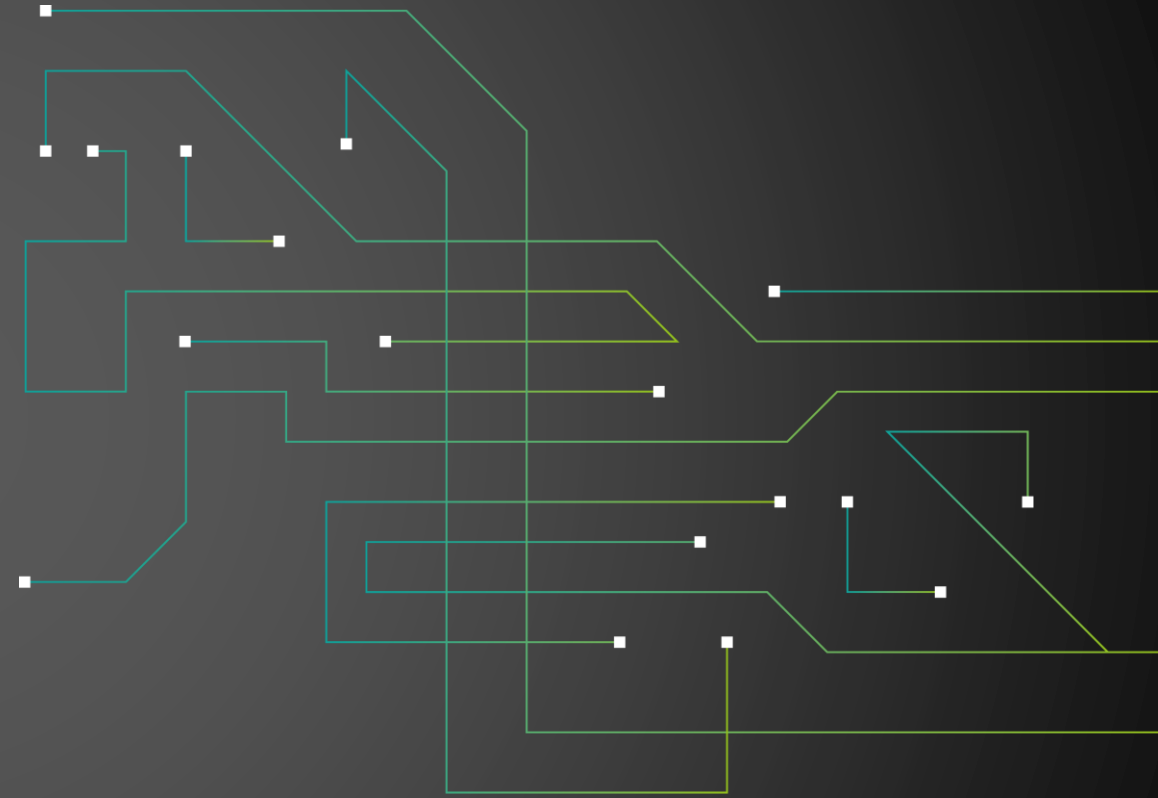


base it



BASE-IT

Webcast: SENTINEL

**professional.
fast.
secure.**

AGENDA

1

Was ist Sentinel

2

Log Analytics

3

Data Connectors

4

Analytic Rules

5

Automation

WAS IST SENTINEL

SIEM & SOAR

baseit



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.

Kusto Query Language

Pricing Pay-as-you-Go

^ Essentials

Resource group (change) : [rg-msdn-vm](#)

Status : Active

Location : West Europe

Subscription (change) : [Visual Studio Enterprise – MPN](#)

Subscription ID : 4ac5a06c-be7e-4ed6-8c97-31dc51078f3d


Tags (change) : [Click here to add tags](#)

Workspace Name : LA-WP-Sentinel

Workspace ID : ce51084c-cd49-402c-be16-398aad47e349

Pricing tier : Pay-as-you-go

Access control mode : Use resource or workspace permissions

Operational issues : 

