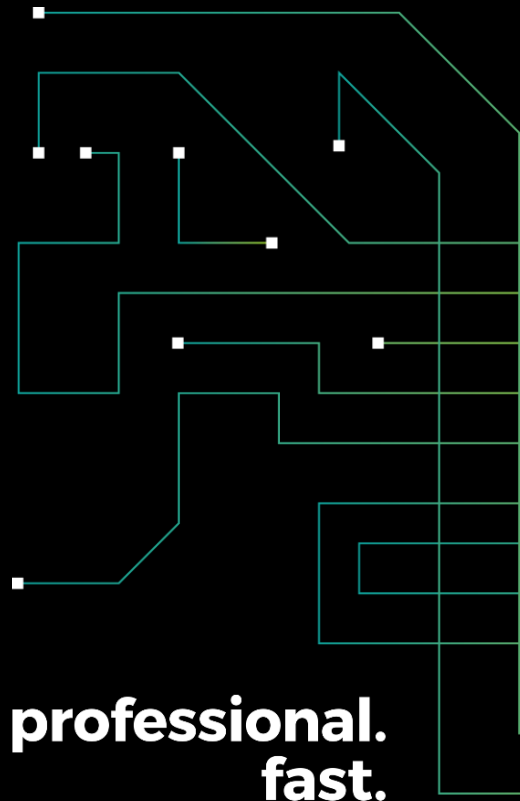
base it

# BASE-IT 24X7 SECURITY SERVICES

Managed Service Security &
Security Operation Center (SOC)



professional.
fast.
secure.

**DER KUNDE STEHT IM MITTELPUNKT UNSERES HANDELNS.**

# WER WIR SIND

## BASE-IT AUF EINEN BLICK

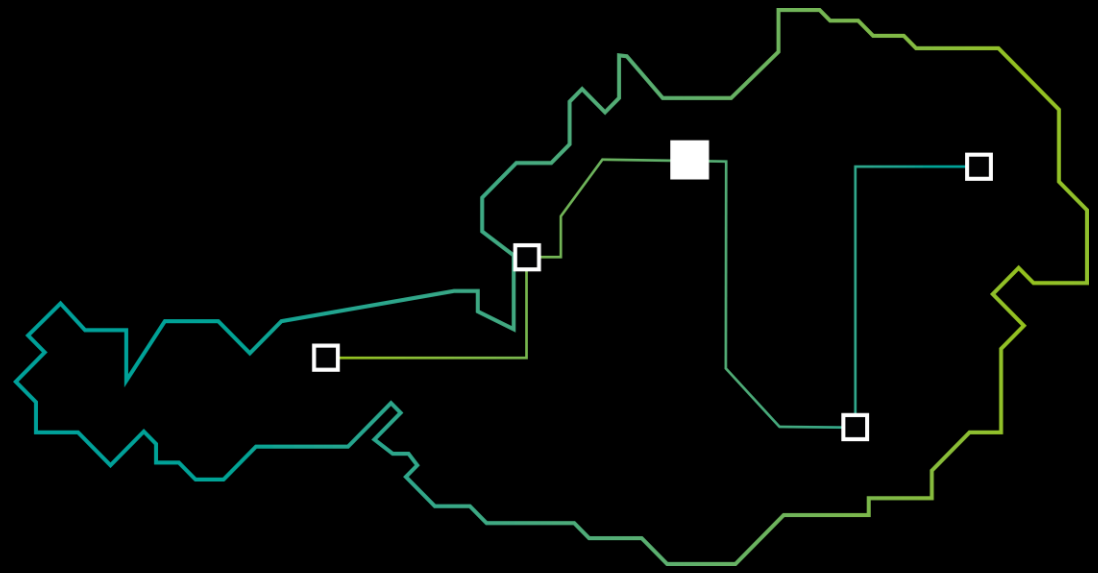
- 2010 gegründet von:
  - Gregor Dedl
  - Christoph Moser
- über 140 engagierte Mitarbeiter*innen (davon mehr als 120 Consultants)
- 5 Standorte:
  - Ansfelden, Wien, Salzburg, Hall in Tirol, Graz
- Über 500 zufriedene Kunden in Österreich und angrenzenden Ländern
- FY 2023/24 Umsatz: 33M €

**KNOW-HOW UND INDIVIDUELLER SERVICE SIND UNSERE MARKENZEICHEN.**

# BASE-IT SPACES

## FÜNF STANDORTE | EINE BASE-IT

- Ansfelden | seit 2010
  - Haider Straße 23, 4052 Ansfelden
- Wien | seit 2016
  - Johannitergasse 2, 1100 Wien
- Salzburg | seit 2022
  - Carl-Zuckmayer-Straße 33, 5020 Salzburg
- Hall in Tirol | seit 2023
  - Brockenweg 2, 6060 Hall in Tirol
- Graz | seit 2025
  - Dr. Auner-Straße 22/2, 8074 Raaba-Grambach



# UNSER PORTFOLIO

## Managed Services & Support Packages

- Data Center Support & Outsourcing
- Client Service Desk Support & Outsourcing
- Security Operation Center
- Managed Service Security
- Managed Service Endpoint Manager
- Managed Service SQL
- Managed Service Firewall
- Managed Service Patchmanagement
- Managed Service SCOM
- Managed Service Azure Local
- individuelle Services nach Vereinbarung
- bis zu 24x7 Verfügbarkeit

