MUNICH AIRPORT

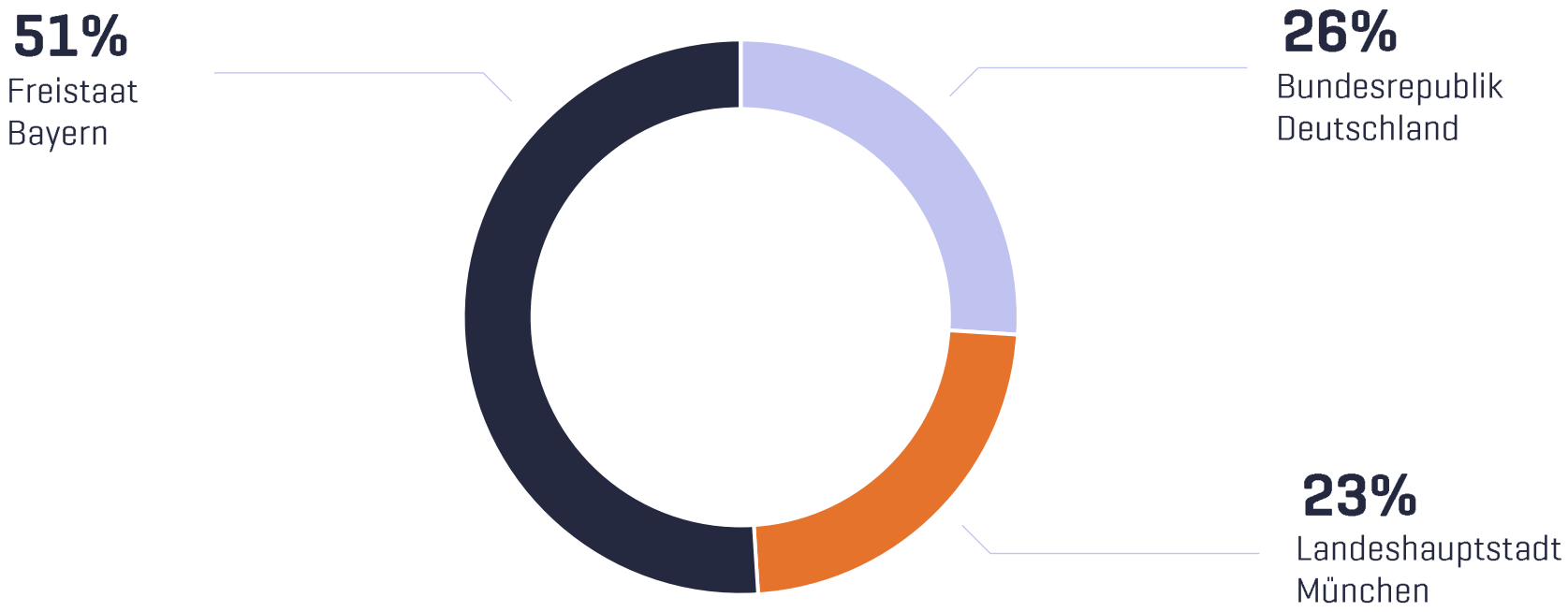
Flughafen München
Zahlen, Fakten und Wissenswertes.

Flughafen München

Unternehmenspräsentation Flughafen München,
Zahlen und Angaben Stand 01/2026

Die Gesellschafter

Gesellschafter der Flughafen München GmbH (FMG) sind der Freistaat Bayern mit 51 Prozent, die Bundesrepublik Deutschland mit 26 Prozent und die Landeshauptstadt München mit 23 Prozent.



Der Flughafen München: faszinierend und vielfältig

337.450
Starts & Landungen

43,4 Millionen
Fluggäste

341.000
Tonnen Luftfracht
und Luftpost

37.000
Beschäftigte am Campus*

468
Betriebe am Campus*

1.575
Hektar Gesamtfläche

Unternehmenspräsentation Flughafen München, Zahlen und Angaben Stand 01/2026 // * Zahlen aus der letzten Beschäftigtenerhebung 2024

