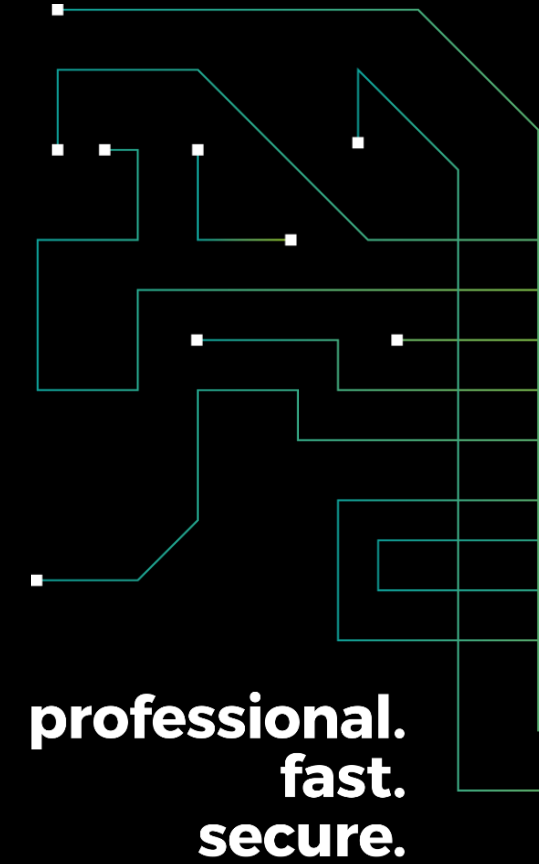


base it

BETTER TOGETHER

Managed Service Security & Purview



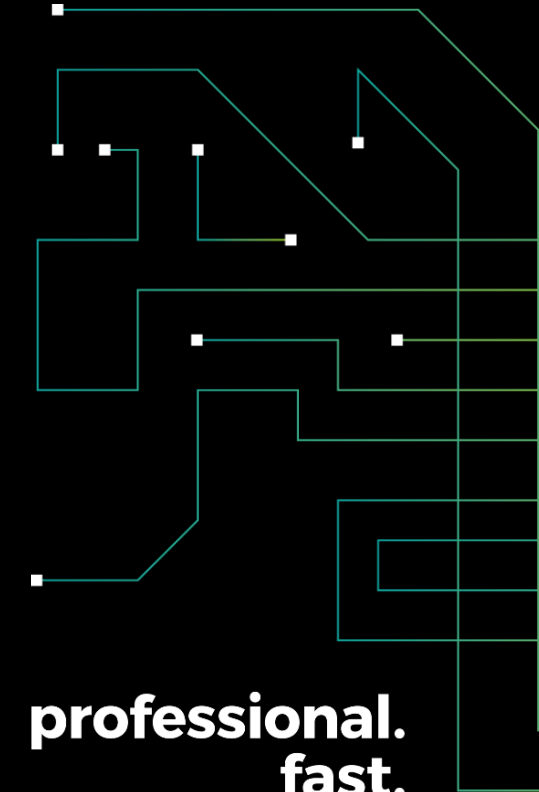
Stefan Nagy

Teamleitung
Communication,
Collaboration & Automation



Thomas Graser

Teamleitung
Modern Workplace & Security



professional.
fast.
secure.

WARUM CYBERSECURITY?

“

**WÄRE *CYBERKRIMINALITÄT* EINE
VOLKSWIRTSCHAFT, WÜRDEN SIE NACH DEN USA UND
CHINA DIE *DRITTGRÖSSTE DER WELT* DARSTELLEN.
DIE ENORMEN WIRTSCHAFTLICHEN SCHÄDEN UND
VERLUSTE, DIE DURCH CYBERANGRIFFE ENTSTEHEN,
VERDEUTLICHEN DIE *DRINGLICHKEIT VON*
*WIRKSAMEN SCHUTZMASSNAHMEN.***

”

DIE 4 HÄUFIGSTEN SECURITY-RISIKEN

SETZEN SIE GEZIELTE GEGENMASSNAHMEN

Phishing und Social Engineering

1

Angreifer nutzen täuschend echte E-Mails oder Nachrichten, um Mitarbeiter dazu zu bringen, vertrauliche Informationen preiszugeben.

Schadsoftware, die Systeme infiziert und Daten verschlüsselt, um Lösegeld zu fordern.

2

Ransomware und Malware

Datenlecks

3

Unbefugter Zugriff auf sensible Daten, oft verursacht durch unzureichende Sicherheitsmaßnahmen oder menschliches Versagen.

Mitarbeiter sind oft das schwächste Glied in der Sicherheitskette, insb. wenn sie nicht ausreichend geschult sind.

4

Mangelndes Bewusstsein



3 ZUKÜNFTIGE SECURITY-RISIKEN

SEIEN SIE VORBEREITET

Künstliche Intelligenz (KI) in Cyberangriffen

1

Angreifer werden zunehmend Künstliche Intelligenz einsetzen, um Schwachstellen zu identifizieren sowie hochentwickelte, schwer erkennbare Angriffe durchzuführen und diese in Echtzeit anzupassen.

Deepfake-Technologie wird immer realistischer und kann verwendet werden, um gefälschte Videos oder Audios zu erstellen, die Personen oder Organisationen schaden.