## Security, Identity & Compliance

- Entra Security
- Defender for Endpoint
- Defender for Office 365
- Defender for Identity
- Defender for Cloud Apps
- Defender for Cloud
- Sentinel
- Secure Authentication
- Identity Management
- Netwrix Password Secure
- Public Key Infrastructure
- Zero Networks
- Cisco ISE
- Blue Shield Umbrella

## Security Management

- Pentesting
- Pingcastle AD Audit
- Vulnerability Management
- AD Tiering
- Nessus
- External Attack Surface Management

## Modern Workplace & Endpoint Management

- Intune & Intune Suite
- Configuration Manager
- Endpoint Analytics
- Entra Only Client
- Autopilot
- Scappman / PatchMyPC
- Windows 365
- Azure Virtual Desktop
- Remote Desktop Services (RDS)
- JAMF
- Yubikey

## Communication & Collaboration

- Exchange OnPrem / Hybrid / Online
- Mail Encryption
- Data Kollaboration mit Teams, Outlook, SharePoint & OneDrive
- Office 365 Cloud to Cloud Backup
- Office 365 Cloud Archiving
- Purview Platform
- Tenant to Tenant Migrationen

## Network & Firewall

- LAN Technologies (Cisco & Fortinet)
- WLAN Technologies (Cisco & Ubiquiti)
- Azure Networking
- Next-Gen Firewalling (Barracuda & Fortinet)
- SASE
- Application Protection & WAF

## Hybrid Cloud

- Azure Infrastructure as a Service
- Azure Platform as a Service
- Azure Local & Hyper-V
- Windows Server
- Backup & Disaster Recovery
- Active Directory
- SQL Databases
- Server Hardware
- Storage Hardware
- System Center Operations Manager
- Azure Monitor
- CheckMK

## Automation

- Power Platform
- Azure Automation
- System Center Orchestrator
- PowerShell
- Scripting

## Enterprise Service Management

- Asset Management & CMDB
- ServiceNow ITSM
- ServiceNow CSM
- ServiceNow ITOM
- Business Process Consulting

## Artificial Intelligence

- Copilot Studio
- Microsoft 365 Copilot
- Microsoft 365 Copilot Agents
- Security Copilot
- Power Platform Copilot
- GitHub Copilot
- AI Builder
- Azure OpenAI Services

## Strategic Services

- Technical Account Management
- IT Lead Architecture
- Project Management
- CISO & CIO Substitution / as a Service
- Innovation Updates (z.B. Microsoft 365, Microsoft Entra Security, Azure Infrastructure Services, ...)
- Mitarbeitertrainings

# MICROSOFT CLOUD SOLUTION PROVIDER

## BASE-IT – IHR CSP PARTNER

### Microsoft Solutions Partner

- jahrelange Erfahrung in der Umsetzung und im Betrieb von Microsoft Produkten
- professionelle Beratung & Unterstützung durch unsere Base-IT Expert*innen für eine optimale Lizenzstrategie und ein ideales Wachstum
- Gold und Silver Kompetenzen
- bestehende & fortlaufende Zertifizierungen


**Gold Competences:**

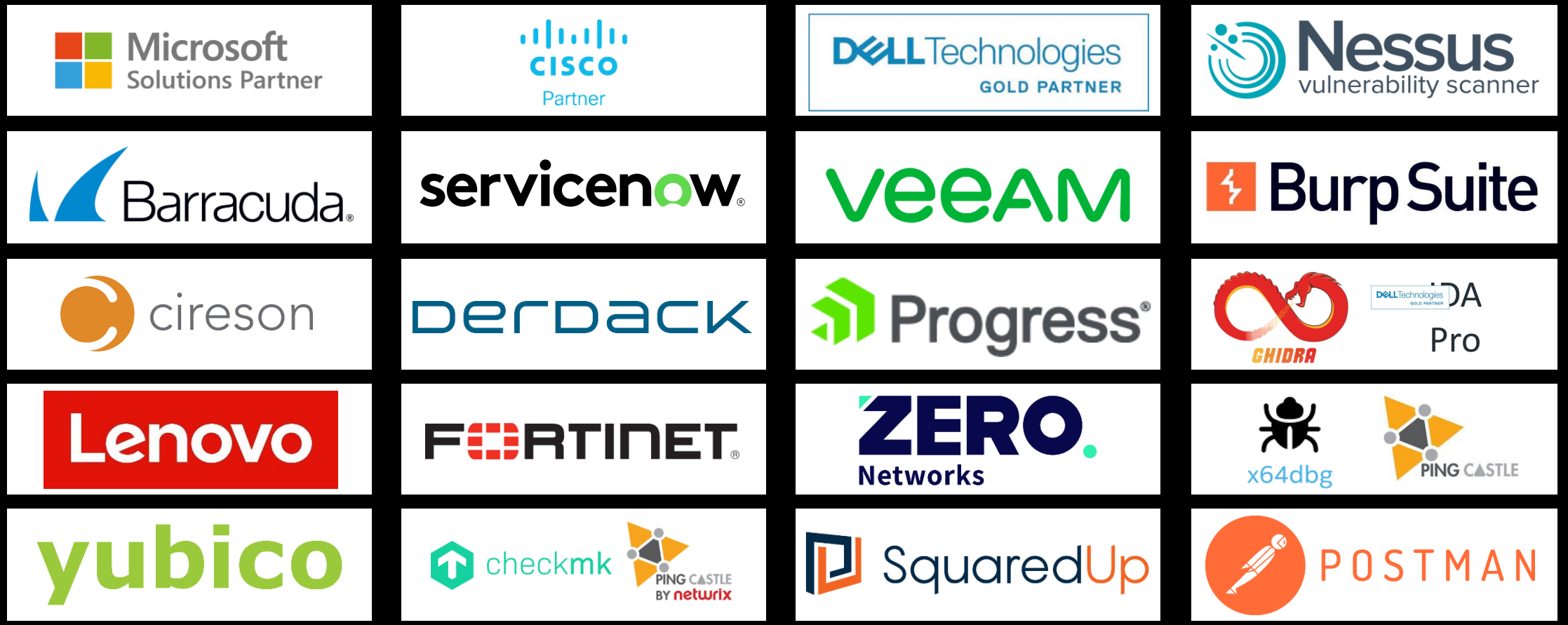
- Cloud Productivity
- Application Integration
- Enterprise Mobility Management
- Datacenter
- Windows & Devices
- Cloud Platform
- Small & Midmarket Cloud Solutions

