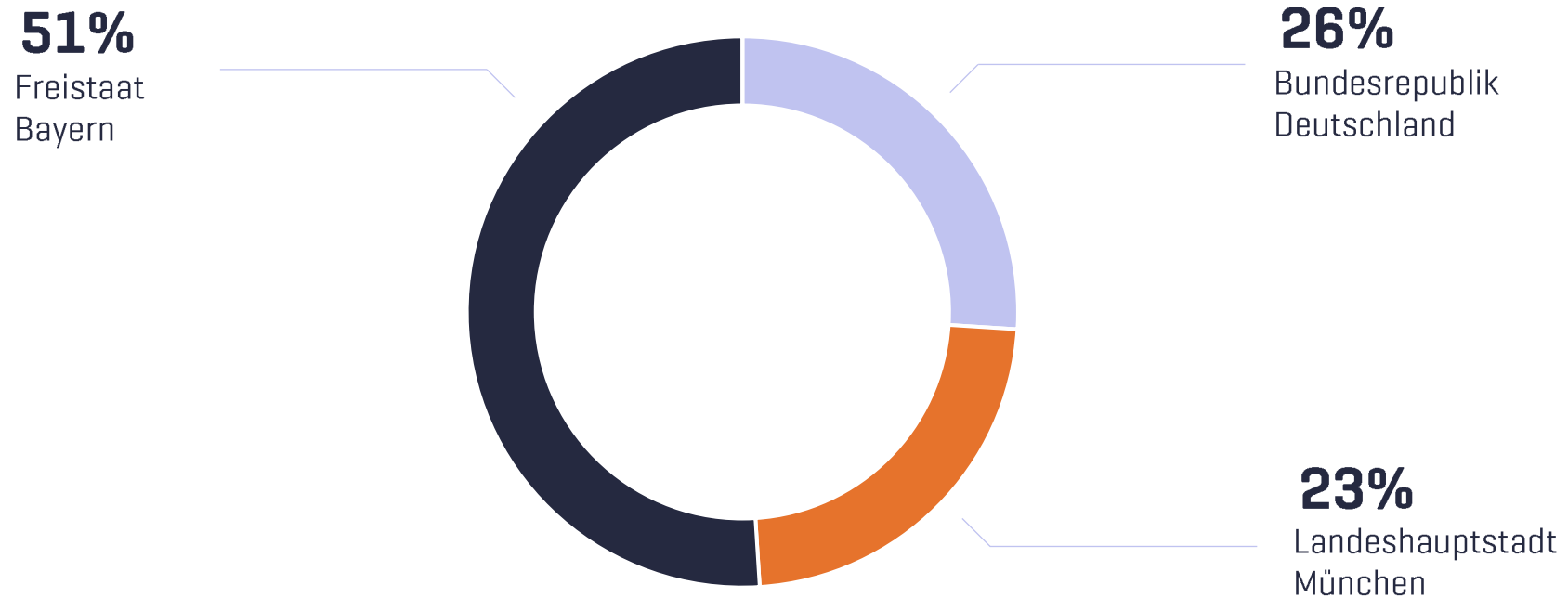


Flughafen München Zahlen, Fakten und Wissenswertes.



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

Bayerns Tor zur Welt. Weltweiter Knotenpunkt

Der Flughafen München ist ein wichtiges internationales Luftverkehrsdrehkreuz.