Bayerns Tor zur Welt. Weltweiter Knotenpunkt

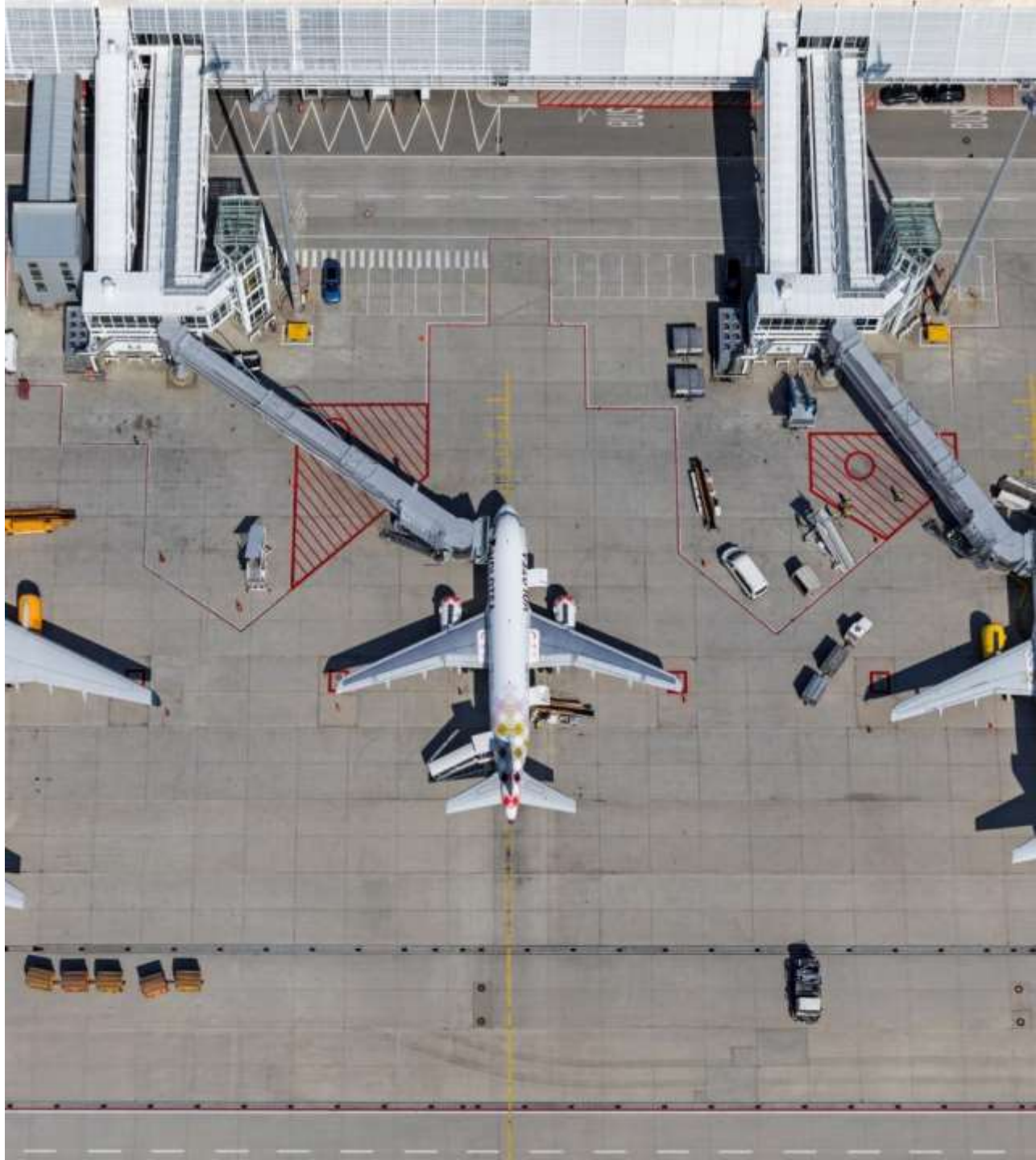
Der Flughafen München ist ein wichtiges internationales Luftverkehrsdrehkreuz.

96*
Fluggesellschaften

232
Ziele

72
Länder

*fünf Airlines davon im reinen Frachtverkehr tätig



Flughafen München setzt Wachstumskurs fort

Der Flughafen München verzeichnete im Jahr 2025 erneut ein deutliches Verkehrswachstum. Insgesamt nutzten 43,4 Millionen Passagiere das bayerische Luftverkehrsdrehkreuz. Gegenüber dem Vorjahr entspricht dies einem Anstieg um 1,8 Millionen Fluggäste und damit einem Passagierwachstum von +4,4%. Der Münchner Airport war damit 2025 der Flughafen mit der höchsten absoluten Passagierzunahme im deutschsprachigen Raum.

Verkehrszahlen	2025	2024	Veränderung
	43,4 Mio.	41,6 Mio.	4,4%
	337.450	327.228	3,1%
	341.000t*	311.091t*	9,5%

Unternehmenspräsentation Flughafen München, Zahlen und Angaben Stand 01/2026 // *Tonnen Luftfracht und Luftpost

Bunte Vielfalt

Der Flughafen München Konzern deckt mit seinen Tochter- und Beteiligungsgesellschaften ein breites Leistungsportfolio ab. Zusätzlich zu seinem Kerngeschäft am Münchner Flughafen bietet der Konzern auch weltweit Beratungs- und Managementdienstleistungen an.