**Silver Competences:**

- Collaboration and Content
- Security
- Application Development

# UNSERE PARTNER

## ZUSAMMENARBEIT MIT RENOMMIERTEN HERSTELLERN



# REFERENZEN

## ZAHLREICHE ZUFRIEDENE KUNDEN

base it

# WARUM CYBERSECURITY?

***WÄRE CYBERKRIMINALITÄT EINE VOLKSWIRTSCHAFT, WÜRDE 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.***

Quelle: Cybercrime is world's third-largest economy thanks to booming black market | Cybernews

# DIE 4 HÄUFIGSTEN SECURITY-RISIKEN

## SETZEN SIE GEZIELTE GEGENMASSNAHMEN

**1 Phishing und Social Engineering**

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

**2 Ransomware und Malware**

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

**3 Datenlecks**

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

**4 Mangelndes Bewusstsein**

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

# 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.*


1 von 3
€250K
81%
94%
30%
80%

**MIT DEM BASE-IT MANAGED SERVICE SECURITY & SECURITY OPERATION CENTER IST IHRE M365-UMGEBUNG RUND UM DIE UHR OPTIMAL GESCHÜTZT!**

# UNSERE 24X7 SECURITY SERVICES

# BESTENS GERÜSTET
## FÜR STEIGENDE ANFORDERUNGEN

### Herausforderungen

- Cyberbedrohungen
- Gesetzliche Richtlinien & Compliance
- Ressourcenmangel
- IT-Security Awareness
- Skalierbarkeit
- Kostentransparenz
- uvm.

### Unsere Lösung

- base-IT 24x7 Managed Service Security & SOC
- M365 E3 bzw. E5 | Defender for Cloud | Microsoft Sentinel | Complete
- Einsatz von innovativen Microsoft Security-Lösungen

### Ihre Vorteile

- IT-Sicherheit auf höchstem Niveau
- Ideale Skalierbarkeit
- Absolute Kostentransparenz
- Operativer Betrieb und Betreuung durch uns
- Entlastung Ihrer Ressourcen für starken Fokus auf Ihr Kerngeschäft

# UNSER SECURITY PORTFOLIO

## AUF EINEN BLICK

### Microsoft-Lösungen

Nutzung modernster Sicherheitslösungen wie:

- Microsoft Entra
- Microsoft Defender XDR
- Microsoft Sentinel
- Defender for Cloud
- Security Copilot
- uvm.

### 24x7 SOC: Security Operation Center

- Überwachung und Schutz vor Cybervorfällen rund um die Uhr.
- Reaktive Überwachung
- Reaktionshandling
- Risikoeinschätzung
- User Interaktion

### 24x7 Managed Service Security

- Verschiedene Pakete, die nahtlos in die Microsoft 365 Umgebung integriert werden können.
- Kontinuierliche Entwicklung des Secure Score
- Regelmäßiges Reporting
- Service Delivery Management

# MANAGED SERVICE SECURITY

## ESSENZIELLE BESTANDTEILE IHRER SECURITY-STRATEGIE

**Proaktive Betriebsführung, Wartung & Purple Teaming**

1

*IT-Security durch proaktive Agilität und Betreuung von Microsoft Security Lösungen auf Basis des gewählten Managed Service Pakets.*

*Betreuung durch das Base-IT SOC für eine lückenlose 24x7 Überwachung und umgehende Reaktion auf potenzielle Bedrohungen durch unser erfahrenes Expertenteam.*

