®LMC aktivieren

Die SIEM-Unterstützung wird auf Ihre Anfrage durch Rohde & Schwarz Networks and Cybersecurity in Ihrem R&S®LMC-Projekt aktiviert.

Stellen Sie eine Anfrage zur Aktivierung der SIEM-Unterstützung an den R&S Networks and Cybersecurity Support und senden in dieser Ihre Projekt-ID mit.

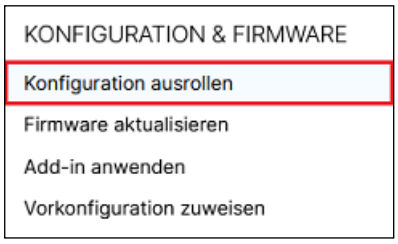
Die Projekt-ID finden Sie in der R&S®LMC im Menü ‚Verwaltung → Eigenschaften'.



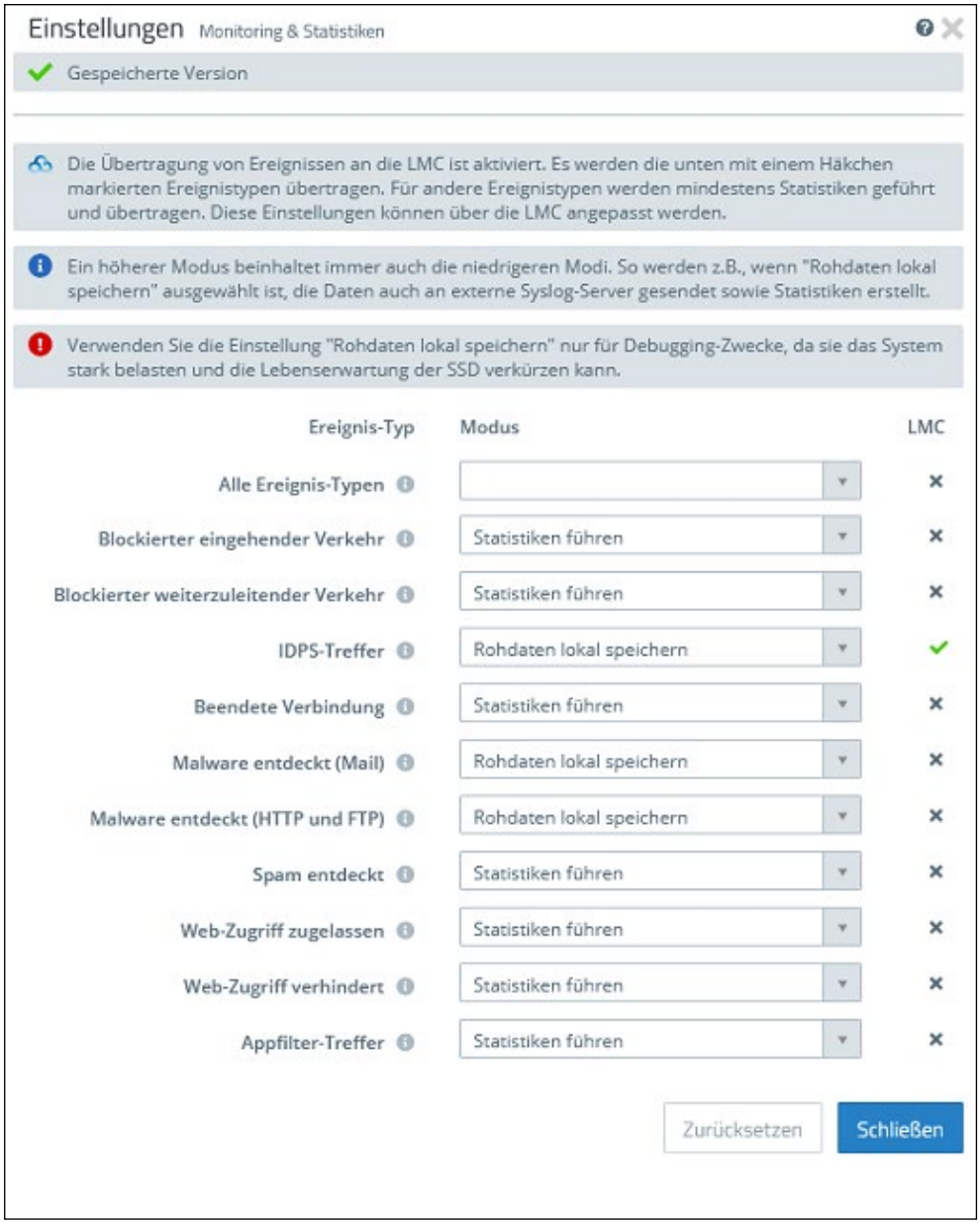
2. IDPS-Meldungen von der Unified Firewall für das SIEM-System bereitstellen

Nach der Aktivierung der SIEM-Unterstützung wechselt die Unified Firewall in den Status ‚Nicht aktuell'. Rollen Sie die Konfiguration auf die Unified Firewall aus, um IDPS-Meldungen für das SIEM-System bereitzustellen.