2

Deepfake-Angriffe

Angriffe auf Lieferketten

3

Cyberkriminelle zielen zunehmend auf die Lieferketten von Unternehmen ab, um Schwachstellen auszunutzen und weitreichende Schäden zu verursachen.



base it

**UNSERE 24X7
SECURITY SERVICES**

24X7 MANAGED SERVICE SECURITY

3 SÄULEN FÜR OPTIMALEN SCHUTZ



**PROACTIVE
SECURITY**



**REACTIVE
SECURITY**



**FORENSIC
ANALYSIS**



24X7 MANAGED SERVICE SECURITY

PROACTIVE SECURITY TECHNOLOGIEN



**PROACTIVE
SECURITY**



MS Entra ID P2



MS Sentinel



MS Defender for Endpoint P2
MS Defender Antivirus
MS Defender for Office 365
MS Defender for Identity
MS Defender for Cloud Apps
MS Defender for Cloud



Security Copilot



24X7 MANAGED SERVICE SECURITY

REACTIVE SECURITY TASKS



**Disaster Recovery
Pläne**



**Incident Response
Team (operativ)**



**24x7 Security
Operation Center**



**REACTIVE
SECURITY**



24X7 MANAGED SERVICE SECURITY

FORENSIC ANALYSIS TASKS



**FORENSIC
ANALYSIS**



**Incident Response
Team (Analyse)**



**Meldung an
Behörden**



**Teil des
Verhandlungsteams**



**Aufbereitung &
Reporting**



**Kommunikation mit
Cyberversicherung**



24X7 MANAGED SERVICE SECURITY

PROACTIVE SECURITY – ENTWICKLUNG BIS HEUTE

Security Innovation
Workshops +

Security Awareness
Trainings +

Schnittstelle zu
Managed Service
Purview +

3rd-Party Patching +

Secure Score
Metering &
Optimization +

Vulnerability Scans
Defender, Pingcastle,
Nessus, Burp, ... +

Phishing Simulation +

Penetration Tests
Red + Blue =
Purple Teaming +

Purple Teaming
Recommendations +



**PROACTIVE
SECURITY**



24X7 MANAGED SERVICE SECURITY

REACTIVE SECURITY EVOLUTION - ENTWICKLUNG BIS HEUTE



**Darknet & Breach
Monitoring** +

**Incident Detection
SIEM Solutions** +
Playbook

**Reaktionskatalog
Weiterentwicklung** +

**Agenten für
Security Copilot** +



24X7 MANAGED SERVICE SECURITY

FUTURE SERVICES

AI Pentesting



**CISO as
a Service**



**Data Leakage
Monitoring**



**Typosquatting
Monitoring**



MANAGED SERVICE SECURITY

PURPLE TEAMING – UNSERE EXPERT*INNEN

Technische Expertise mit einem erfolgreichen Trackrecord:

- Zertifiziert durch mehrtägige Prüfungen: OSCP, OSWA, CPTS, CBBH, und mehr
- CTF-Erfolge: mehrfache Finalisten der Austrian & European Cyber Security Challenge, Vizeweltmeister HackTheBox 2024, Platz 1 Österreich HackTheBox 2024, Gewinner des Stealth Cup des Austrian Institute of Technology 2025, ...
- Engagement in der Incident Response und forensischen Analyse
- Research von aktuellen Threat-Actors und Threat Intelligence



MANAGED SERVICE SECURITY

PURPLE TEAMING VORTEILE

- Tiefgehende Analysen und manuelle, individuelle Tests.
- Simuliert reale Angriffspfade und deren Auswirkungen.
- Verständnis der Zusammenhänge zwischen verschiedenen Schwachstellen sowie Abwehrmaßnahmen.
- Identifiziert und behebt unbekannte, ausnutzbare Schwachstellen.
- Bewertet Schwachstellen nach Gefahr und Schaden, um die Ressourcen für Gegenmaßnahmen effektiv einzusetzen zu können.
 - Informationale, Low, Medium, High, Critical



MANAGED SERVICE SECURITY

PURPLE TEAMING – STANDARD-PAKETE

Entra Threat Simulation

- Analyse der Angriffsoberfläche
- Baseline-Checks zu Identity & Access
- Prüfung von Rollen, Berechtigungen & Policies
- Manuelle Analyse kritischer Konfigurationen & Rollen
- Proof-of-Concept-Angriffe auf gefundene Lücken
- Reporting zur Behebung

Azure Threat Simulation

- Analyse der Angriffsoberfläche
- Baseline-Checks nach CIS & MS-Benchmarks
- Erkennung kritischer Konfigurationen & Rollen
- Simulation realistischer Angriffspfade
- Reporting zur Behebung

Active Directory Threat Simulation

- Analyse der Angriffsoberfläche
- Enumeration von Trusts, Rechten, Strukturen, ...
- Schwachstellen-Überprüfung wie Kerberoasting, ACL-Missbrauch, Pass-the-Hash
- Simulation typischer Angriffstechniken
- Reporting zur Behebung



MANAGED SERVICE SECURITY

PURPLE TEAMING – ADD-ONS: APPLICATION SERVICE PACKAGES

AD Security Pingcastle Analyse

*Analyse der
Angriffs-
Oberfläche,
Trusts &
Rechte.*

Vulnerability Assesment

*Intern:
Scans, Host-
Analyse &
Leak-Suche.*

*Extern:
Schwachstellen
- & Web-Scans,
manuelle Tests.*

Client/Server Hardening Review

*Prüfung von
Konfiguration &
Privilege
Escalation.*

SQL Server Review

*Analyse von
Konfiguration &
Authentifizierung.*

Application Review

*Code- &
Security-
Checks nach
Standards &
Injection.*



WARUM PURVIEW?