- Check-in, Gepäck- und Flugzeugabfertigung
- Abfertigung von Luftfracht
- Passagier- und Informationsdienste

- Rangieren und Enteisen von Flugzeugen
- Bewachungs- und Sicherheitsdienste
- Betrieb von Ladengeschäften

- Hotel- und Gastronomiebetriebe
- IT-Dienstleistungen
- Gebäudemanagement und vieles mehr

MUNICH AIRPORT

IT am Flughafen München
Zahlen, Fakten und Wissenswertes.

Flughafen München

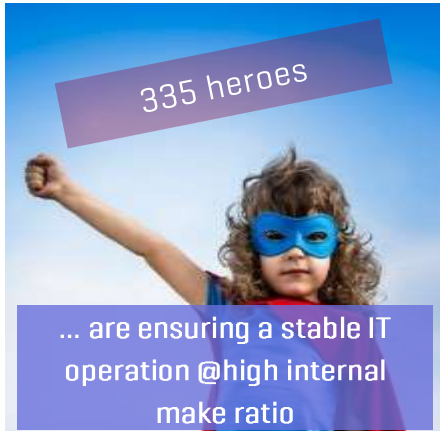
Die IT unseres Flughafens ist Teil der kritischen Infrastruktur, zwingende Voraussetzung für einen stabilen Betrieb und bildet ein sehr breites Lösungsportfolio ab.

★★★★★
5 Star Airport

We manage numerous **digital endpoints**, i.e.

5,400 Windows accounts
42,000 LAN connex ports
15,000 different telephone connections
14,500 different endpoints

3100 UDS displays
900+ applications
3,400 CCTV cameras & clients



Best Airport in Central Europe

1,900 servers
2.3 PB data storage
62,250 km
data cabling

Our heterogeneous **solution portfolio** from ground radar system to PC includes e.g.

Serving over
450+
campus customers
with IT

9,100
employees at the Munich Airport Group

24
different trainee professions within the Group

>100
different nationalities within the Group

MUNICH AIRPORT

SPLUNK
Zahlen, Fakten und Wissenswertes.