96*
Fluggesellschaften

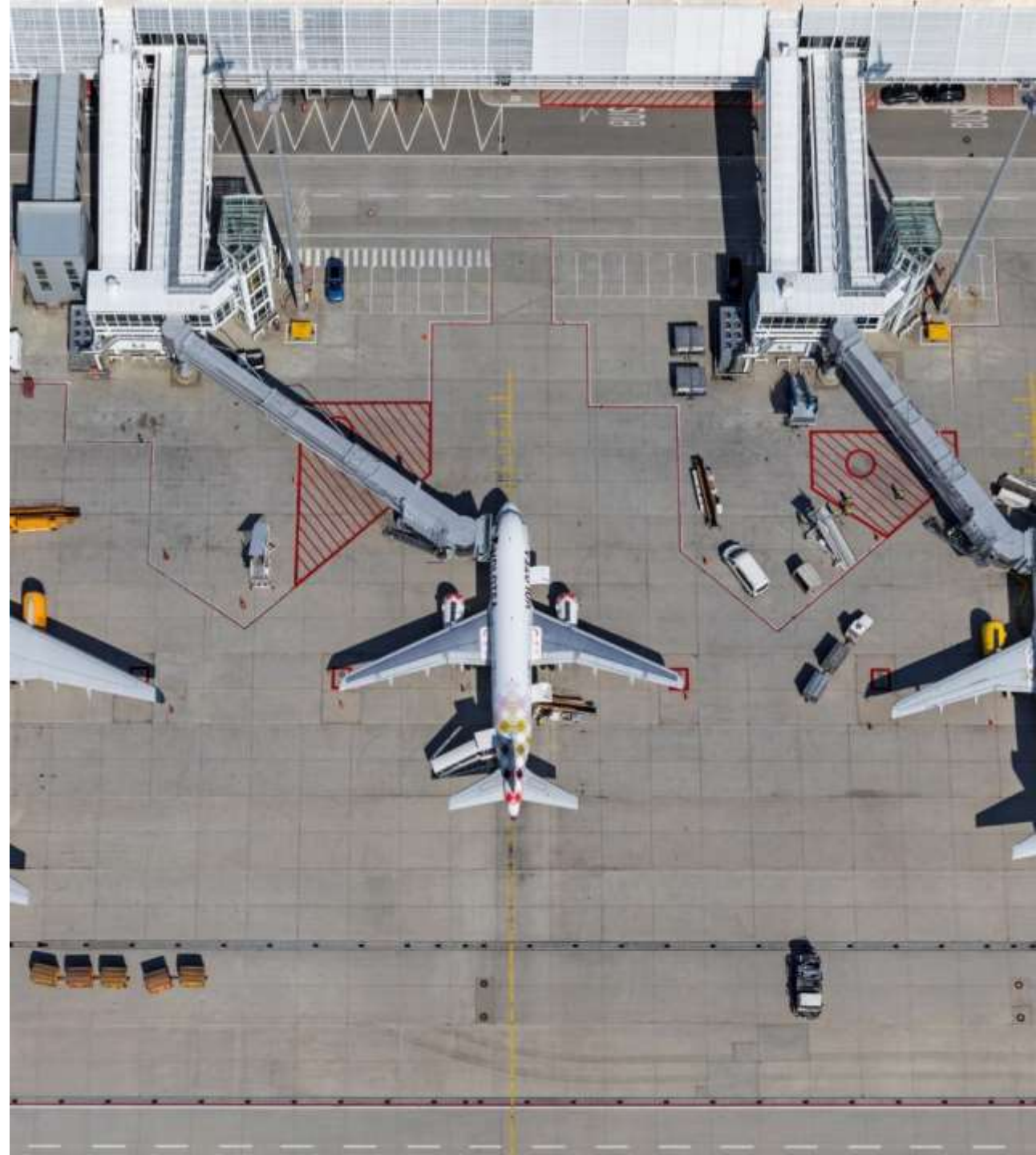


232
Ziele



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%



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

IT am Flughafen München Zahlen, Fakten und Wissenswertes.

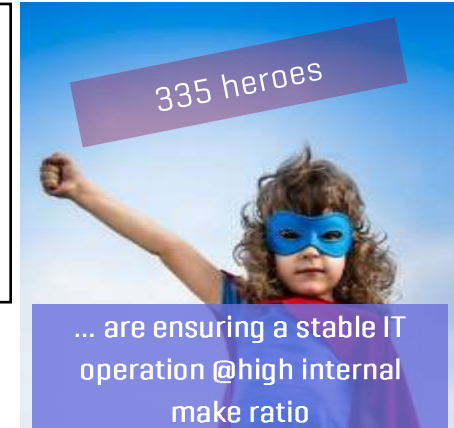


Die IT unseres Flughafens ist Teil der kritischen Infrastruktur, zwingende Voraussetzung für einen stabilen Betrieb und bildet ein sehr breites Lösungsportfolio ab.



We manage numerous digital endpoints, i.e.

5,400 Windows accounts	3100 UDS displays
42,000 LAN connex ports	900+ applications
15,000 different telephone connections	3,400 CCTV cameras & clients
14,500 different endpoints	



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

SPLUNK

Zahlen, Fakten und Wissenswertes.

MARTIN HABICHT
16.03.2025

splunk >

CYBERSECURITY MONITORING

THREAT ACTIVITY



EVENTS BY CATEGORY

 Suspicious Network Traffic Detected

 Brute Force Attack Attempt

 Malware Signature Match

 Unusual User Login Pattern

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

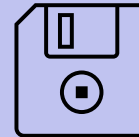
Clustermanager



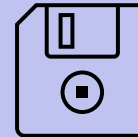
Search Head



Indexer



Indexer



Infrastruktur bis 2024

Clustermanager



Search Head



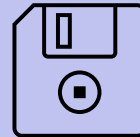
Search Head



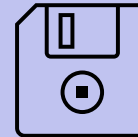
Deploymentsserver



Indexer

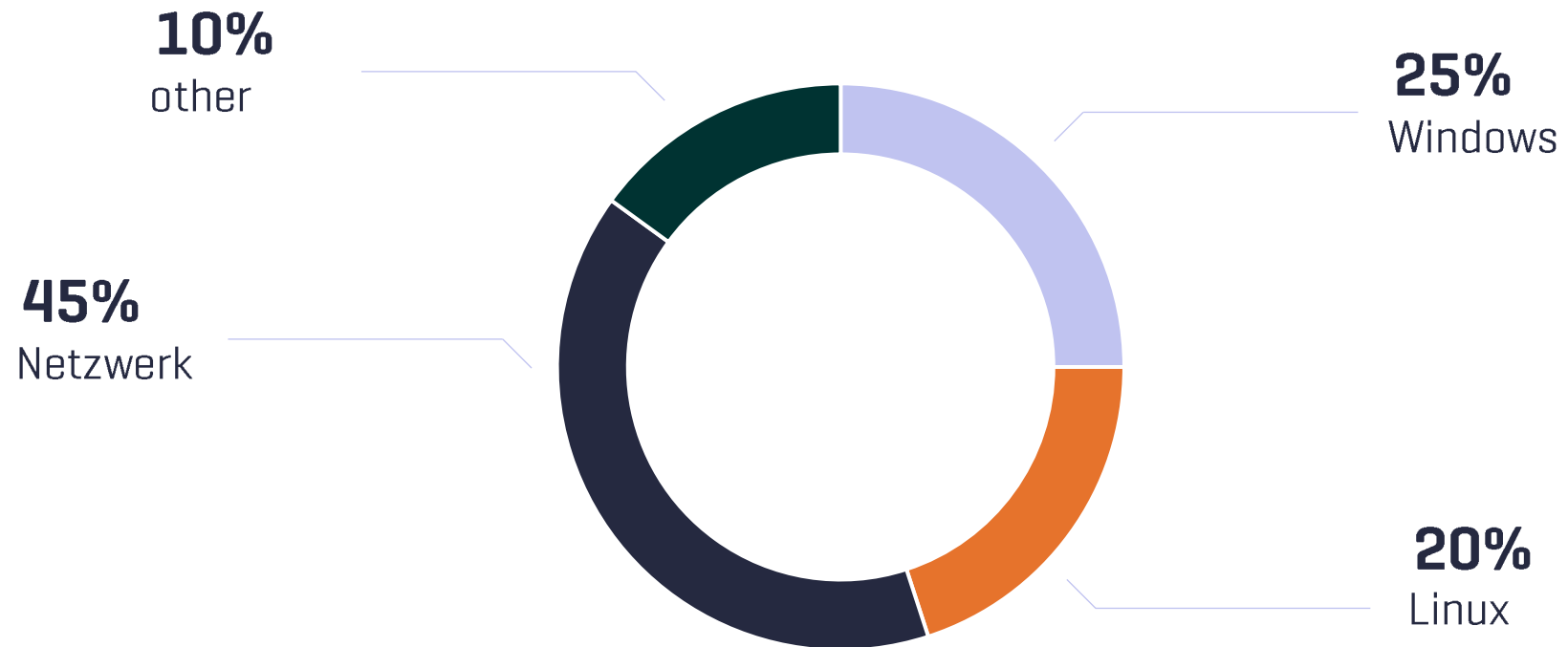


Indexer



650 GB

Logquellen bis 2024



Infrastruktur ab 2025

Clustermanager



Search Head



Search Head



Search Head



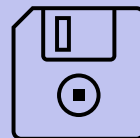
Search Head
[Backup]



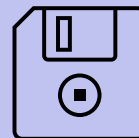
Deploymentserver



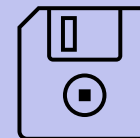
Indexer



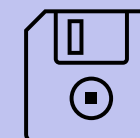
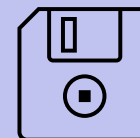
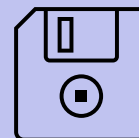
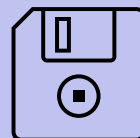
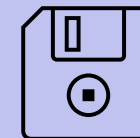
Indexer



Indexer



Indexer



Indexer

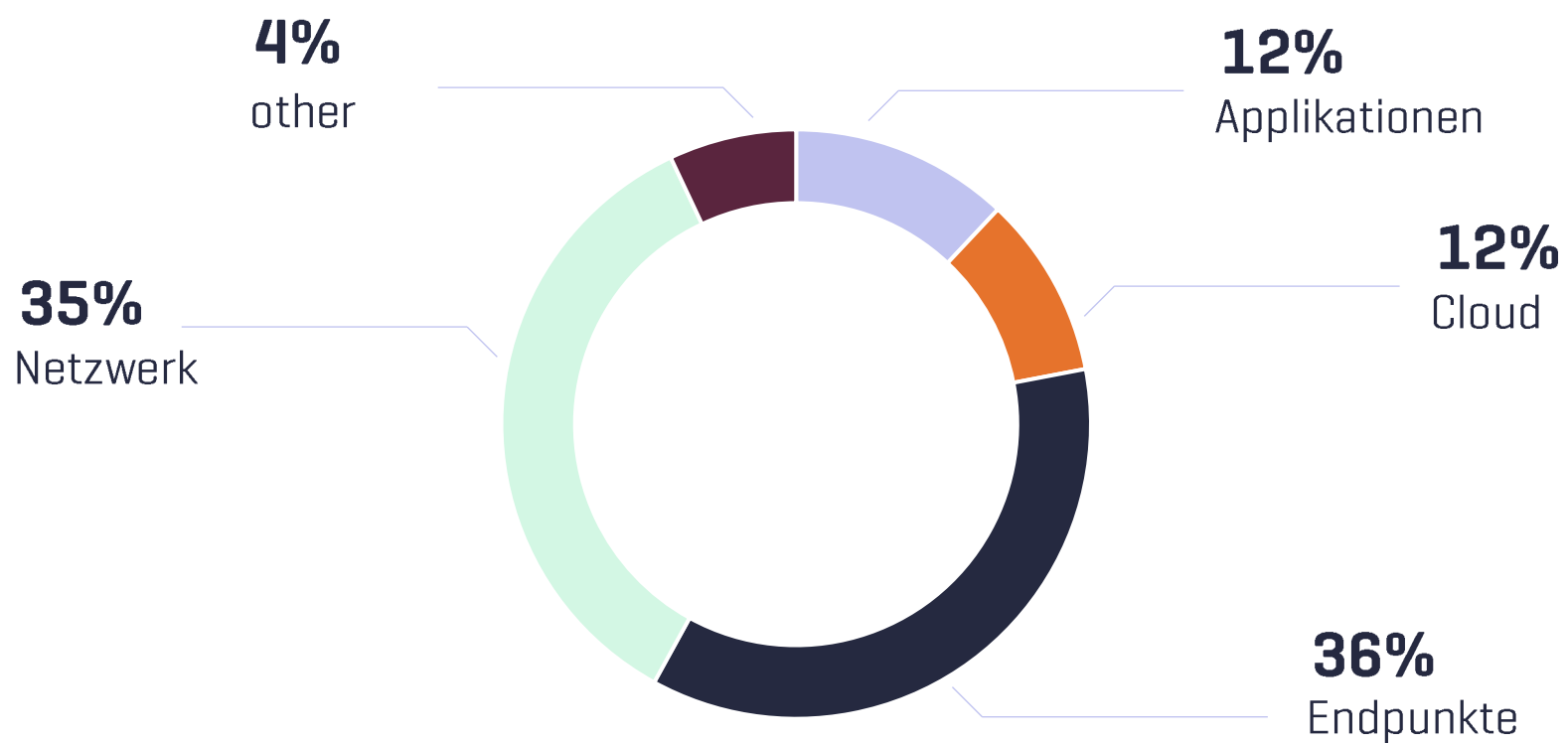
Indexer

Indexer

Indexer

2 TB

Logquellen bis 2026



Infrastruktur ab 2026

Clustermanager



Search Head



Search Head



Search Head



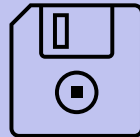
Search Head
[Backup]



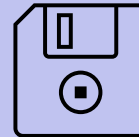
Deploymentsserver



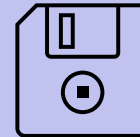
Indexer



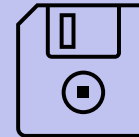
Indexer



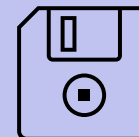
Indexer



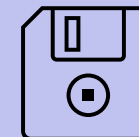
Indexer



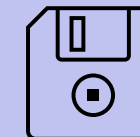
Indexer



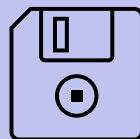
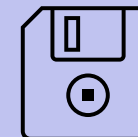
Indexer



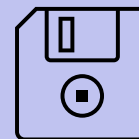
Indexer



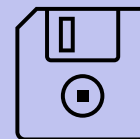
Indexer



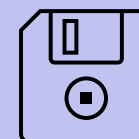
Indexer



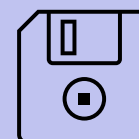
Indexer



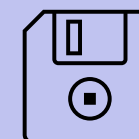
Indexer



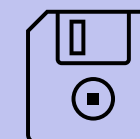
Indexer



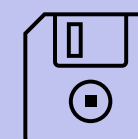
Indexer



Indexer



Indexer

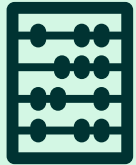


Indexer

Clusterüberblick

1010
1010

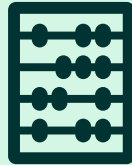
16
Indexer



118 TB
Coldstorage



368 Tage
Datenalter [Median]



24 TB
Hotstorage



215 TB
Indexgröße



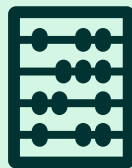
14 TB
pro Indexer

1010
1010

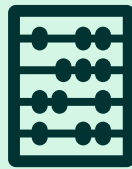
3,5 Billionen
avg. Events per
Day

1010
1010

5,5 Billionen
max. Events per
Day



128 Cores
Indexer CPU



0,5 TB
Physical Memory

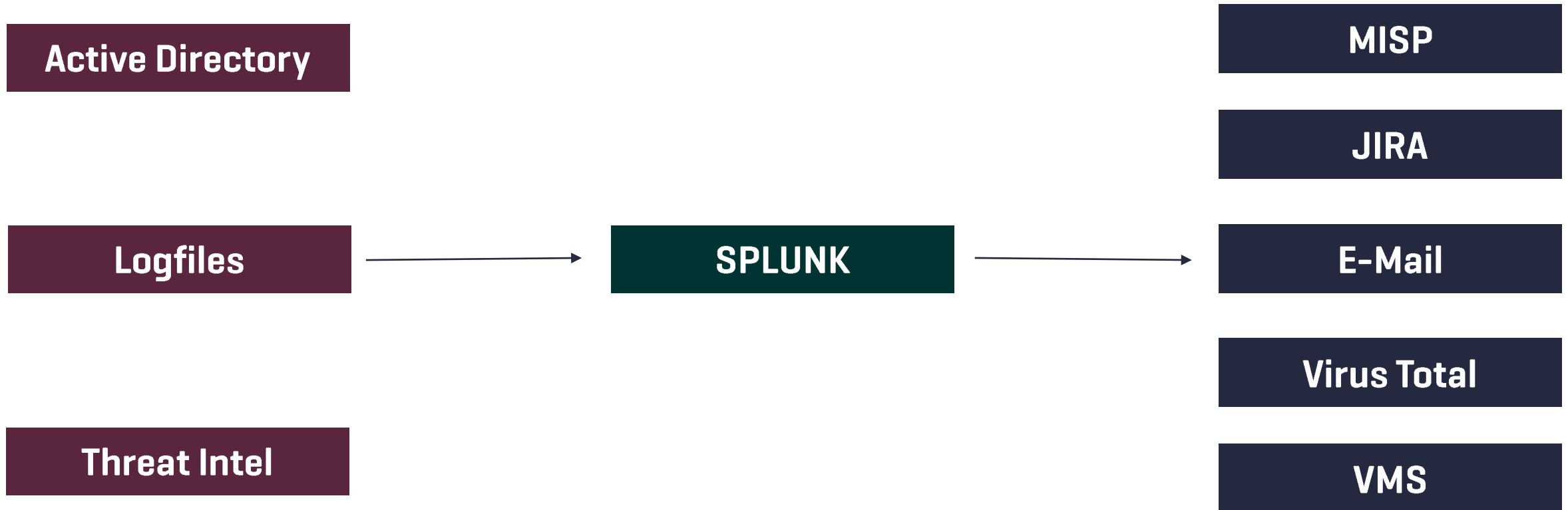


114 TB
Indexer Diskspace



10.500
Universal Forwarder

Workflows mit Splunk Enterprise



SPLUNK ES 8.0

MARTIN HABICHT
16.03.2025



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



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

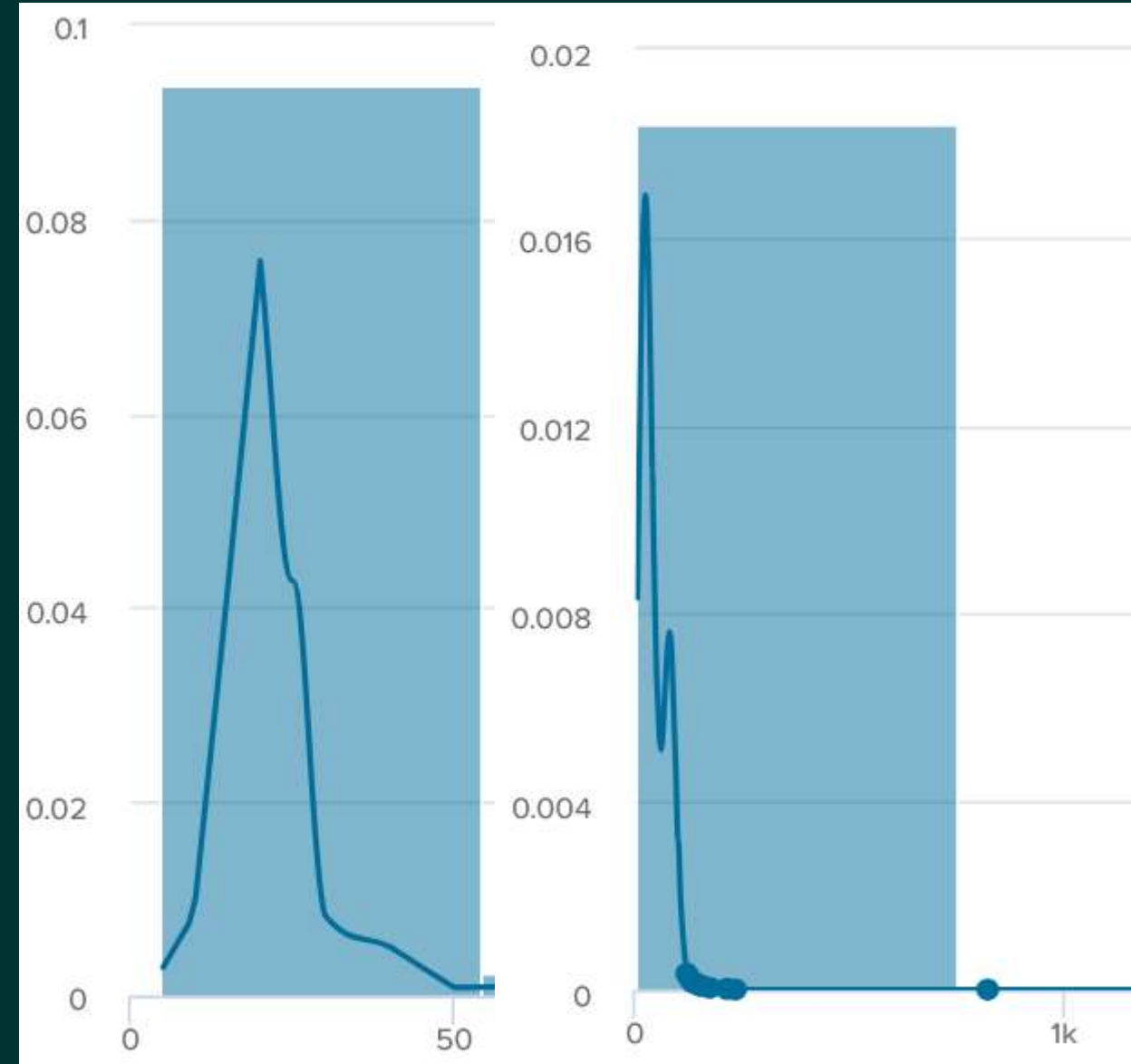
„Keine“ zeitzentrische Alarmierung

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 Fehllarmen

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**

Entity type	Entity	Finding risk score
user	user	20
system	src	20
system	dest	20



splunk>

DETECTION FRAMEWORK

 DATA SOURCE	Network Traffic
 RULE TYPE	Threat Match
 THREAT OBJECT	Malicious Domain

Produktspezifische Detections & Dokumentation

Analytic Story Details: FMG Flightmanagement

Produktinformationen

Kontakt- & Betreiberinformationen

Abdeckungsgrad anhand versch. Frameworks

Mapping auf notwendige Technologien / Datenquellen

Detection-Beschreibung

Created: _____ N/A
Last Modified: _____ 2025-08-21
Version: _____ 1

Kill Chain

Reconnaissance Exploitation Access or Objectives

MITRE ATT&CK

T1116 T1270 T1078 T1008 T1555.002 T1134 T1021 T1550
T1003.001 T1555.001 T1134.005

Technologies

Windows Network Switch

Mitre ATT&CK Coverage

DETECTION COVERAGE

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
T1595	T1586	T1678	T1055	T1098	T1098	T1562	T1118	T1201	T1021	T3560	T1185	T1038	T1499
T1528	T1584	T1190	T1055	T1078	T1078	T1112	T1003	T1087	T1072	T1114	T1071	T1048	T1485
T1597	T1547	T1133	T1047	T1136	T1053	T1078	T1536	T1089	T1218	T1046	T1572	T1041	T1565
T1583	T1585	T1526	T1588	T1053	T1543	T1218	T1558	T1018	T1563	T1825	T1219	T1052	T1458
T1598	T1658	T1189	T1283	T1543	T1484	T1484	T1535	T1049	T1558	T1213	T1071	T1567	T1458
T1591	T1548	T1208	T1072	T1133	T1548	T1548	T1621	T1083	T1578	T1056	T1088	T1537	T1529
T1586	T1608	T1199	T1284	T1538	T1055	T1036	T1648	T1033	T1534	T1039	T1685	T1028	T1488
T1589	T1583	T1659	T1196	T1596	T1134	T1084	T1552	T1046	T1091	T1074	T1132	T1011	T1531
T1594		T1195	T1648	T1546	T1546	T1555	T1181	T1016	T1088	T1125	T1095	T1029	T1057
T1592		T1091	T1051	T1574	T1574	T1078	T1056	T1482		T1185	T1573		T1489
			T1598	T1547	T1547	T1222	T1187	T1057		T1538	T1001		T1496
			T1099	T1053	T1088	T1055	T1212	T1082		T1115	T1184		T1496
			T1618	T1197	T1011	T1127	T1696	T1124		T1119	T1182		T1491
			T1129	T1554	T1037	T1134	T1528	T1622		T1123	T1568		T1561
				T1542		T1027	T1048	T1538		T1682	T1088		
				T1525		T1574	T1539	T1518		T1557	T1092		
				T1285		T1681	T1537	T1526		T1113	T1285		
				T1176		T1558		T1014			T1659		
				T1137		T1148		T1012					
				T1037		T1282		T1054					
						T1578		T1019					
						T1211		T1487					

TRIGGERED DETECTION COVERAGE

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Collection	Command and Control	Exfiltration
T1078	T1059	T1078	T1078	T1078	T1118	T1083	T1568	T1185	T1038
T1565	T1053	T1574	T1574	T1574	T1535	T1015			
T1198		T1136	T1098	T1562					
		T1098	T1051	T1112					
		T1053	T1547	T1218					
		T1547		T1036					

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



splunk >

ASSET & IDENTITY MANAGEMENT

ASSETS

- Workstation
- Aircraft

IDENTITY

- John Smith
- Pilot

THREAT ACTIVITY

HOST EVENTS

WAS LIEF GUT UND WIE GEHT'S WEITER

Enterprise Security, und jetzt ?

BASISWISSEN SPLUNK ENTERPRISE IST UNABDINGBAR FÜR DIE ES APP

LOG-DATENQUALITÄT, SOWIE CIM-COMPLIANCE IST DIE ENTSCHIEDENDE 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

**Vielen
Dank!**