DIE 4 HÄUFIGSTEN DATA SECURITY-RISIKEN & MAßNAHMEN

Wissen des Unternehmens schützen

1

Schützenswerte Daten identifizieren - Schutzmaßnahmen aktivieren.

Compliance ist kein „Set and Forget“ sondern ein laufender Prozess.

2

Maßnahmen und Nachhaltigkeit

Datenlecks

3

Unbefugter Zugriff auf sensible Daten, oft verursacht durch unzureichende Sicherheitsmaßnahmen oder menschliches Versagen.

Alerts und Reports unterstützen die Administratoren im täglichen Betrieb.

4

Reporting und Alerting



“

**MIT DEM BASE-IT *MANAGED*
SERVICE PURVIEW SETZEN WIR
NEUE AKZENTE IM BEREICH
COMPLIANCE UND AGIEREN
NACHHALTIG.**

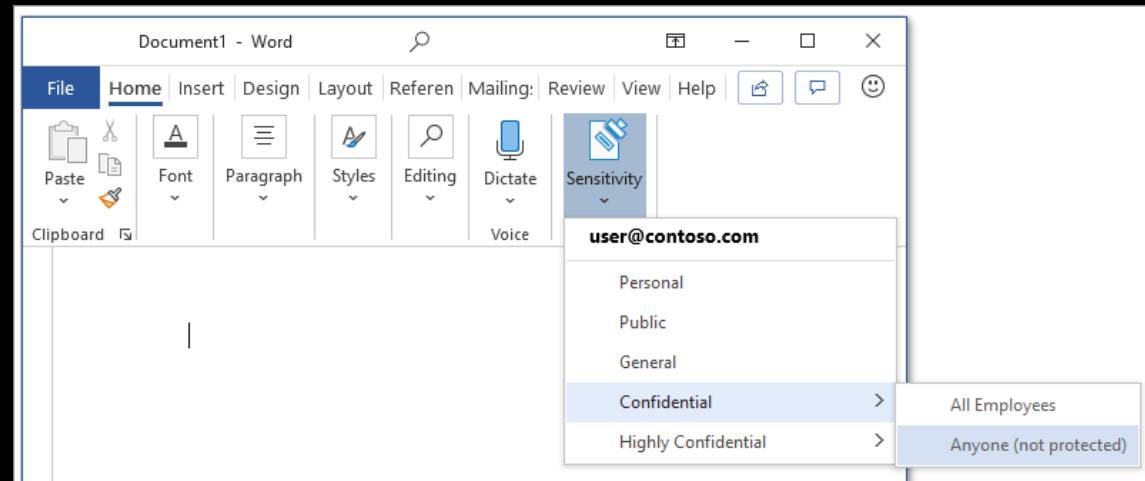
”

base it

INFORMATION PROTECTION

INFORMATION PROTECTION LABELING

- Optische Markierung des „Labels“ auf den Dokumenten
 - Footer
 - Header
 - Watermark



INFORMATION PROTECTION

VERSCHLÜSSELUNG

- Schutz und Markierung des Labels
 - **Verschlüsselung** und **Rechtevergabe** auf bestimmte Benutzer (Intern oder Extern)
 - Nicht kopieren, weiterleiten, ausdrucken...
- Verschlüsselung am Dokument **unabhängig des Speicherorts**
 - E-Mails
 - Teams / SharePoint / OneDrive – Daten
 - SharePoint Seiten
 - File Share/Cloud Storage
 - USB-Stick
 - Teams Meeting



SENSITIVE INFO TYPES

SENSITIVE INFO TYPES

VORSCHLÄGE AUF BASIS INHALT

- Inhaltserkennung auf Basis **vordefinierter** „Info Types“
 - IBAN
 - Kreditkarte
 - Reisepass
 - Sozialversicherungsnummer
 - Gesundheitsdaten
 - IP-Adressen
 - User login Credentials
- Inhaltserkennung auf **customer** created „Info Types“
 - Regular Expressions (RegEx)
 - Keyword List
 - Keyword Dictionary
 - Functions

Define patterns for this sensitive info type

Sensitive info types are defined by one or more patterns. Each pattern must contain a primary element and confidence level, but you can also include supporting elements and additional checks to further refine the evaluation and detection of matching items. [Learn about defining patterns](#)

Select to create an additional pattern

Name	Confidence level	Copy	Edit	Delete
▼ Pattern #1	High	<input type="button" value="Copy"/>	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>



Word

Search

POLICY TIP Your organization recommends that you apply the sensitivity: Highly Confidential Label - Internal Only

- What features of a package drive emotional response?
- What package elements elicit strong, positive emotional responses?
- What package elements elicit strong, negative emotional responses?