2

**Reaktives Alert-Handling**

**Forensische Analyse & zentralisiertes Logging**

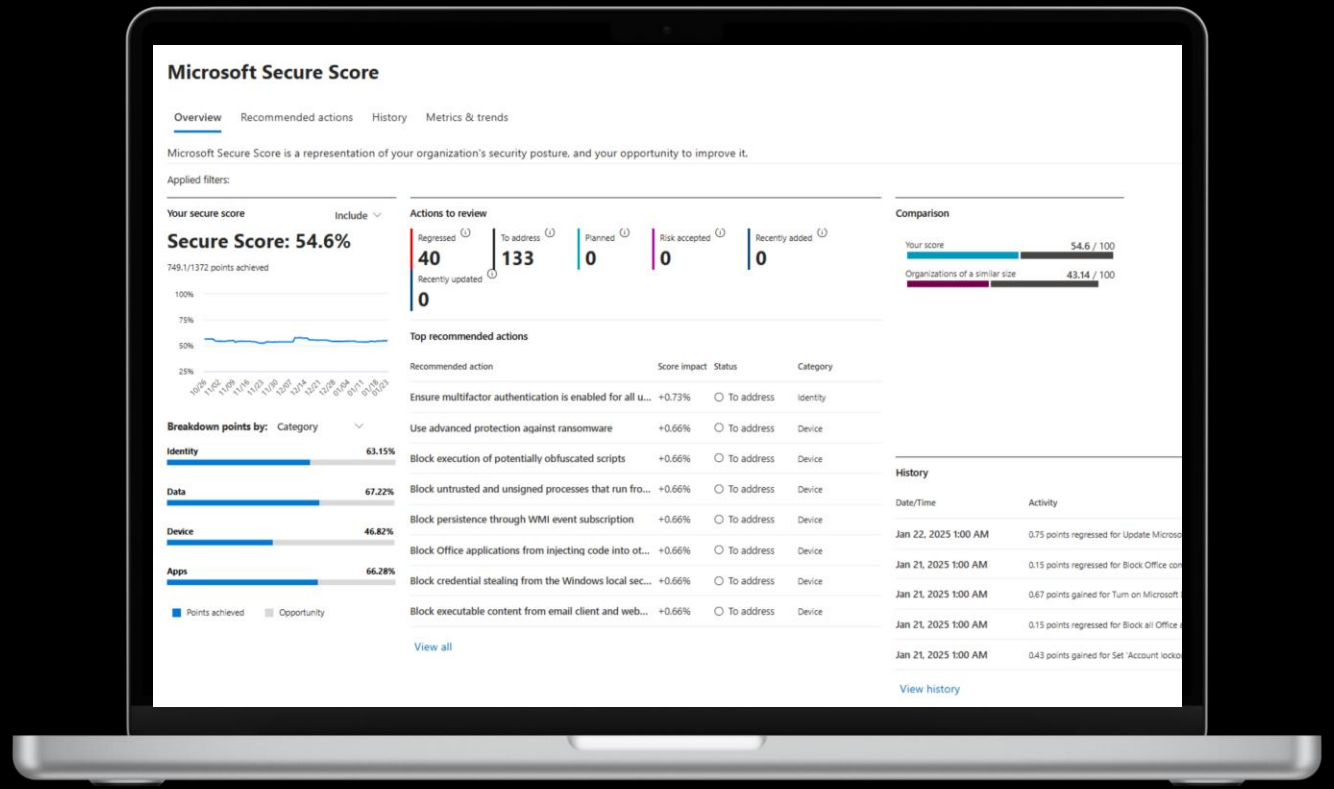
3

*Aufarbeiten von Incidents durch das Base-IT Security Expert*innen Team, um zukünftige Angriffe zu verhindern.*

# MANAGED SERVICE SECURITY

## SECURE SCORE – PROAKTIVE ZIELE

- Kontinuierliche Analyse der Empfehlungen aus Microsoft-Sicherheitslösungen.
- Abstimmung und Priorisierung der Maßnahmen gemeinsam mit dem Kunden.
- Umsetzung rascher Optimierungen direkt im Managed Service Security.
- Größere Anpassungen als eigenständiges Projekt mit Freigabe durch den Kunden.