Get started with Log Analytics

Log Analytics collects data from a variety of sources and uses a powerful query language to give you insights into the operation of your applications and resources. Use Azure Monitor to access the complete set of tools for monitoring all of your Azure resources.

```
let GetAccountActions = (Account_Name: string, Account_NTDomain: string, Account_UPNSuffix: string, Account_AADUserId: string, Account_Sid: string) {
    let Account_UPN = strcat(Account_Name, '@', Account_UPNSuffix);
    let Account_Win = strcat(Account_NTDomain, '\\', Account_Name);
    union isfuzzy=true
        (AuditLogs
        | where tostring(bag_keys(InitiatedBy)[0]) == "user"
        | where OperationName in~ ('Add user', 'Update user', 'Delete user', 'Change user password', 'Reset user password', 'Reset password (by admin)', 'Change password (self-service)', 'Reset password (self-service)')
        | where Account_UPN =~ tostring(parse_json(tostring(InitiatedBy.user)).userPrincipalName) or Account_AADUserId =~ tostring(parse_json(tostring(InitiatedBy.user)).id)
        ...
```

Useful links

[Documentation site](#)
[Community](#)

ON-PREM CONNECTION

CEF Syslog



SYSLOG

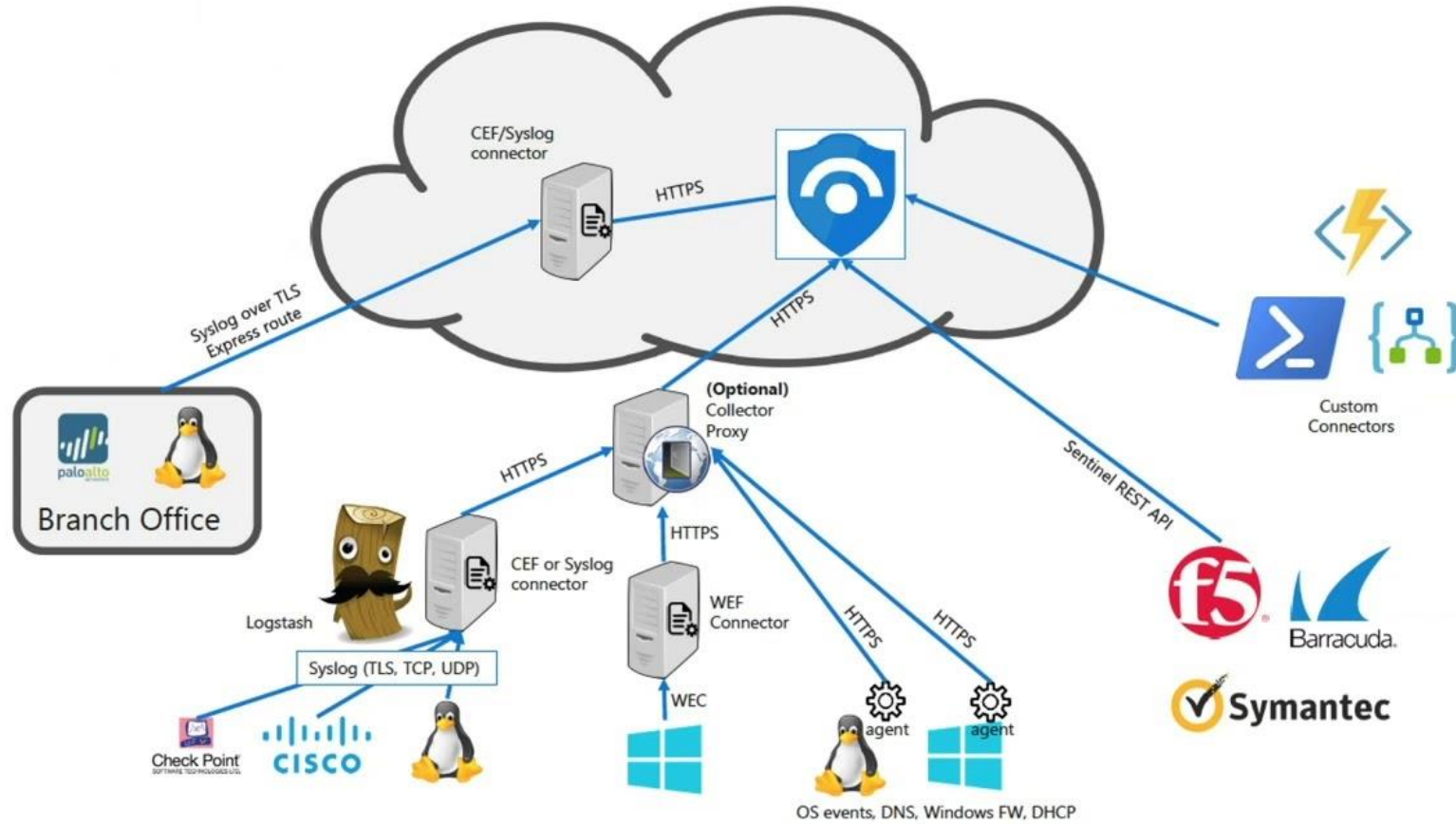
CEF

```
          VERSION                                PROCID
PRI |   TIMESTAMP                                HOSTNAME                                APP-NAME |   MSGID
<165>1 2003-10-11T22:14:15.003Z mymachine.example.com evntslg - ID47
[exampleSDID@32473 iut="3" eventSource="Application" eventID="1011"] BOMAn application event log entry...
STRUCTURED-DATA                                MSG
```

```
<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
```

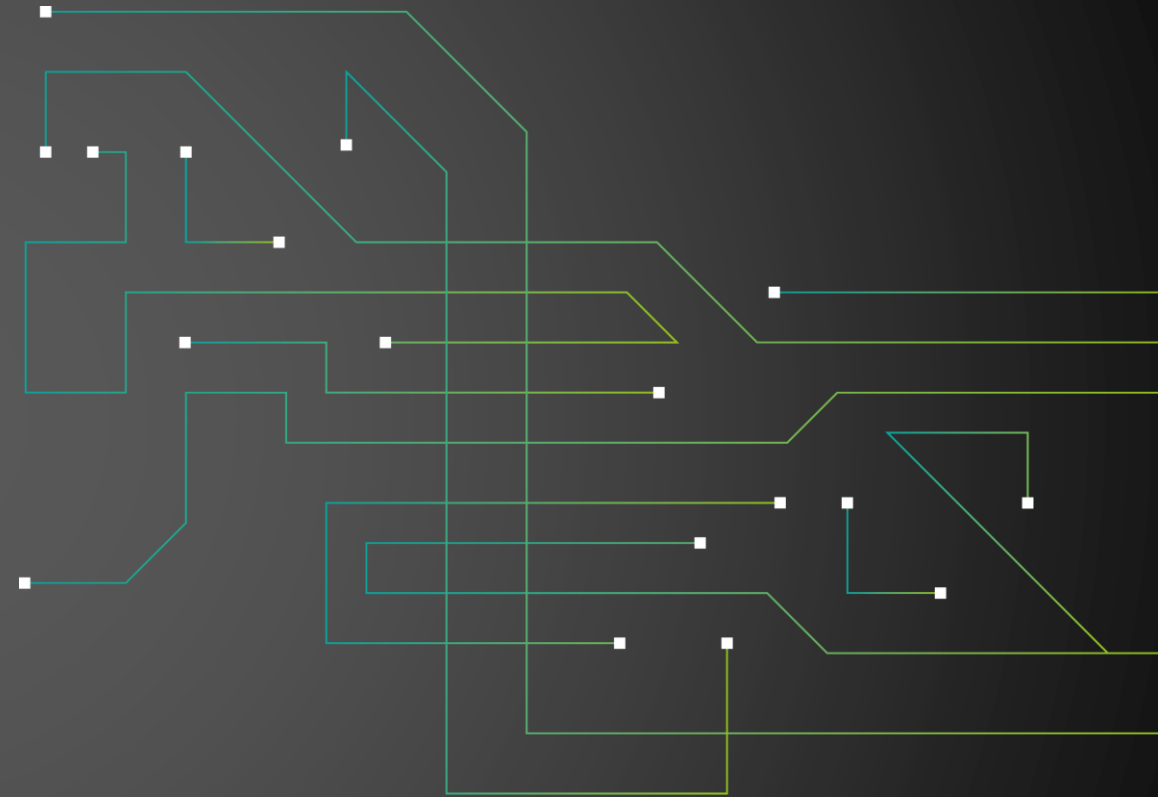
ON-PREM CONNECTION

Connectors



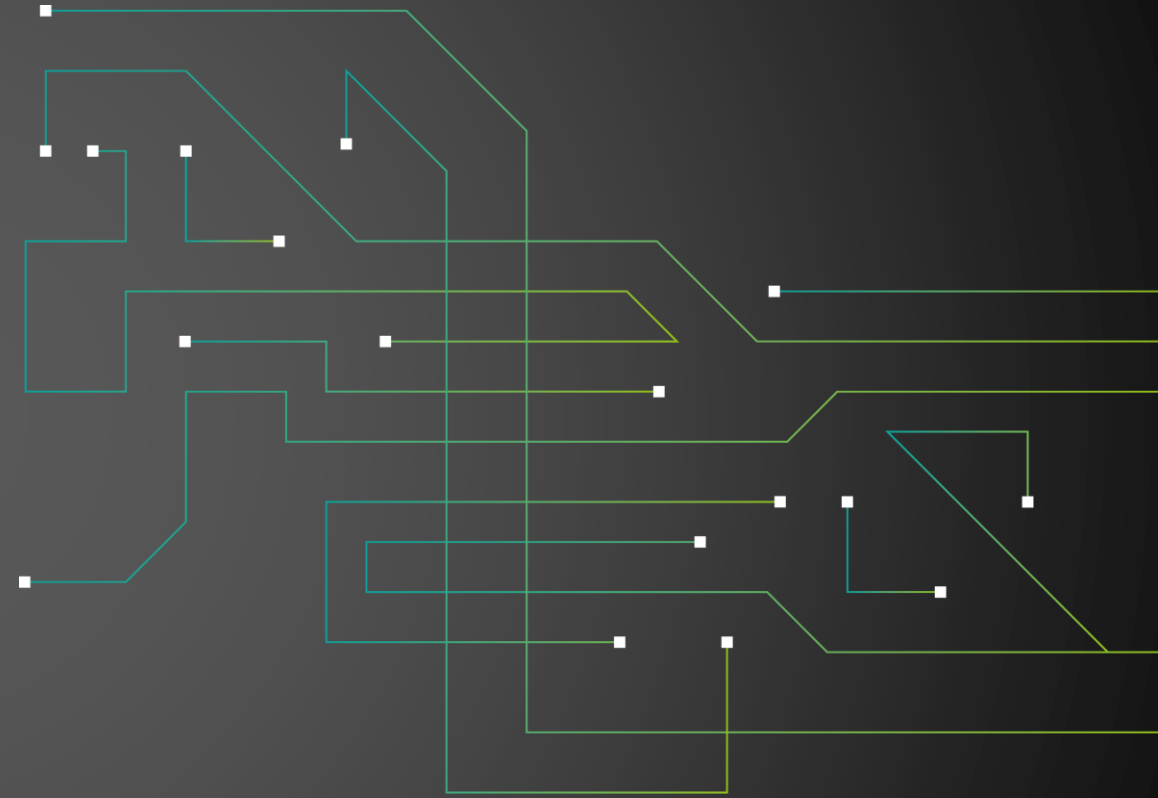
ROBERT SPIESBERGER

ROBERT.SPIESBERGER@BASEIT.AT



professional.
fast.
secure.

**DANKE FÜR IHRE
AUFMERKSAMKEIT**



**professional.
fast.
secure.**