Earnings Distribution

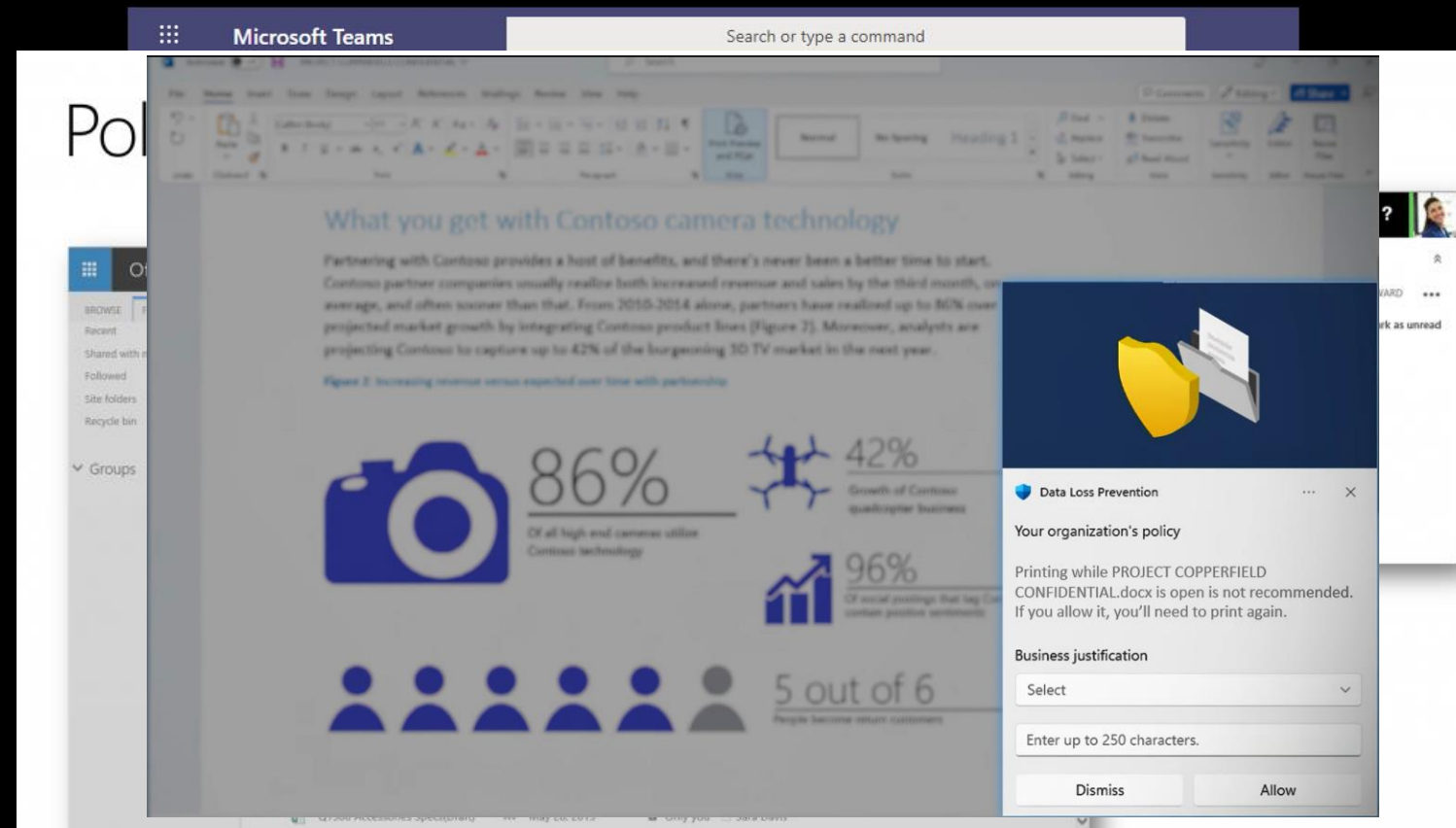
CONFIDENTIAL

DATA LOSS PREVENTION

DATA LOSS PREVENTION

DIREKTER SCHUTZ

- Maßnahme gegen **Verlust** von **sensiblen Daten**
 - Integration in Microsoft 365 Applikationen:
 1. Exchange Online & Outlook
 2. Microsoft Teams
 3. SharePoint / OneDrive
 4. Client Endpoint



“

**MIT *DLP* HABEN WIR EINEN
GAMECHANGER: DLP ÜBERWACHT
KONTINUIERLICH UND ERGREIFT
SOFORTIGE MAßNAHMEN BEI
DATENVERLUST.**

”

DATA LOSS PREVENTION

STAGED ROLLOUT

- Phase 1 – **Reporting Only**:
 - Erstellung der DLP Policies für M365 auf Basis Information Protection Labels oder Sensitive Info Types
 - Analyse der Reports und Alerts (Ohne Eingriff bei Endbenutzern)
- Phase 2 – **Enduser Notification**:
 - Notifizierung der Endbenutzer
 - Analyse der Reports und Alerts
- Phase 3 – **Restrictions**:
 - Einschränkung bei Datenverlust
 - Notifizierung der Endbenutzer
 - Generierung Alerts
 - Analyse der Reports und Alerts