# MANAGED SERVICE SECURITY

## SECURE SCORE – LINKSAMMLUNG

Microsoft-Sicherheitsbewertung – Microsoft 365 Security

Security recommendations – Microsoft 365 Security

Identity Secure Score - Microsoft Azure

Security Center - Microsoft Azure

# MANAGED SERVICE SECURITY

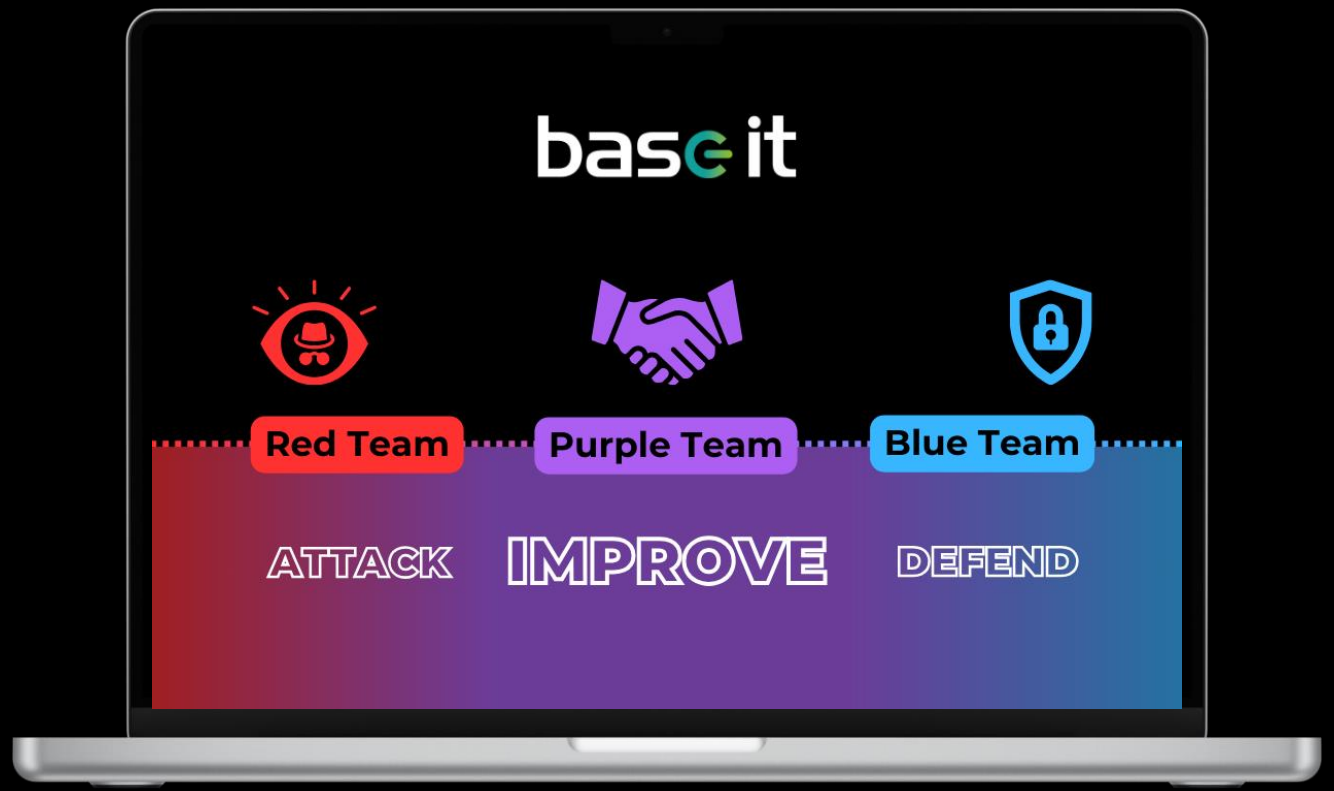
## ÜBERBLICK PURPLE TEAMING

Purple Teaming ist ein kollaborativer Sicherheitsansatz, bei dem das Red Team (Angreifer) und das Blue Team (Verteidiger) gemeinsam agieren. Ziel ist es, Sicherheitslücken frühzeitig zu erkennen und die Abwehrmechanismen gezielt zu verbessern.

Typische Red Team-Aktivitäten sind:

- Phishing-Kampagnen zur Erkennung menschlicher Schwächen
- Exploitation von Schwachstellen in Systemen und Anwendungen
- Lateral Movement zur Ausbreitung im Netzwerk
- Credential Dumping und Privilege Escalation

Durch die direkte Zusammenarbeit mit dem Blue Team können Verteidigungsmaßnahmen in Echtzeit getestet und optimiert werden.



# 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.
  - Informational, 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.*

# MANAGED SERVICE SECURITY

## AD SECURITY PINGCASTLE ANALYSE (ADD-ON)

### Herausforderungen

- AD ist komplex und schwer manuell zu prüfen.
- Schwachstellen bleiben ohne Tools oft unerkannt.
- Änderungen sind schwer nachvollziehbar.
- Compliance und Reporting sind manuell mit hohem Aufwand verbunden.

### Unsere Analyse

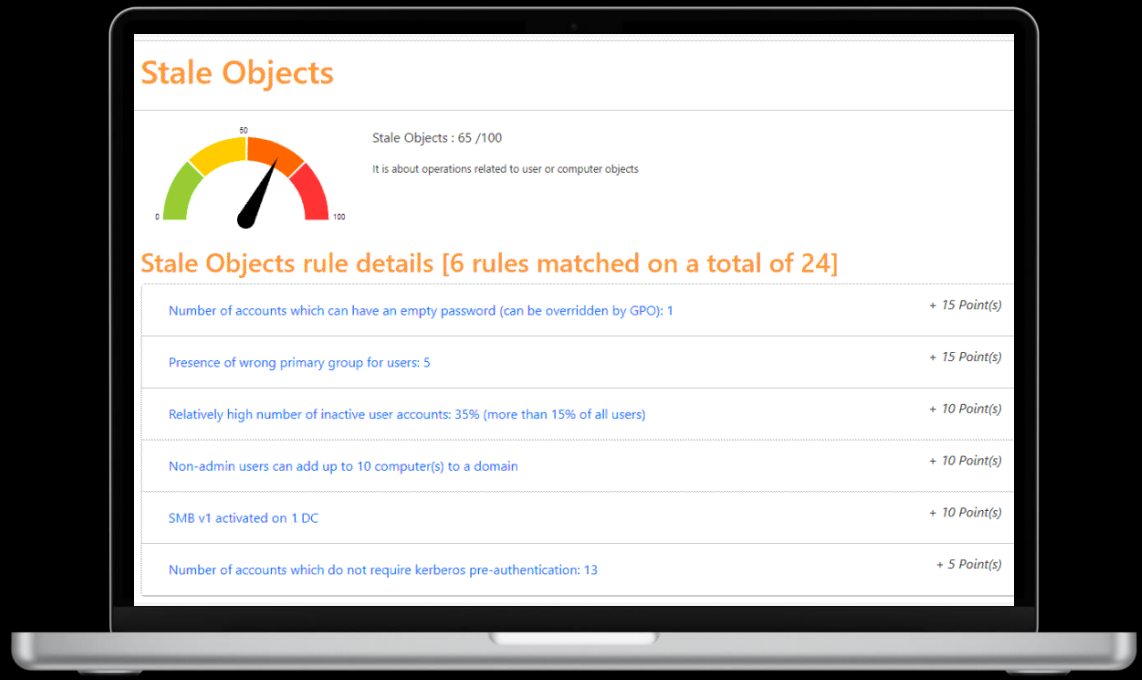
- Schaffung einer fundierten Basis für umfassende AD-Sicherheit.
- Detaillierte Analyse der aktuellen Ist-Situation.
- Entwicklung eines nachhaltigen Maßnahmenplans.
- Einsatz erprobter Best-Practice-Methoden

### Ihre Benefits

- Einheitliche, standardisierte Regelwerke.
- Übersicht der Ist-Situation.
- Vergleichbarkeit mit zukünftigen Scans.
- Sicherstellung der Compliance-Konformität.
- Ständig aktualisierte Risikodatenbank.

# MANAGED SERVICE SECURITY

## BEISPIELAUSGABE – HEALTH CHECK ANALYSE


Quelle: Ping Castle (msxfaq.de)

# MANAGED SERVICE SECURITY

## INTERNAL/EXTERNAL VULNERABILITY MANAGEMENT (ADD-ON)

Nessus vulnerability scanner

### Herausforderungen

- Fehlende Transparenz über Schwachstellen im Netzwerk.
- Komplexe Netzwerkinfrastrukturen mit unterschiedlichen VLANs.
- Zeit- und ressourcenintensive manuelle Sicherheitsprüfungen.
- Unsicherheit bei der Priorisierung und Behebung von Risiken.

### Unser Audit

- Durchführung eines umfassenden Schwachstellen-Scans.
- Analyse der Ergebnisse und Erstellung eines professionellen Berichts.
- Gemeinsame Besprechung der Findings und Empfehlungen.
- Laufende Unterstützung bei kritischen Schwachstellen und AD-Themen.

### Ihre Benefits

- Klare Übersicht über sicherheitsrelevante Schwachstellen.
- Priorisierte Maßnahmenliste zur schnellen Umsetzung.
- Unterstützung bei kritischen Themen wie Netzwerksegmentierung, Patch-Management und AD-Härtung.
- Höhere Sicherheit und Compliance durch gezielte Nachbereitung.

# MANAGED SERVICE SECURITY

## ROADMAP SECURITY ADD-ONS

**Kick-Off**

1

*Workshop zur Vorbereitung von organisatorischen Themen sowie zur Klärung und Bereitstellung der Zugriffe.*

*Mit gezieltem Scanning identifizieren wir sicherheitsrelevante Schwachstellen.*

2

**Analyse**

**Präsentation**

3

*Aufbereitung, ausführliche Bewertung und Vorstellung der Erkenntnisse sowie Präsentation eines Maßnahmenplans.*

*Auf Wunsch stärken wir mit bewährten Methoden Ihre IT-Sicherheitslage.*

4

**Optimierung**

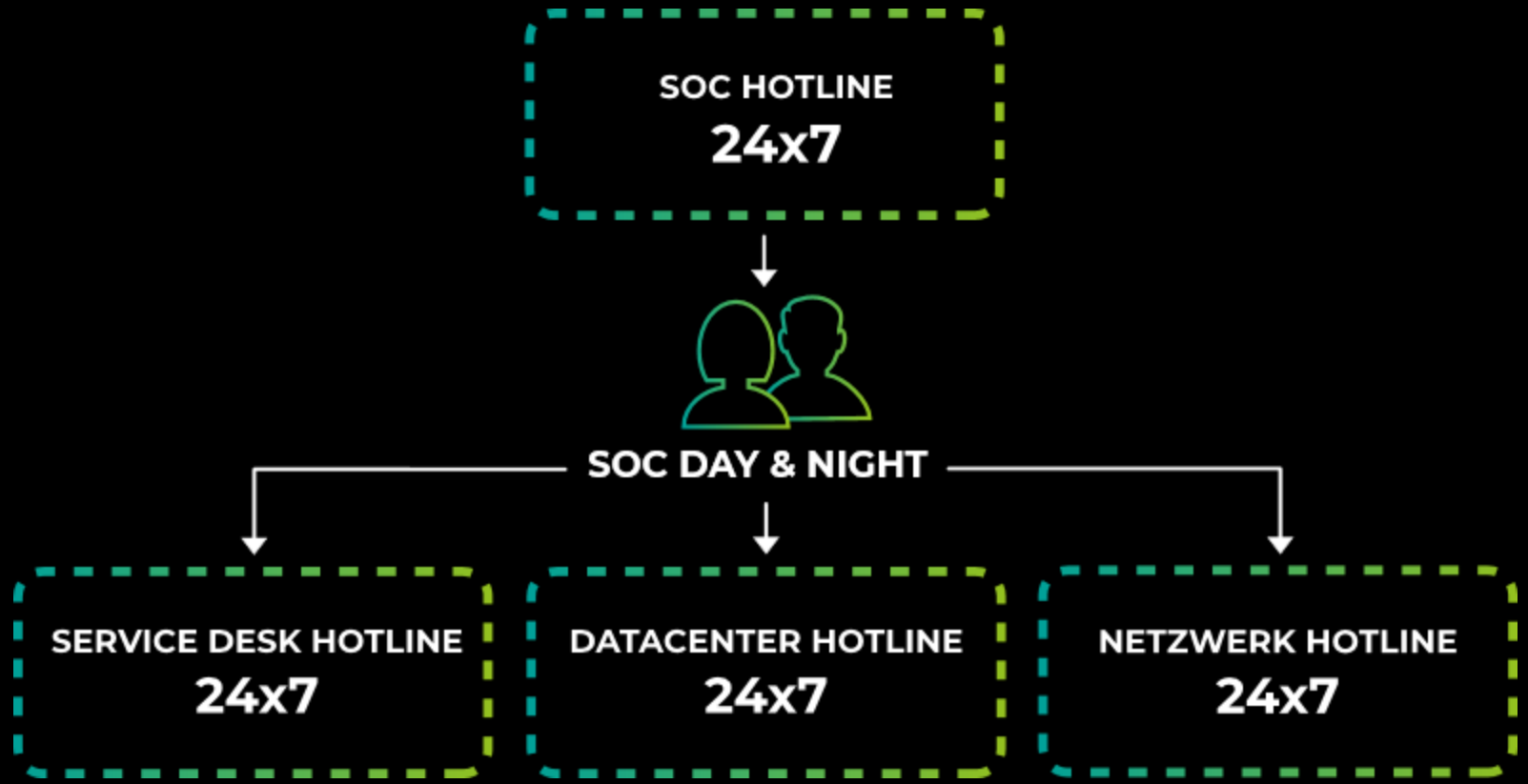
**Timeline & Kosten abhängig von Paket**

# SECURITY OPERATION CENTER

## 24X7 GESCHÜTZT DURCH UNSERE EXPERT*INNEN

Durch das base-IT Security Operation Center (SOC) profitieren Sie von:

- Überwachung und Bearbeitung von Alerts rund um die Uhr
- Alert-Bearbeitung basierend auf der Kundenvereinbarung
- Monatliche Alert-Berichte
- SLA für Alert-Bearbeitung



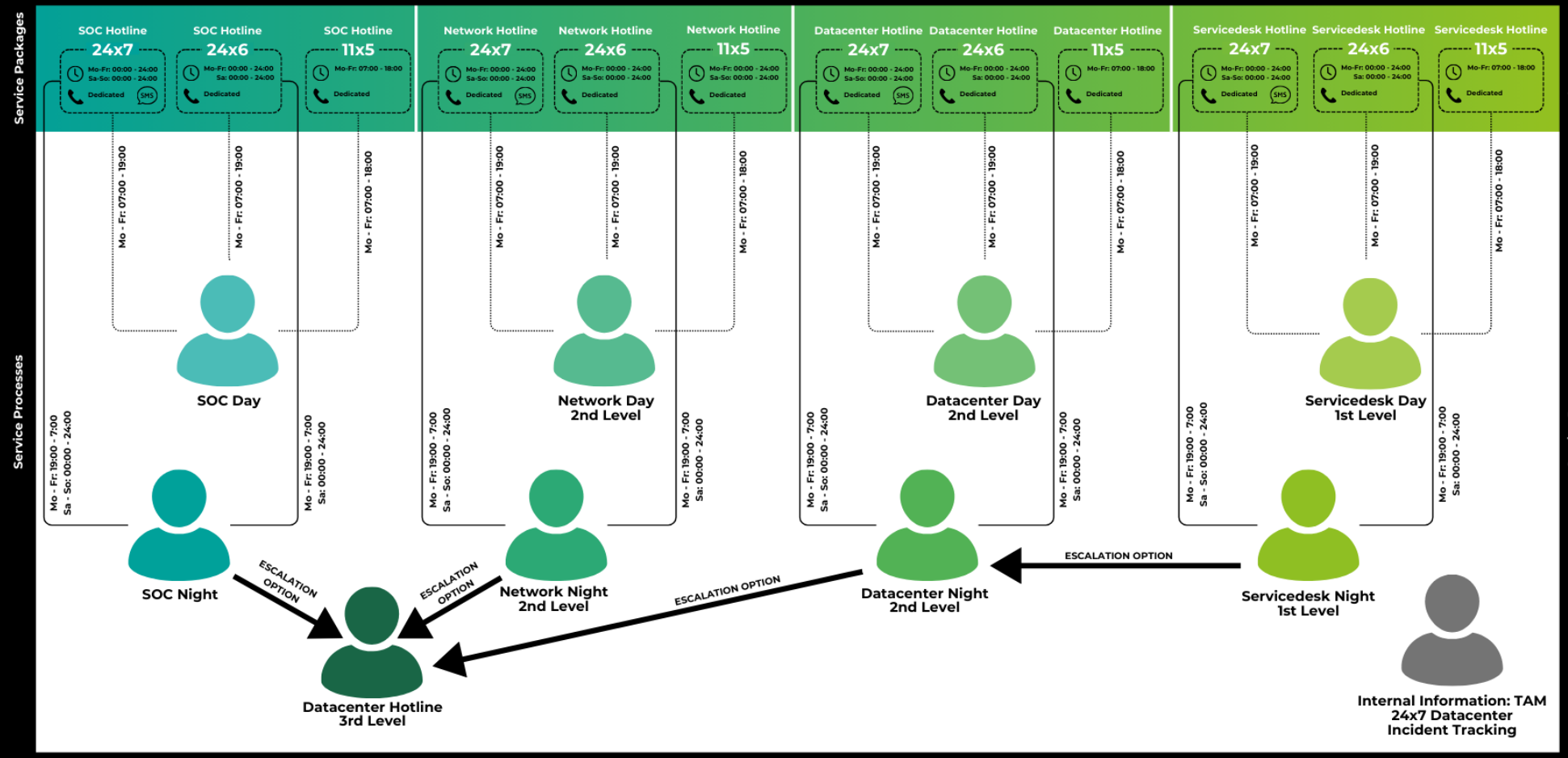
# SECURITY OPERATION CENTER

## REAKTIONSKATALOG - AUSZUG

| Produkt | Incident | High | Medium | Low | Informational |
|---|---|---|---|---|---|
| Identity Protection | Risky User (Persönlicher User) | User blockieren und kontakieren, Passwortänderung anfordern falls die Anmeldung nicht vom User initiiert wurde | User kontaktieren, Passwortänderung falls die Anmeldung nicht vom User initiiert wurde | Sign In`s auf Auffälligkeiten prüfen, Bei Auffälligkeiten mit User abstimmen | nicht zutreffend |
| Identity Protection | Risky User (Service User) | Kunde kontaktieren, Passwortänderung anfordern falls die Anmeldung nicht vom Service | Kunde kontaktieren, Passwortänderung anfordern falls die Anmeldung nicht vom Service | Sign In`s auf Auffälligkeiten prüfen, Bei Auffälligkeiten mit Kunde abstimmen | nicht zutreffend |
| Identity Protection | Risky Sign In (Persönlicher User) | User kontaktieren, Passwortänderung falls die | User kontaktieren, Passwortänderung falls die | Sign In`s auf Auffälligkeiten prüfen, Bei Auffälligkeiten mit | nicht zutreffend |
| Identity Protection | Risky Sign In (Service User) | Kunde kontaktieren, Passwortänderung anfordern falls die Anmeldung nicht vom Service | Kunde kontaktieren, Passwortänderung anfordern falls die Anmeldung nicht vom Service | Sign In`s auf Auffälligkeiten prüfen, Bei Auffälligkeiten mit Kunde abstimmen | nicht zutreffend |
| Identity Protection | Risk Detection (Persönlicher User) | User kontaktieren, Passwortänderung falls die | User kontaktieren, Passwortänderung falls die | Sign In`s auf Auffälligkeiten prüfen, Bei Auffälligkeiten mit | nicht zutreffend |
| Identity Protection | Risk Detection (Service User) | Kunde kontaktieren, Passwortänderung anfordern falls die Anmeldung nicht vom Service | Kunde kontaktieren, Passwortänderung anfordern falls die Anmeldung nicht vom Service | Sign In`s auf Auffälligkeiten prüfen, Bei Auffälligkeiten mit Kunde abstimmen | nicht zutreffend |
| AzureSentinel | Generell | Incident prüfen, Betroffene Rechner in Defender for Endpoint kontrollieren und bei Bedarf Isolieren + User informieren, Auf betroffene Server verbinden und | Incident prüfen, Betroffene Rechner in Defender for Endpoint kontrollieren + User informieren, Auf betroffene Server verbinden und pürfen + Kontakt mit Kunde | Incident prüfen, Betroffene Rechner in Defender for Endpoint kontrollieren + User informieren, Auf betroffene Server verbinden und pürfen + Kontakt mit Kunde | nicht zutreffend |
| AzureSentinel | MFA disabled for User | nicht zutreffend | Prüfen wer die MFA disabled hat, Kontaktaufnahme mit Admin, Grund für Deaktivierung fragen, Im besten fall wieder aktivieren | nicht zutreffend | nicht zutreffend |
| AzureSentinel | GlassbreakAdmin Logon Detected | GlassbreakAdmin - Block Sign In, Prüfen der Audit Logs im Azure AD ob User erstellt/geändert wurden (Rechtevergabe, