
CONSULTING
PAIRING
HUMANS
AND
TECHNOLOGY

PHAT CONSULTING
HAMBURG, 2025

MCI ENGAGEMENT DATA SECURITY

AGENDA

1. **BESCHREIBUNG DES ENGAGEMENTS**
2. **ZIELE DES ENGAGEMENTS**
3. **ABLAUF/DURCHFÜHRUNG DES ENGAGEMENTS**
4. **OUTCOMES**
5. **OUT OF SCOPE**

ENGLISH VERSION BELOW

BESCHREIBUNG DES ENGAGEMENTS

Das Data Security Engagement kann Kunden begeistern, Microsoft Purview-Lösungen einzusetzen und zu nutzen. Durch die Bereitstellung realer, datenbasierter Beispiele für Datensicherheit und regulatorische Risiken in ihren eigenen Umgebungen, kombiniert mit gemeinsamen Workshops, unterstützt das Engagement dabei, überzeugende Möglichkeiten für Kunden zu entwickeln, Datensicherheitsrisiken mithilfe von Microsoft Purview-Technologien (E5 Compliance) zu beheben und zu verhindern.

ZIELE DES ENGAGEMENTS

Grundlegendes zu vertraulichen Datenbeständen

Verschaffen Sie sich einen Überblick über vertrauliche und veraltete Daten in Ihrer Microsoft 365 Cloud- und On-Premises-Umgebung, um Informationsrisiken zu identifizieren, Datenklassifizierungen zu verbessern und gesetzliche Anforderungen besser zu erfüllen.

I

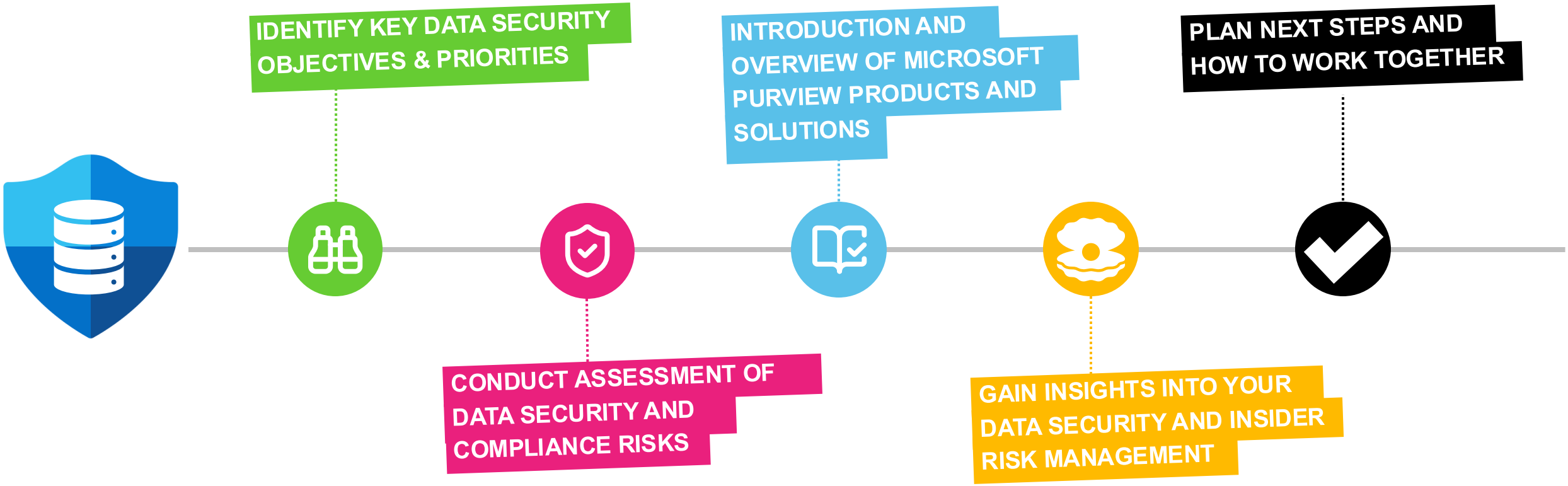
dentifizieren Sie Datenverluste und Insider-Bedrohungsrisiken

Identifizieren Sie potenzielle Risiken wie Datenlecks, fehlerhafte Freigaben, versehentlichen Datenverlust oder verdächtiges Benutzerverhalten. Ziel ist es, gefährdete Informationen und unsichere Prozesse sichtbar zu machen und gezielt zu sichern.

Definieren Sie die nächsten Schritte für die Absicherung

Im Rahmen des Engagements erarbeiten wir gemeinsam einen priorisierten Maßnahmenkatalog. Diese basiert auf den Ergebnissen der Datenanalyse und zeigt, wie Microsoft Purview – insbesondere Data Loss Prevention, Informationsschutz und Insider-Risikomanagement – gezielt eingesetzt werden kann, um Risiken zu reduzieren.

WHAT YOU'LL ACHIEVE DATA SECURITY MCI ENGAGEMENT



WAS BEKOMMEN SIE MIT DEM DATA SECURITY ENGAGEMENT?

+

- Besseres Verstehen, Klassifizieren und Kontrollieren sensibler und veralteter Daten in Microsoft 365.
- Verschaffen Sie sich einen Überblick über die Risiken von Datenlecks, Insider-Bedrohungen und nicht konformem Umgang mit Informationen.
- Erhalten Sie klare Empfehlungen zum Implementieren von Microsoft Purview-Lösungen für Data Loss Prevention, Information Protection und Insider-Risikomanagement.
- Sie verfügen über eine Roadmap mit priorisierten Maßnahmen, die auf ihre Compliance-Ziele und ihre Datenschutzstrategie zugeschnitten sind.

OUTCOMES

Data Discovery Findings

Erkenntnisse aus der Ermittlung veralteter, vertraulicher oder offengelegter Daten in Microsoft 365 Diensten. Enthält Speicherorte, Zugriffskontrollen, Klassifizierungslücken und Anomalien im Datenlebenszyklus.

Data Risk Exploration Results

Beobachtungen zu Datenverlustrisiken, zu viel freigegebenen Dateien, nicht autorisiertem Zugriff und Insider-Verhaltensmustern basierend auf Telemetrie und Microsoft Purview-Analysen.

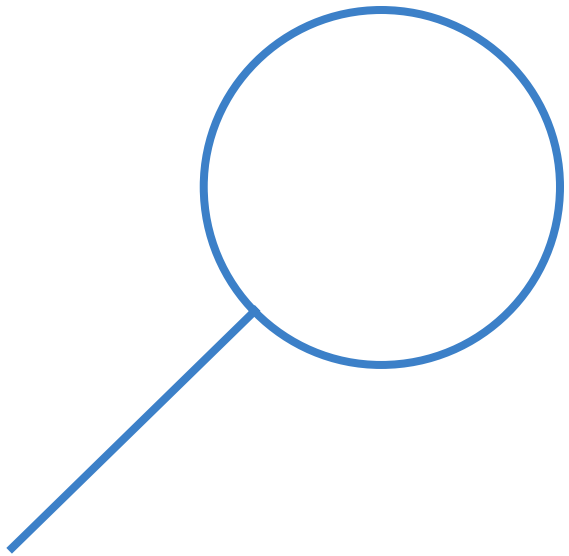
Mitigation Recommendations

Leitfaden zur Verwendung von Microsoft Purview-Funktionen (z. B. DLP, Information Protection, Vertraulichkeitsbezeichnungen), um identifizierte Risiken zu minimieren und richtlinienbasierten Schutz durchzusetzen.

Insider Risk Insights

Erste Indikatoren für Insider-Bedrohungen oder -Missbrauch basierend auf Verhaltensanalysen, Dateiverschiebungsmustern und Regelauslösern, die während des Engagements beobachtet wurden.

OUT OF SCOPE



- Konfiguration von Microsoft Purview-Features über illustrative Anleitungen hinaus Tiefgreifende forensische Analyse oder eDiscovery von spezifischen Datenvorfällen
- Bewertungen der Einhaltung gesetzlicher Vorschriften (z. B. DSGVO-Audits)
- Sanierung von Altdatenstrukturen oder Datenmigration
- Entwicklung einer benutzerdefinierten Klassifizierungs- oder Kennzeichnungstaxonomie
- Bereitstellung produktionsbereiter Richtlinien (außerhalb des Demoumfangs)

WIR FREUEN UNS AUF EUCH
LET‘S GO!

Arno von Lengerke

Martin Goldberger

PHAT CONSULTING

Holger Gerling

Una Nagel

PHAT CONSULTING GMBH
Nobistor 10 | 22767 Hamburg
040 226 383 - 100
info@phatconsulting.de

PHAT CONSULTING
HAMBURG, 2025

MCI ENGAGEMENT DATA SECURITY

AGENDA

1. **DESCRIPTION OF THE ENGAGEMENT**
2. **GOALS OF THE ENGAGEMENT**
3. **PROCESS/IMPLEMENTATION OF THE ENGAGEMENT**
4. **OUTCOMES**
5. **OUT OF SCOPE**

DESCRIPTION OF ENGAGEMENTS

The Data Security Engagement is designed to create customer intent for deploying and adopting Microsoft Purview solutions. By providing real data driven examples of data security and regulatory risks in their own environments combined with collaborative workshop sessions, the engagement helps partners create compelling ways for customers to remediate and prevent data security risks using Microsoft Purview (E5 Compliance) technologies.

GOALS OF ENGAGEMENT

Understanding sensitive data assets

Gain visibility into sensitive and outdated data across your Microsoft 365 cloud and on-premises environment to identify information risks, improve data classifications, and better meet regulatory requirements.

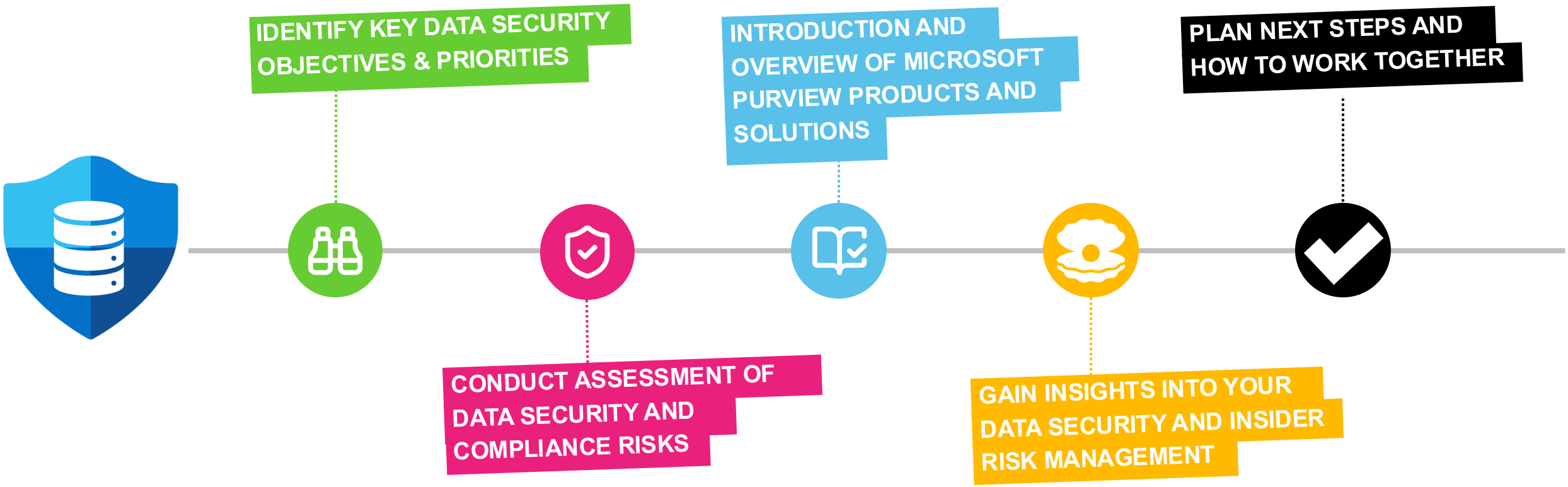
Identify data loss and insider threat risks

Identify potential risks such as data leakage, erroneous shares, accidental data loss, or suspicious user behavior. The aim is to make endangered information and insecure processes visible and to secure them in a targeted manner.

Define next steps for hedging

As part of the commitment, we work together to develop a prioritized list of measures. This is based on the results of the data analysis and shows how Microsoft Purview – in particular data loss prevention, information protection and insider risk management – can be used in a targeted manner to reduce risk.

WHAT YOU'LL ACHIEVE DATA SECURITY MCI ENGAGEMENT



AFTER THE DATA SECURITY ENGAGEMENT, YOU WILL …

- Better understand, classify, and control sensitive and stale data across Microsoft 365.
- Gain visibility into risks of data leakage, insider threats, and non-compliant information handling.
- Receive clear recommendations on how to implement Microsoft Purview solutions for Data Loss Prevention, Information Protection, and Insider Risk Management.
- Have a roadmap of prioritized actions tailored to their compliance goals and data protection strategy.

OUTCOMES

Data Discovery Findings

Insights from the discovery of stale, sensitive, or exposed data across Microsoft 365 services. Includes storage locations, access controls, classification gaps, and data lifecycle anomalies.

Data Risk Exploration Results

Observations on data loss risks, overshared files, unauthorized access, and insider behavior patterns based on telemetry and Microsoft Purview analytics.

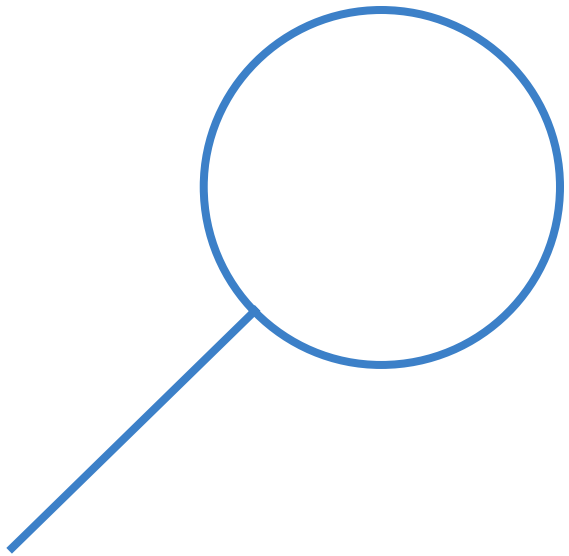
Mitigation Recommendations

Guidance on using Microsoft Purview capabilities (e.g., DLP, Information Protection, Sensitivity Labels) to mitigate identified risks and enforce policy-based protection.

Insider Risk Insights

Initial indicators of insider threats or misuse based on behavior analytics, file movement patterns, and rule triggers observed during the engagement.

OUT OF SCOPE



- Configuration of Microsoft Purview features beyond illustrative guidance
  Deep forensic analysis or eDiscovery of specific data incidents
- Legal compliance assessments (e.g., GDPR audits)
- Remediation of legacy data structures or data migration
- Custom classification or labelling taxonomy development
- Deployment of production-ready policies (outside demo scope)

WE LOOK FORWARD TO SEEING YOU
LET'S GO!

Arno von Lengerke

Martin Goldberger

Holger Gerling

Una Nagel

PHAT CONSULTING GMBH
Nobistor 10 | 22767 Hamburg
040 226 383 - 100
info@phatconsulting.de