MARTIN HABICHT
16.03.2025

Unsere Historie

2016 Splunk Enterprise

IT-Operation
| eval ingest = 800.000.000.000

2018 Splunk Enterprise

IT-Security
| eval ingest = ingest * 6,5

2024 Splunk Enterprise

IT-Security
| eval ingest = ingest + 2.800.000.000.000

2025 Splunk Enterprise Security

IT-Security
| eval ingest = ingest *2

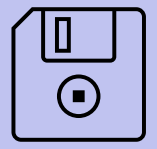
2026 Splunk Enterprise Security

Infrastruktur bis 2017

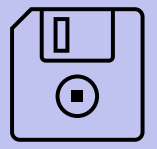
Clustermanager

Search Head

Indexer



Indexer



Infrastruktur bis 2024

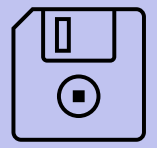
Clustermanager

Search Head

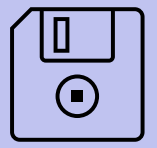
Search Head

Deploymentserver

Indexer

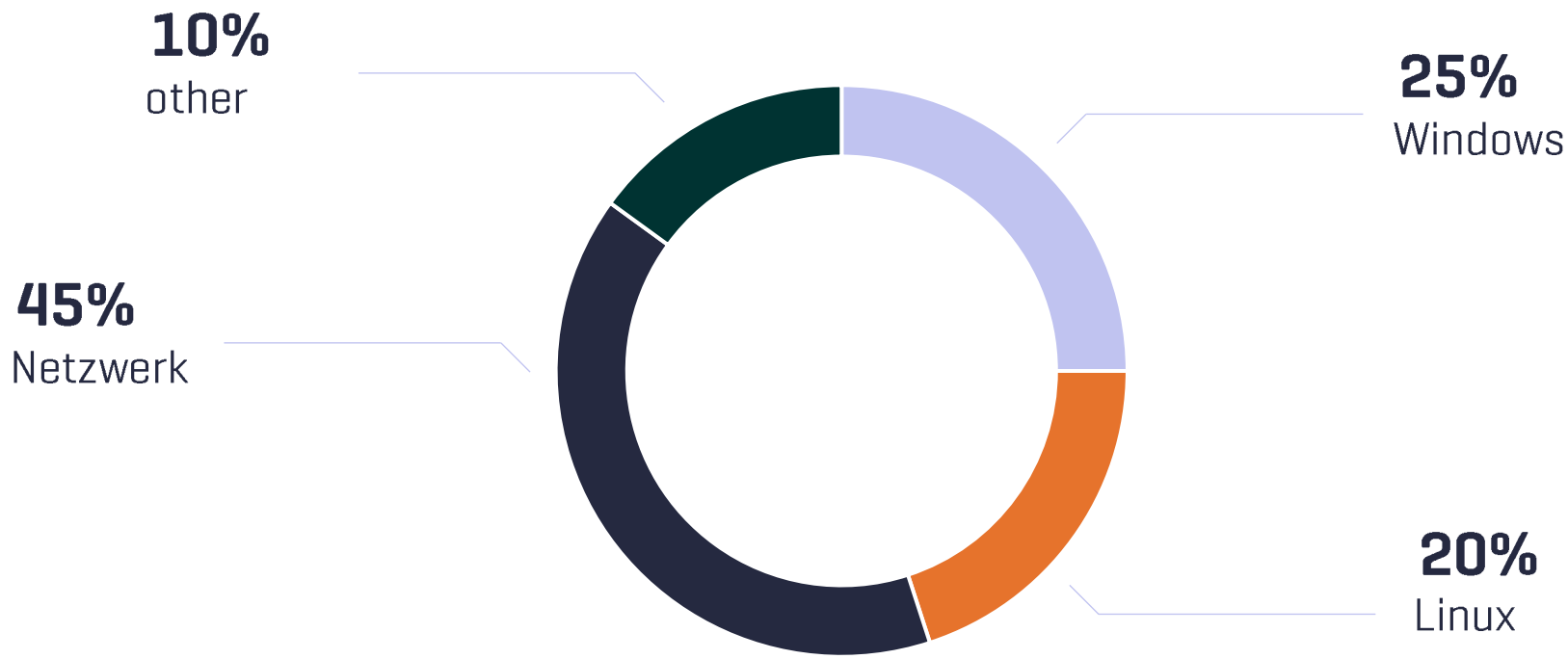


Indexer



650 GB

Logquellen bis 2024



Infrastruktur ab 2025

Clustermanager

Deploymentserver

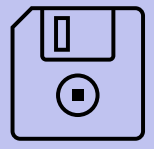
Search Head

Search Head

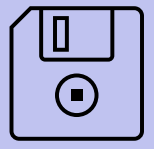
Search Head

Search Head (Backup)

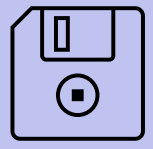
Indexer



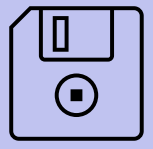
Indexer



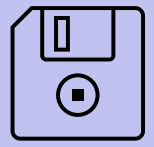
Indexer



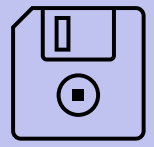
Indexer



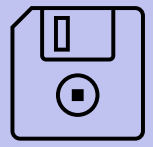
Indexer



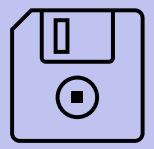
Indexer



Indexer

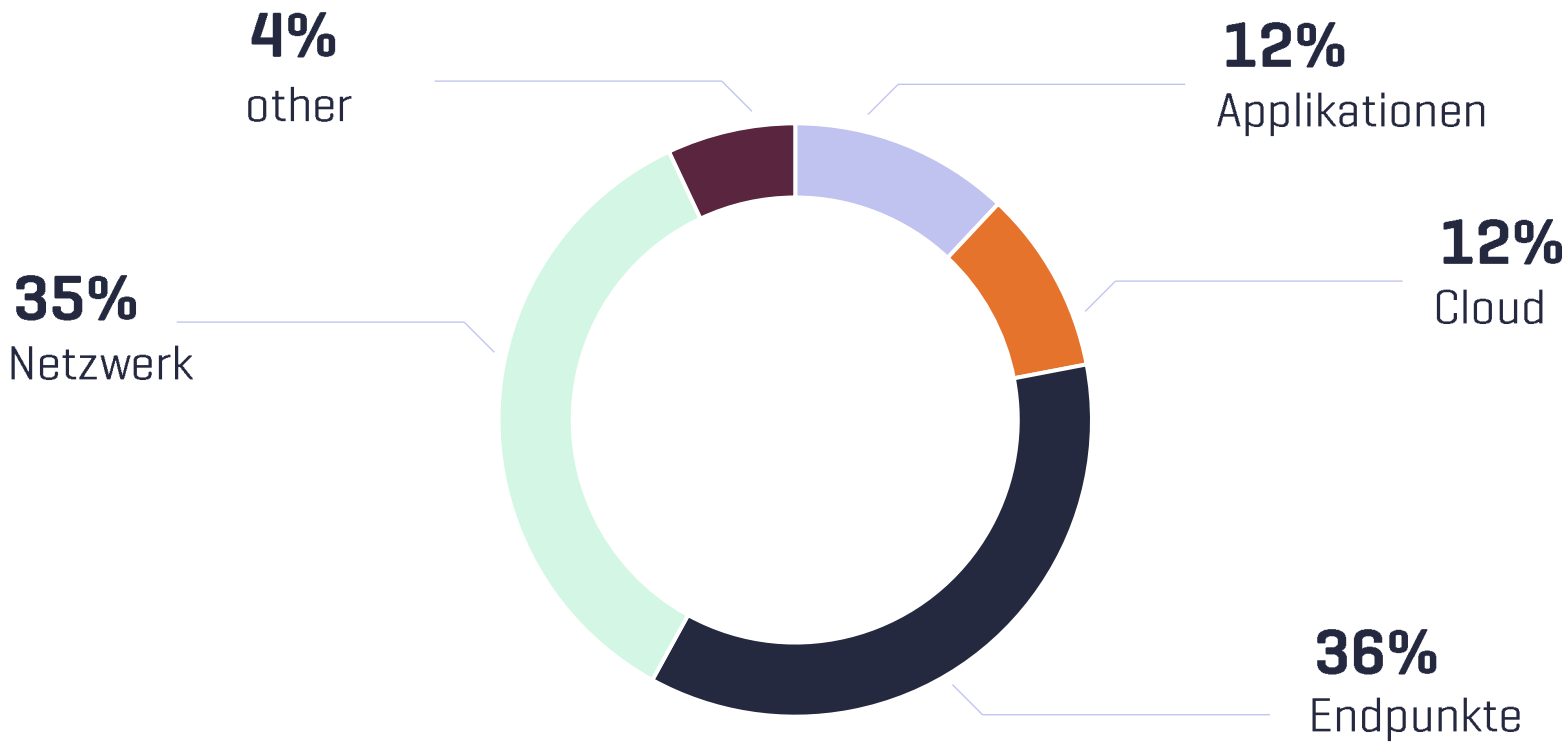


Indexer



2 TB

Logquellen bis 2026



Infrastruktur ab 2026

Clustermanager

Search Head

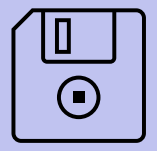
Search Head

Search Head

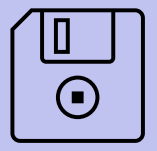
Search Head (Backup)

Deploymentserver

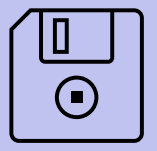
Indexer



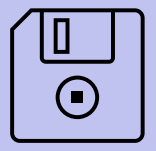
Indexer

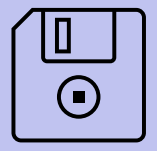


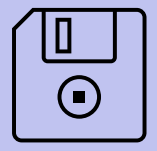
Indexer

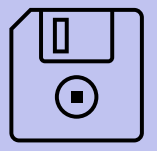


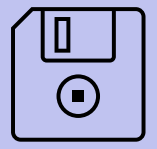
Indexer











Indexer

Indexer

Indexer

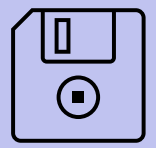
Indexer

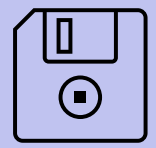
Indexer

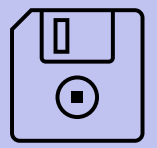
Indexer

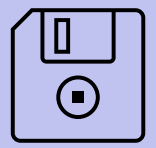
Indexer

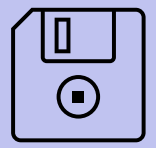
Indexer

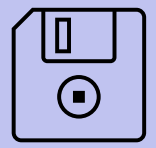


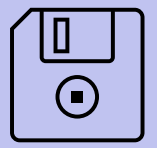


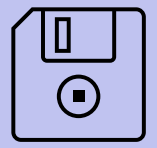












Indexer

Indexer

Indexer

Indexer

Flughafen München

Clusterüberblick

16
Indexer

368 Tage
Datenalter (Median)

215 TB
Indexgröße

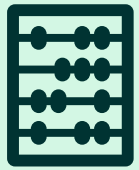
118 TB
Coldstorage

24 TB
Hotstorage

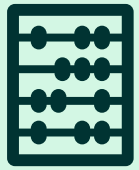
14 TB
pro Indexer

3,5 Billionen
avg. Events per Day

5,5 Billionen
max. Events per Day



128 Cores
Indexer CPU

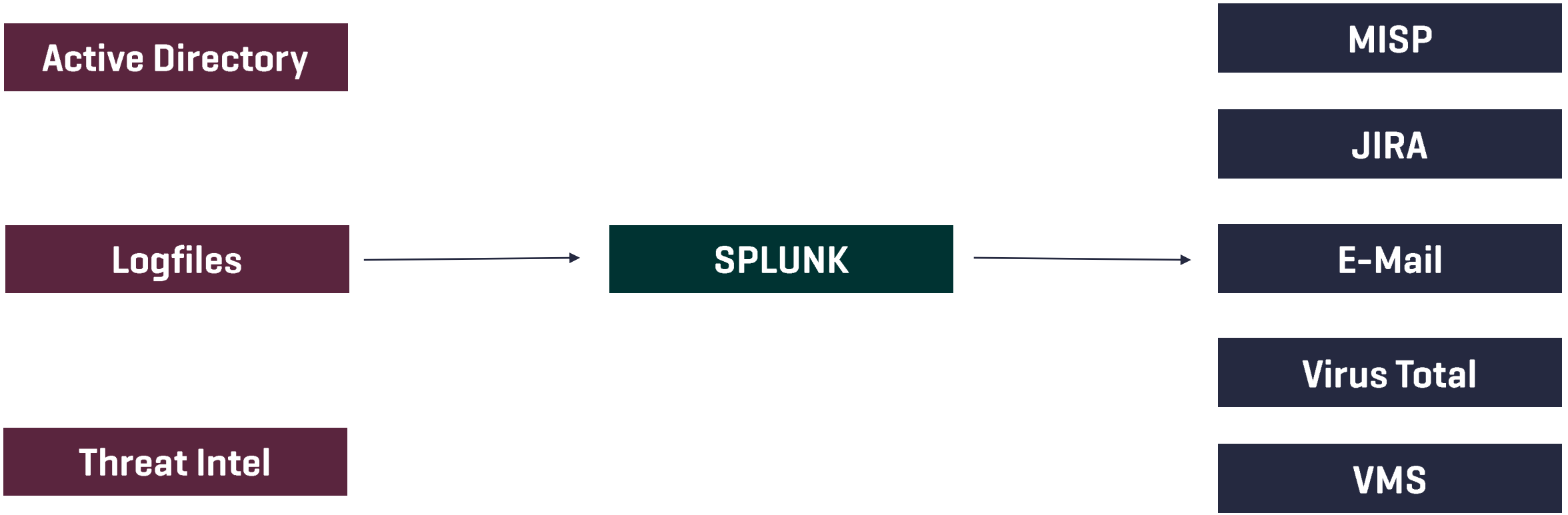


0,5 TB
Physical Memory

114 TB
Indexer Diskspace

10.500
Universal Forwarder

Workflows mit Splunk Enterprise



MUNICH AIRPORT

SPLUNK ES 8.0

MARTIN HABICHT
16.03.2025

Flughafen München

Startschuss für Splunk Enterprise Security

HIER SIND WIR GESTARTET

- SAVED SEARCHES
- CASE MANAGEMENT IN JIRA
- ASSETS & IDENTITÄTEN AUS „EINER“ QUELLE
- KEINE RISIKOBEWERTUNG FÜR ASSETS & IDENTITÄTEN
- KEINE PRIORISIERUNG DER USE CASES
- RUDIMENTÄRE NUTZUNG DER SPLUNK SECURITY ESSENTIALS
- NETZWERK- & BETRIEBSSYSTEMZENTRISCHE ÜBERWACHUNG
- KAUM BUSINESS BETRACHTUNG

HIER WOLLEN WIR HIN

- DETECTION MANAGEMENT
- 90 % CASE MANAGEMENT IN ES
- KONTEXT- & RISIKOTRANSPARENZ DER ASSETS & IDENTITÄTEN
- AKTIVE NUTZUNG DER ESCU-APP
- CIM / DATENMODELLE
- FALSE POSITIVES MINIMIEREN
- RISIKO BASIERTE PRIORISIERUNG
- PRIORISIERUNG NACH BUSINESS VALUE

Workflows mit Splunk Enterprise

IAM

Defender

Active Directory

PAM

Logfiles

EAM

Threat Intel

VMS

ASM

Plattform

TI Framework

Detection Framework

Splunk Enterprise Security

Risk Framework

A&I Framework

Risk Framework

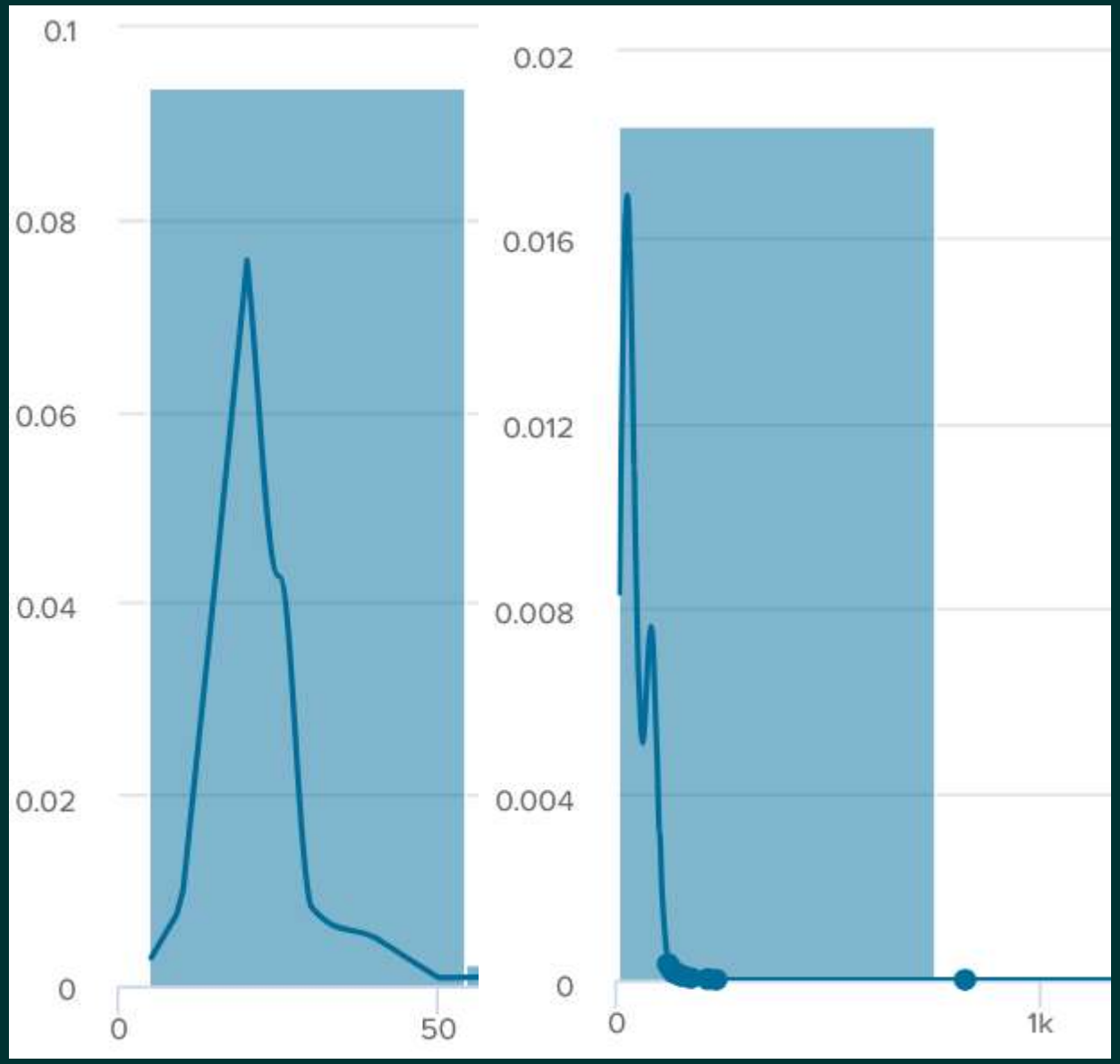
- Unproportionales Wachstum von Detections gegenüber dem Alert Volume
- Attack-Story & Threat Topology
- Realistische Kategorisierung & Priorisierung
- Dynamischer Alarmierungsschwellwert
- Vergabe der RISK- Werte anhand der UC Severity
- Entity Risk Score zur schnellen Klassifizierung

„Keine“ zeitzentrische Alarmierung

Keine Angst vor neuen Detections

Risk Framework & AI Toolkit

```
| EVAL RISK_OBJECT_GROUP = CASE(
MATCH(NORMALIZED_RISK_OBJECT, "^FMG-"), "FMG-SERVER",
MATCH(NORMALIZED_RISK_OBJECT, "^NB"), "FMG-CLIENT",
MATCH(NORMALIZED_RISK_OBJECT, "^PC"), "FMG-CLIENT",
MATCH(RISK_OBJECT_TYPE, "USER"), "USER",
MATCH(RISK_OBJECT, "@"), "USER",
CIDRMATCH(NORMALIZED_RISK_OBJECT, „*.*.*.*/*"), "FMG-IP",
CIDRMATCH(NORMALIZED_RISK_OBJECT, "10.0.0.0/8"), "FMG-
IP",
CIDRMATCH(NORMALIZED_RISK_OBJECT, "192.168.0.0/16"),
"FMG-IP",
MATCH(NORMALIZED_RISK_OBJECT, "\D+\.\D+\.\D+\.\D+"), "IP",
TRUE(), "NOT_CLASSIFIED")
| EVAL "_ATF_HOUR_OF_DAY"=STRFTIME(_TIME, "%H")
| EVAL "_ATF_NUM_DAY_OF_WEEK"=STRFTIME(_TIME, "%W")
| EVAL IS_WORKDAY=IF(_ATF_NUM_DAY_OF_WEEK>0 OR
ATF_NUM_DAY_OF_WEEK<6, 1, 0)
| EVAL IS_WORKTIME=IF((_ATF_HOUR_OF_DAY>6 OR
ATF_HOUR_OF_DAY<19 ) AND (IS_WORKDAY=1), 1, 0)
```



AI Toolkit

8 aktive Machine Learning Detections -> Outlier Detection

- Network
- Authentication
- Process

Reduktion von Alarmrauschen und Fehlalarmen

ML_Apply_Risk Threshold Exceeded For Object Over 24 Hour

- Gruppierung der Risk Scores
- *„Grundrauschen“ -30d@d*

Detection Framework

- Zentrale Oberfläche zur Use Case Dokumentation
- Versionierung mit Rollback
- Strukturiertes Template für neue Detections
- Aktive Unterstützung der Analysten durch Drill-Down`s
- Dokumentierte Abdeckung durch Annotationen
- **Finding Based Detections**

Produktspezifische Detections & Dokumentation

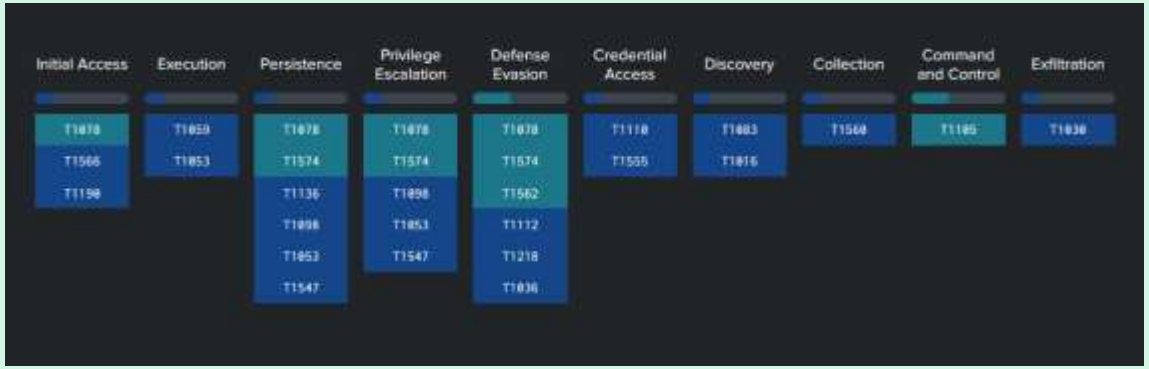
Analytic Story Details: FMG Flightmanagement

- Produktinformationen
- Kontakt-& Betreiberinformationen
- Abdeckungsgrad anhand versch. Frameworks
- Mapping auf notwendige Technologien / Datenqullen
- Detection-Beschreibung

Mitre ATT&CK Coverage

DETECTION COVERAGE

TRIGGERED DETECTION COVERAGE



Asset & Identity Framework

67.000 Identitäten aus 14 Quellen

60.000 Assets aus 30 Quellen

Erweiterung der Assets-Felder um *vpn* und *product*

Kontextualisierung für unsere Analysten

Realistische Kategorisierung & Priorisierung

Enterprise Security, und jetzt ?

BASISWISSEN SPLUNK ENTERPRISE IST UNABDINGBAR FÜR DIE ES APP

LOG-DATENQUALITÄT, SOWIE CIM-COMPLIANCE IST DIE ENTSCHEIDENDE GRUNDLAGE

KEINE NAHTLOSE INTEGRATION EINER VERTEILTEN UMGEBUNG

INVESTIGATION DIENEN AKTUELL EHER ZUM CLUSTERN VON FINDINGS

INTEGRATION MCP GATEWAY, UM ON-PREM LLM NUTZBAR ZU MACHEN

FINDING GROUPS ZUM CLUSTERN GLEICHARTIGER FINDINGS

IMPLEMENTATION SOAR

MUNICH AIRPORT

Vielen Dank!