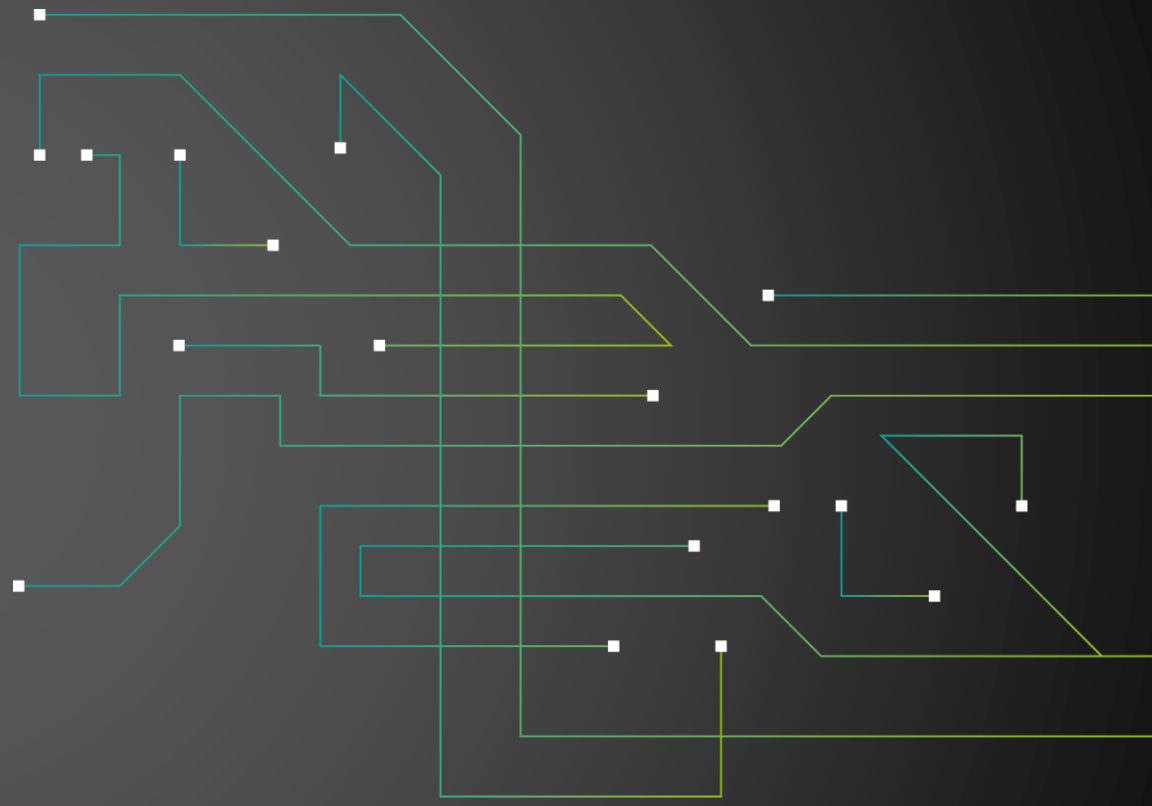
BASE-IT

Webcast: SENTINEL



professional.
fast.
secure.

AGENDA

basc it

1. Was ist Sentinel
2. Log Analytics
3. Data Connectors
4. Analytic Rules
5. Automation

WAS IST SENTINEL

SIEM & SOAR

Sammeln Sie Daten auf Cloudebene – für alle Benutzer, Geräte, Anwendungen und Infrastrukturen, lokal und in mehreren Clouds.

Ermitteln Sie bisher unentdeckte Bedrohungen, und minimieren Sie falsch positive Ergebnisse mithilfe von Analysefunktionen und den unvergleichlichen Informationen zu Bedrohungen von Microsoft.

Untersuchen Sie Bedrohungen mit KI, und verfolgen Sie verdächtige Aktivitäten in großem Stil. Dabei profitieren Sie von der jahrzehntelangen Erfahrung von Microsoft in Sachen Cybersicherheit.

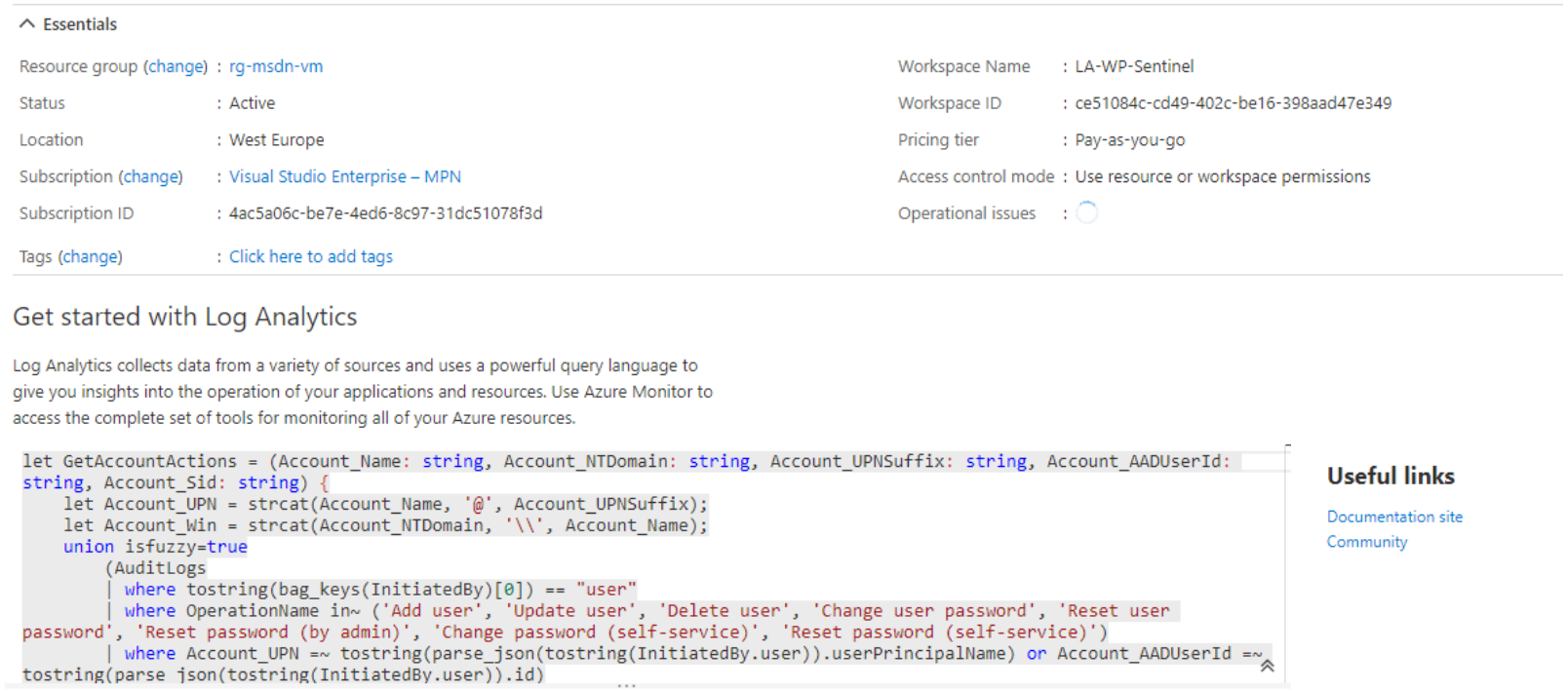
Reagieren Sie dank der integrierten Orchestrierung und Automatisierung häufiger Aufgaben schnell auf Incidents.

LOG ANALYTICS

basc it

Kusto Query Language

Pricing Pay-as-you-Go



ON-PREM CONNECTION

CEF Syslog

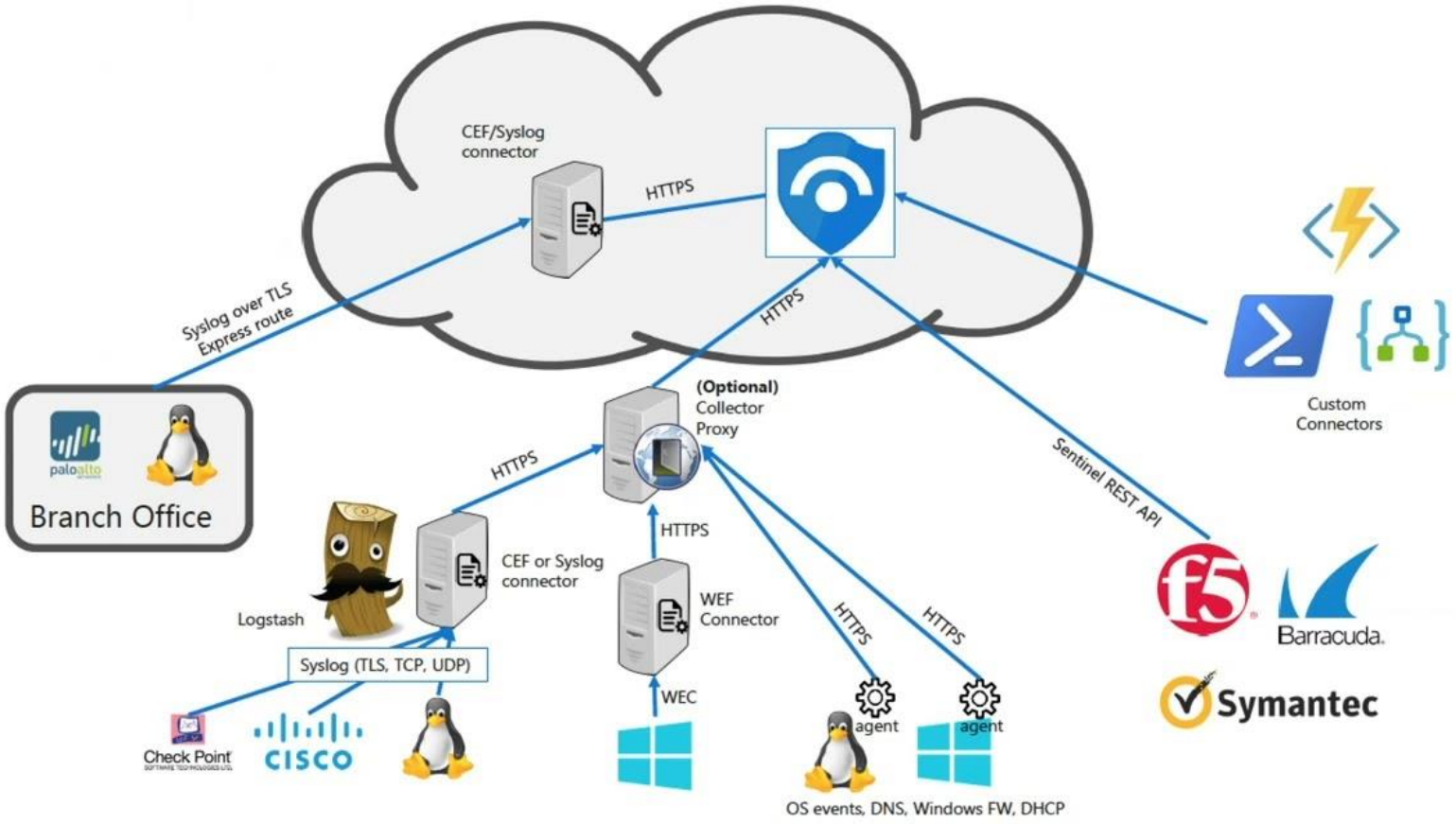
SYSLOG

CEF

<134> Dec 06 16:51:38 hostname CEF:0|JATP|Cortex|3.6.0.1444|email|Phishing|8|externalId=1504 eventId=14067 lastActivityTime=2016-12-06 23:51:38+00 src= dst= src_hostname= dst_hostname= src_username= dst_username=src_email_id=src@abc.comdst_email_id={test@abc.com} startTime=2016-12- 06 23:51:38+00 url=http://greatfilesarey.asia/QA/files_to_pcaps/74280968a4917da52b5555351eeda969.bin fileHash=bce00351cfc559afec5beb90ea387b03788e4af5 fileType=PE32 executable (GUI) Intel 80386, for MS Windows

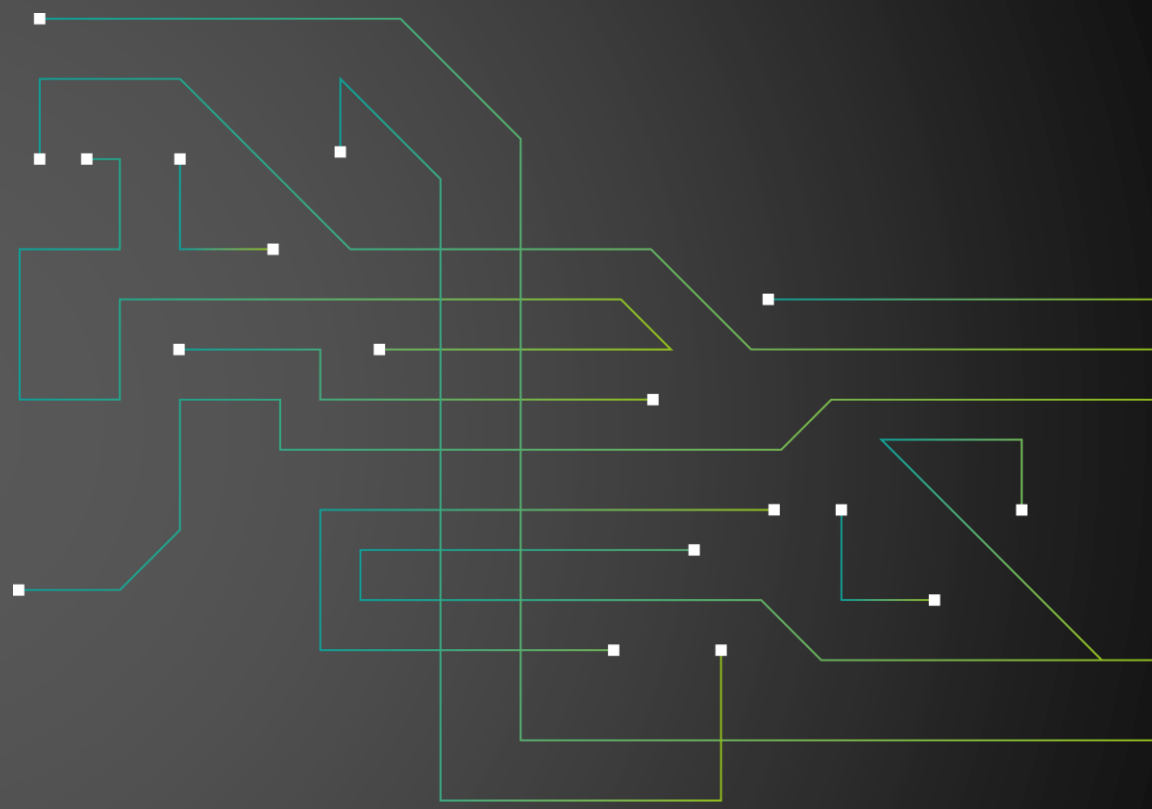
ON-PREM CONNECTION

Connectors



ROBERT SPIESBERGER

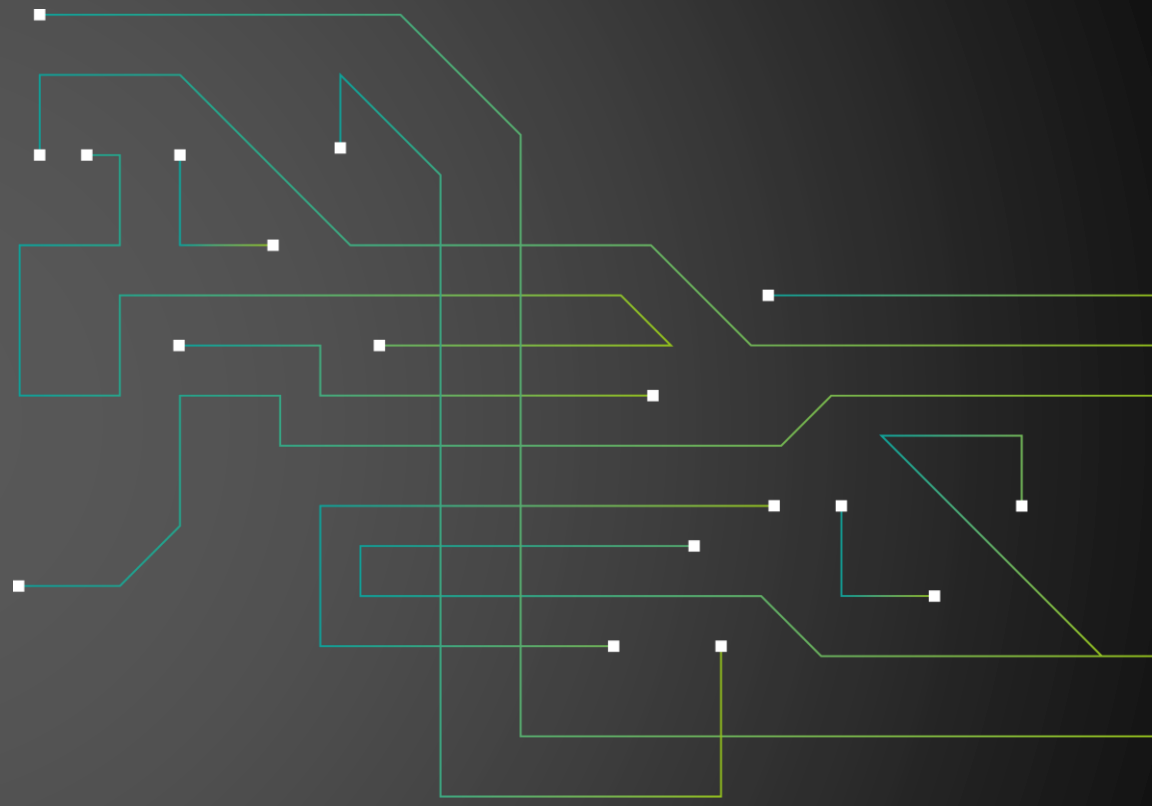
ROBERT.SPIESBERGER@BASEIT.AT



professional.
fast.
secure.

base it

DANKE FÜR IHRE AUFMERKSAMKEIT



professional.
fast.
secure.