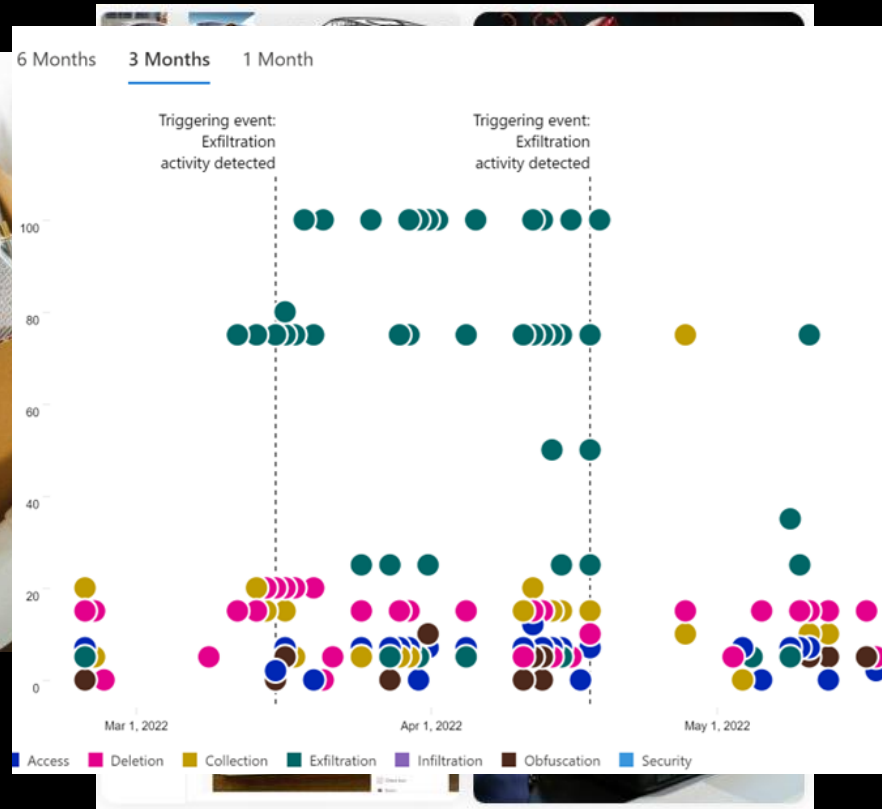


INSIDER RISK MANAGEMENT

INSIDER RISK MANAGEMENT

SIGNALERKENNUNG AUF BASIS KI

- Schutz vor Datendiebstahl von internen Benutzer*innen
- Basis: Erkennung von Anomalien im „Daily Work“
 - Beispiel: Offboarding



INSIDER RISK MANAGEMENT

SIGNALERKENNUNG AUF BASIS KI

- Phase 1 – **Activation & Policy Creation**:
 - Aktivierung IRM – 48h
- Phase 2 – **Reporting Only**:
 - Erstellung der IRM Policies
 - Analyse der Reports und Alerts (Ohne Eingriff bei Endbenutzern)
- Phase 3 – **Restrictions**:
 - Einschränkung bei Datenverlust
 - Notifizierung der Endbenutzer
 - Generierung Alerts
 - Analyse der Reports und Alerts



EDISCOVERY

CONTENT SEARCH

Schnelle Datensuche:

- Exchange, SharePoint, Teams, OneDrive
 - Basis: Regular Expression (Regex)

Einhaltung gesetzlicher Vorschriften:

- Bei regulatorischen Anforderungen bzgl. Bereitstellung der Daten

Risikominimierung:

- Sensible Daten gezielt zu finden

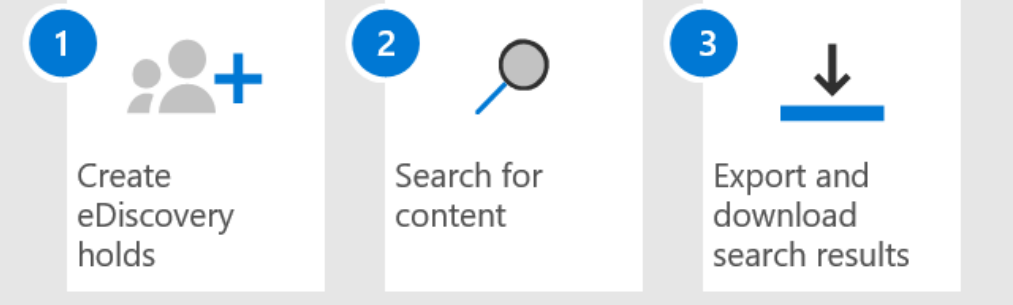
Kosteneffizienz:

- Zeit-, Kosten- und Ressourcenersparnis durch Automatisierung des Such- und Analyseprozesses

Benutzerfreundlichkeit:

- Einfache Bedienung für Admins mit korrekter RBAC-Rolle

Core eDiscovery workflow



DATA LIFECYCLE

DATA LIFECYCLE RETENTION POLICIES

- Wie lange werden / müssen Daten im Unternehmen aufbewahrt werden
 - Löschpolicy
 - Aufbewahrungspolicy
 - Kombination: Aufbewahrungspolicy & Löschpolicy



base it

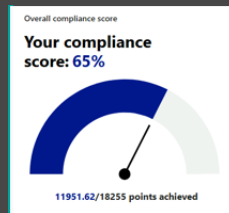
COMPLIANCE MANAGER & ALERTS

COMPLIANCE MANAGER & ALERTS

STETIGE VERBESSERUNG & ANALYSEN

Manager

- Vorschläge seitens Microsoft zur Verbesserung des „Compliance Scores“
- Hinzufügung Neuerungen im Feature Set
- Integration von Microsoft Purview Copilot im Admin Portal



Alerts

- Zentrale Stelle für die Bearbeitung aller Alerts aus Purview Diensten
 - DLP
 - IRM
 - Retention Policies
 - Uvm.
- → Übermittlung
 - an Security



Neue Verordnungen

- NIS-2
- ISO 27001
- Bank Revisionen
- Gesundheitsvorgaben
- Neues
- Uvm.



IMPLEMENTIERUNG PURVIEW DIENSTE

IMPLEMENTIERUNG

PURVIEW DIENSTE

Selektierung der benötigten Dienste

1

Erstellung Phasenplan für Rollout der Services.

Durch Feedback der Fachabteilungen müssen schützenswerte Daten immer wieder angepasst & verbessert werden. Kein „Set and Forget“.

2

Stetige Nachbesserung

Nachhaltige Analysen und Alerting

3

Aufarbeiten von Alerts, Analysen von Reports, Verbesserungsvorschläge für neue Verordnungen.



IMPLEMENTIERUNG

AUFWÄNDE UND UMSETZUNG

1. Identifizierung der Purview Dienste
2. Aufwandsschätzung für Rollout & Implementierung
3. Technische Umsetzung
4. Stetige Nachbesserung und Nachbetreuung:
Managed Service Purview



**STETIGE
VERBESSERUNG &
ANALYSEN**

PURVIEW MANAGED SERVICE

BETREUUNG

DATA LOSS PREVENTION | INSIDER RISK MANAGEMENT | INFORMATION PROTECTION
SENSITIVE INFO TYPES | EDISCOVERY | RETENTION POLICIES
ALERTS & REPORTING



**Feedback
Fachabteilungen**



Neuerungen

Nachhaltigkeit



RegEx



Apps



Policies



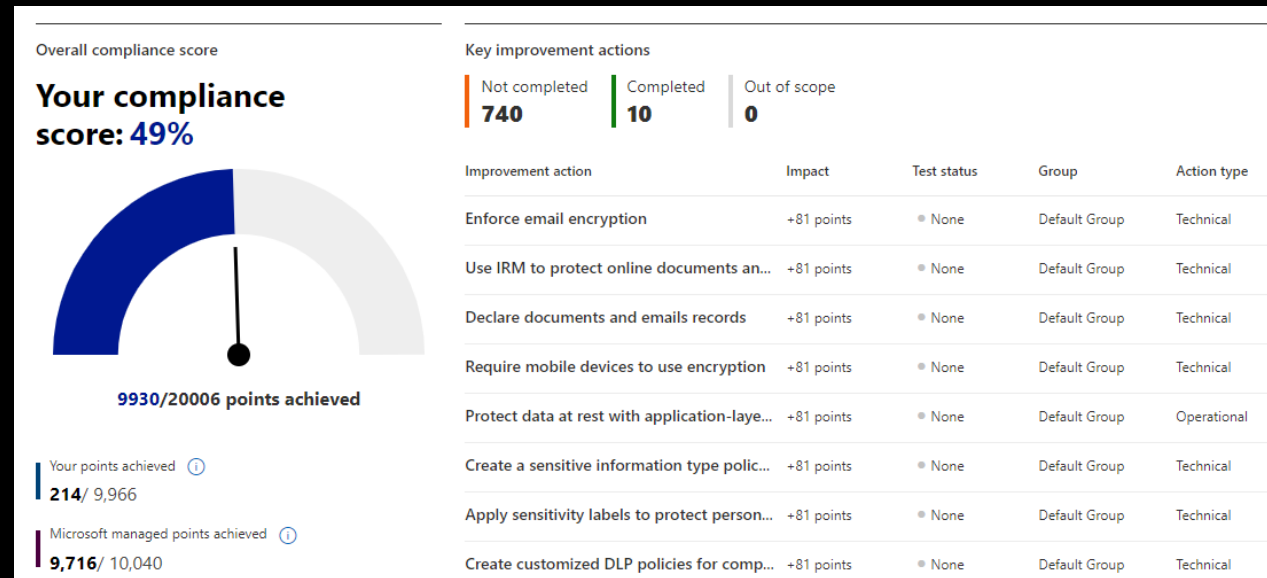
Alerts



PURVIEW MANAGED SERVICE

COMPLIANCE SCORE

- Analyse Verbesserungsvorschläge in **Compliance Manager**
- Erstellung Vorschlagskatalog inkl. **Risikoanalyse**
- Tracking von nicht umgesetzten Aktionen



MANAGED SERVICE PURVIEW

SYSTEMCHECK BEISPIELE

Information Protection				
LINK:	https://purview.microsoft.com/informationprotection/purviewmip			
Component	Doing (Generic)	Done	Status	Comment
Data Location	Check Data locations for Files and Export Report			
Check Information Protection Labels	Export Report Label Summary			
Reporting	Analyze and Export Reports for Information Protection			
Recommendations	Check Recommendations for Information Protection Labeling and Encryption			
Explorers	Check Information Protection Explorers (Data Explorer, Activity Explorer, Content Explorer)			
Classifiers	Check Trainable Classifiers, EDM Classifiers, Collection Policies			
Sensitive Info Types	Check automated Sensitive Info Types			

Data Loss Prevention				
LINK:	https://purview.microsoft.com/datalossprevention			
Component	Doing (Generic)	Done	Status	Comment
Policy Check	Check Data Loss Prevention Policies			
Check Top Activities Reporting	Check Top Activity Detection regarding Data Leakage Analyze and Export Reports for Data Loss Prevention			
Recommendations	Check Recommendations for Data Loss Prevention			
Explorers	Check Information Protection Explorers (Data Explorer, Activity Explorer, Content Explorer)			
Data Leakage	Identify and Prevent Users from potential Data Leak with unprotected data at risk			
Alerts	Check Alerts for DLP and Export Top Alerts for Customer			

Sensitive Info Types				
LINK:	https://purview.microsoft.com/informationprotection/informationprotectionlabels/sensitivitylabels			
Component	Doing (Generic)	Done	Status	Comment
Info Types	Check configured Sensitive Info Types and Create New Ones at customer feedback			
Check Sensitivity Labels	Analyze and Explore assigned sensitivity labels (Microsoft Created and Customer Created)			
Reporting	Analyze and Export Reports for Sensitivity Labels			
Recommendations	Check Recommendations for Sensitivity Labels			
Scope	Check Scoping of Labels			
Sensitive Info Types	Check automated Sensitive Info Types			

Compliance Manager & Score				
LINK:	https://purview.microsoft.com/compliancemanager			
Component	Doing (Generic)	Done	Status	Comment
Compliance Manager	Check Overview of Compliance Manager			
Improvement Action	Check and Summarize Improvement Actions for Customer			
Compliance Score	Scale and Increase Compliance Score Points with Purview Recommendations (if possible)			
Solutions	Analyze possible solutions for point increase			
Regulations	Check Customer required regulations and needed baseline policies			
Alerting	Edit Alerts and Check Readiness Templates			
Reporting	Report Key Improvement Actions and Export possibilities to improve compliance score			

Insider Risk Management				
LINK:	https://purview.microsoft.com/insiderriskgmt			
Component	Doing (Generic)	Done	Status	Comment
Risks	Analyze potential Risks and Report to Customer (e.g. Data Breaches and Extractions)			
Check Information Protection	Identify Information Protection fraud with decreasing labels			
Reporting	Analyze and Export Reports for Insider Risks			
Forensic Evidence	Provide forensic evidence to customer if needed			
Recommendations	View Recommendations for insider risk management for compliance improvements			



PURVIEW MANAGED SERVICE

AUFWÄNDE LAUFENDE BETREUUNG

Phase 1: 8h / Monat

- Anfangsphase
- Anpassungen
- Alert Analyse
- Compliance Score Improvements
- Erstellung Vorschlagskatalog
- Report

Phase 2: 4h / Monat

- Alert Analyse
- Compliance Score Improvements
- Erstellung Vorschlagskatalog
- Report



PURVIEW & SECURITY

BETTER TOGETHER

- Beispiele Enduser / Admin Verhalten

The screenshot displays the Microsoft Purview interface. On the left, a navigation pane shows the 'Content Search' option highlighted with an orange box. The main content area is titled 'Content search' and includes a search bar and a 'New search' button, also highlighted with an orange box. Below the search bar, there is a table with search results.

Vertraulichkeit: PurMa_Test_Internal Richtlinientipp: Ihre E-Mail steht im Konflikt mit einer Richtlinie in Ihrer Organisation. [Details ausblenden](#)
Purker Matthias | base-IT: Überprüfen Sie die Empfänger und den Inhalt, da sie mit der Organisationsrichtlinie in Konflikt geraten. [Empfänger entfernen](#)
Details zu den scheinbar vertraulichen Informationen anzeigen. [Weitere Informationen](#)

Diese E-Mail während der Arbeitszeit der meisten Empfänger senden: Do, März 05 um 8:00 AM

Microsoft Purview Search

Home
Solutions
Learn
Settings
eDiscovery

Content search

Search your organization for content in emails, documents, Skype for Business conversations, and more. You can also search for content in external sources like OneDrive and SharePoint.

This page is being retired in August 2025. You can now manage all your searches in our new, unified eDiscovery experience, which combines Content Search capabilities into the eDiscovery case workflow, giving admins better control over who can search and an improved experience today to enjoy these new capabilities. [Learn more about the new experience.](#)

Search Export

+ New search ↓ Export list ↻ Refresh

Name	Description
<input type="checkbox"/> Teams data	
<input type="checkbox"/> Inbox	
<input type="checkbox"/> Credit Card	Credit Card

PURVIEW & SECURITY BETTER TOGETHER

- Alerts Purview
- eDiscovery
- Data Loss Prevention
- Insider Risk Management
- Uvm.

Purker Matthias | base-IT (Benutzeraktivitätsbericht) Aktionen melden ▾

Zeitraum: 4.12.2025 - 2.3.2026

Benutzeraktivität **Aktivitäten-Explorer**

Filter: Risikofaktor: Beliebig ✕

Sortieren nach ▾

- **Collection: Dateien, die während der Synchronisierung von SharePoint heruntergeladen wurden** ...
4. März 2026 (UTC) | Risikobewertung: 5/100
2-Ereignisse: Von 1 SharePoint-Site synchronisierte Dateien
2-Ereignisse: Dateien mit sensiblen Informationen, einschließlich: Indonesia Passport Number, Philippines Passport Number, All Full Names, Diseases, UAE Passport Number
2-Ereignisse: Dateien, die Bezeichnungen haben, einschließlich: Öffentlich
- **Exfiltration: E-Mails mit Anlagen, die außerhalb der Organisation versendet wurden** ...
4. März 2026 (UTC) | Risikobewertung: 25/100
2-E-Mails: wurden an 1 Empfänger außerhalb der Organisation gesendet
- **Exfiltration: E-Mails mit Anlagen, die außerhalb der Organisation versendet wurden** ...
3. März 2026 (UTC) | Risikobewertung: 75/100
- **Collection: Dateien, die während der Synchronisierung von SharePoint heruntergeladen wurden** ...
2. März 2026 (UTC) | Risikobewertung: 5/100
3-Ereignisse: Von 1 SharePoint-Site synchronisierte Dateien

↓ Exportieren 122 Elemente ✕ Spalten zurücksetzen Spalten anpassen Diese Ansicht speichern Anzahl der Anzeigen

Datum (UTC) ▾	Aktivität ▾	Dateiname ▾	Objekt-ID ▾	Workload ▾	Elementtyp ▾
<input type="checkbox"/> 4. März 2026 12:56	Email sent to external recipient	d5be2a4f-3110-44b5-8fa6-...	<DB9PR04MB11511483E4652...	IrmHygiene	Email
<input type="checkbox"/> 4. März 2026 12:56	Email sent to external recipient	d5be2a4f-3110-44b5-8fa6-...	<DB9PR04MB11511483E4652...	IrmHygiene	Email
<input type="checkbox"/> 4. März 2026 12:03	File synced from SharePoint	MKI Project Controlling.xlsx	https://baseit.sharepoint.com/...	SharePoint	File
<input type="checkbox"/> 4. März 2026 07:55	File synced from SharePoint	MKI Project Controlling.xlsx	https://baseit.sharepoint.com/...	SharePoint	File
<input type="checkbox"/> 3. März 2026 18:26	Email sent to external recipient	Outlook-lx20gh1s.png.a4e...	<DB9PR04MB11511091080AA...	IrmHygiene	Email
<input type="checkbox"/> 3. März 2026 18:26	Email sent to external recipient	Outlook-lx20gh1s.png.a4e...	<DB9PR04MB11511091080AA...	IrmHygiene	Email
<input type="checkbox"/> 3. März 2026 18:26	Email sent to external recipient	Outlook-lx20gh1s.png.a4e...	<DB9PR04MB11511091080AA...	IrmHygiene	Email
<input type="checkbox"/> 3. März 2026 18:26	Email sent to external recipient	Outlook-lx20gh1s.png.a4e...	<DB9PR04MB11511091080AA...	IrmHygiene	Email
<input type="checkbox"/> 3. März 2026 13:32	File synced from SharePoint	MKI Project Controlling.xlsx	https://baseit.sharepoint.com/...	SharePoint	File
<input type="checkbox"/> 3. März 2026 09:43	File synced from SharePoint	MKI Project Controlling.xlsx	https://baseit.sharepoint.com/...	SharePoint	File
<input type="checkbox"/> 3. März 2026 09:01	Email sent to external recipient	Outlook-25w5kvwe.png.Ou...	<DB9PR04MB115113D654EE7...	IrmHygiene	Email



Q&A

FRAGEN AUS DEM CHAT?



BASE-IT TECH-TONIC (WIEN)

6 EVENTS VON MÄRZ BIS JUNI

TECH-TONIC

SHIFTING TO THE
NEXT STATE OF IT

Gewinnchance direkt bei jedem Shift:

- Ticket für die techConference
- Dell Pro Plus Earbuds

Power Platform Shift

AI Shift

Security Shift

Data Security Shift

Hybrid Cloud Shift

Modern Endpoint Shift

GEWINNSPIEL

Microsoft Ignite Package im Wert von € 5.000,-

Ticket, Flug & Hotel inklusive!

- Für 3 oder mehr TECH-TONIC Events kostenlos anmelden:
www.baseit.at/tech-tonic
- Events besuchen

Schon landet Ihr Name
im Lostopf!



San Francisco 



Security Shift



14.04.2026



09:00 Uhr



Wien



Thomas Graser
Teamleitung Modern Workplace
& Security | base-IT



Jürgen Waldl
Lead Architect Security | base-IT



Markus Mayer
Pentesting Lead & Lead Architect
Security | base-IT



Irina Sukič
Partner Solution Sales Manager
Security | Microsoft



Daniel Fraubaum
Lead Architect Security | base-IT



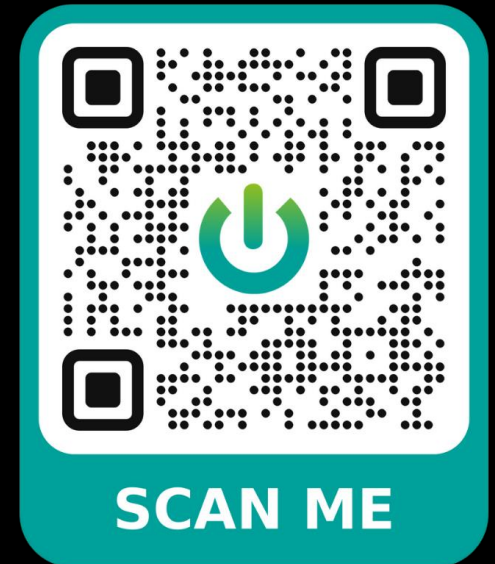
Philipp Ortner
Senior Solution Architect | Barracuda



UPCOMING WEBCASTS

JETZT ANMELDEN

- **EntraID: Hybrid Authentication, Security & Governance | 17.04.2026**
- **Azure Local: Hybrid Cloud Update & Use Cases | 24.04.2026**
- **Low-Code. High Impact: Digitaler Vorsprung mit der Power Platform | 12.06.2026**
- **Network Security Updates | 19.06.2026**



www.baseit.at/webcasts



baseit

Haider Straße 23 | 4052 Ansfelden | AT
+43 7229 87800 - 0 | office@baseit.at |
www.baseit.at

[Base-IT GmbH \(unserebroschuere.at\)](http://Base-IT GmbH (unserebroschuere.at))