Mit Stand Dezember 2024 werden nur IDPS-Meldungen bereitgestellt. In zukünftigen R&S®LMC- und LCOS FX-Versionen wird die Unterstützung für weitere Logs implementiert.

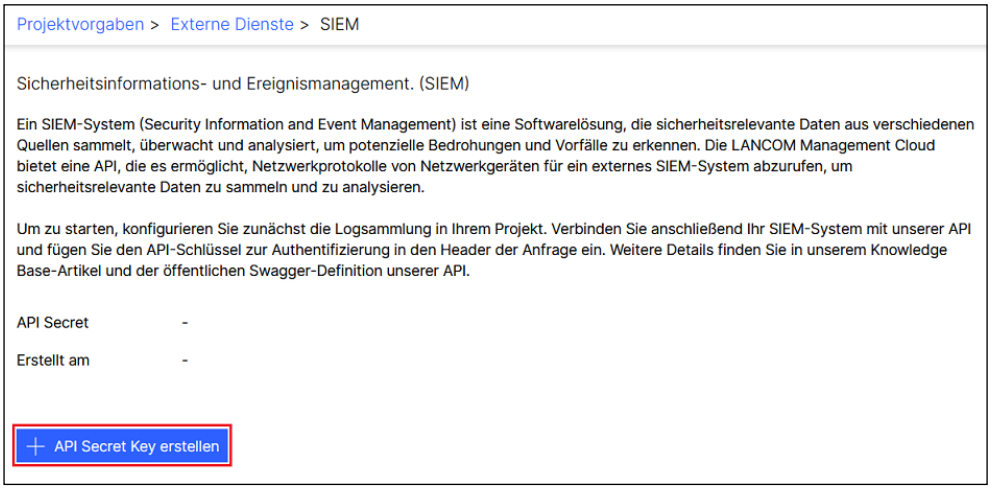


Verbinden Sie sich per WEBconfig-Tunnel in der R&S®LMC mit der Unified Firewall und prüfen im Menü ‚Monitoring & Statistiken → Einstellungen', ob die zusätzliche Spalte R&S®LMC ausgerollt wurde und die Option für die IDPS-Treffer aktiv ist.

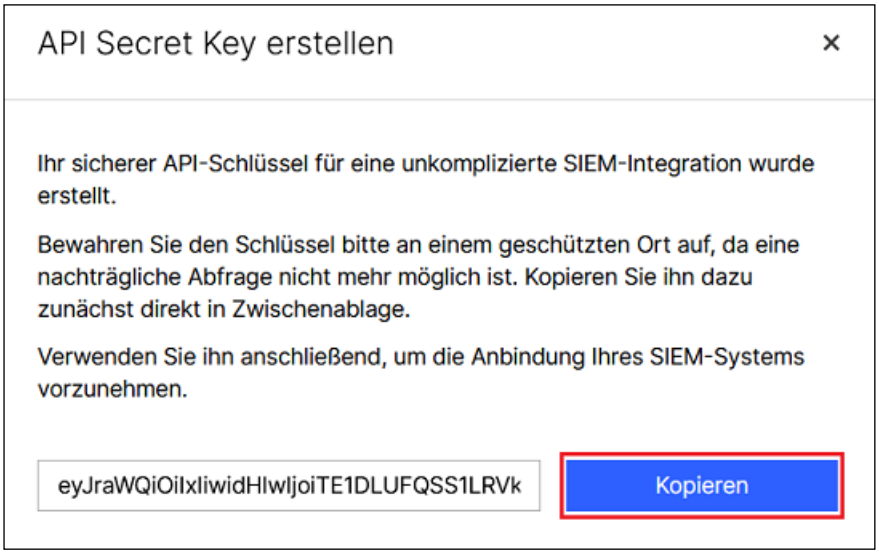


3. SIEM-API-Secret in der R&S®LMC generieren

Wechseln Sie in der R&S®LMC in das Menü ‚Projektvorgaben → Externe Dienste → SIEM' und klicken Sie auf ‚API Secret Key erstellen'.



Kopieren Sie den Secret Key und speichern diesen gesichert ab. Tragen Sie den Secret Key anschließend in Ihrem SIEM-System ein.

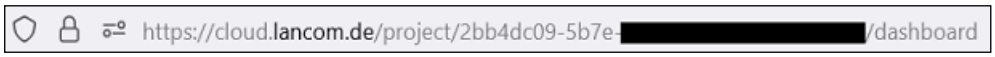


4. Beispiel-Befehle in der SIEM-API

Die SIEM-API-Dokumentation (swagger) finden Sie unter dem folgenden Link.

Um die SIEM-API verwenden zu können, benötigen Sie die UUID Ihres R&S®LMC-Projektes sowie den API Secret Key (siehe Schritt 3).

Wenn Sie im R&S®LMC-Projekt eingebucht sind, finden Sie die UUID in der Adresszeile des Browsers hinter project/.



DeviceLogs

Mit dem Endpunkt DeviceLogs können die Geräte-Logs für den angegebenen Account ausgelesen werden.

Der Befehl muss im folgenden Format angegeben werden:

GET /cloud-service-siem/accounts/<UUID Ihres R&S®LMC-Projekts>/logs HTTP/1.1

Host: cloud.lancom.de

Authorization: LMC-API-KEY <API Secret Key (siehe Schritt 3)>

Beispielanfrage zum Testen (ohne gültige Account-Daten oder Secret Key)

curl --request GET \

--url https://cloud.lancom.de/cloud-service-siem/accounts/ea96d5d0-01f6-498a-b9ec-629be24eae9e/logs \

--header ‚Authorization: LMC-API-KEY eyJraWQiOiIxIiwidHlwIjoiTE1DLUFQSS1LRVkiLCJhbGciOiJIUzI1NiJ9.3zezFHKzC YJICgh-3V1KN0yEe8lTUQEE75DXc-Vv2Dc._93wf35NVk8Q6yt7omWzyohTgW58424tQzRFIPgr111‘ \

Erfolgreiche Ausgabe


```
{
  “startOffset”: 10,
  “endOffset”: 109,
  “nextOffset”: 110,
  “count”: 100,
  “deviceLogs”: [
   {
     “deviceId”: “ea96d5d0-01f6-498a-b9ec-629be24eae9e”,
     “accountId”: “ea96d5d0-01f6-498a-b9ec-629be24eae9e”,
     “siteId”: “ea96d5d0-01f6-498a-b9ec-629be24eae9e”,
```

```
    "messageId": "8bb136e3-0c4e-459e-8cd7-85b8209e2e3b",
    "createdAt": "2022-12-21T13:17:40.78731Z",
    "receivedAt": "2022-12-21T13:17:40.78731Z",
    "rawMessage": "IDPS: Malicious message detected [Classification: ] [Severity: 3] [Signature Id: 5000000] [Action: allowed] [Source: 10.10.10.20:0] [Destination: 8.8.76.5:0]",
    "severity": "3",
    "additionalProperties": {
      "category": "IDPS",
      "idps_event_type": "alert",
      "signature": "5000000",
      "idps_category": "",
      "source_ip": "10.10.10.20",
      "source_port": "0",
      "destination_ip": "8.8.76.5",
      "destination_port": "0",
      "action": "allowed"
    }
  }
 ],
 "_links": {
   "self": "https://cloud.lancom.de/cloud-service-siem/accounts/ea96d5d0-01f6-498a-b9ec-629be24eae9e/logs?offset=1&limit=100",
   "next": "https://cloud.lancom.de/cloud-service-siem/accounts/ea96d5d0-01f6-498a-b9ec-629be24eae9e/logs?offset=101&limit=100"
 }
}
```


Offsets

Mit dem Endpunkt Offsets wird für den angegebenen Account die Nummer der ersten Log-Datei und der nächsten ungelesenen Log-Datei sowie das Offset-Limit ausgegeben.

Der Befehl muss im folgenden Format angegeben werden:

GET /cloud-service-siem/accounts/<UUID Ihres R&S®LMC-Projekts>/offsets HTTP/1.1

Host: cloud.lancom.de

Authorization: LMC-API-KEY <API Secret Key (siehe Schritt 3)>

Beispielanfrage zum Testen (ohne gültige Account-Daten oder Secret Key)

```
curl --request GET \
--url https://cloud.lancom.de/cloud-service-siem/accounts/30995a43-3705-439a-9c2c-da1331bb5106/offsets \
--header 'Authorization: LMC-API-KEY eyJraWQiOiIxIiwidHlwIjoiTE1DLUFQSS1LRVkiLCJhbGciOiJIUzI1NiJ9.3zezFHKzC
YJlCgh-3V1KN0yEe8lTUQEE75DXc-Vv2Dc._93wf35NVk8Q6yt7omWzyohTgW58424tQzRFIP11111' \
```

Erfolgreiche Ausgabe

```
{
  "startMinOffset": 0,
  "nextUnreadOffset": 99,
  "endMaxOffset": 100
}
```

Technische Voraussetzungen

- Ihre R&S®LANCOM Unified Firewalls (alle Modelle) werden in der R&S®LANCOM Management Cloud (R&S®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 R&S®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!

Rohde & Schwarz Networks and Cybersecurity GmbH
Adenauerstr. 20/B2
52146 Würselen | Deutschland
info.rs-nc@rohde-schwarz.com | www.rohde-schwarz.com/networks-and-cybersecurity

ROHDE&SCHWARZ
Make ideas real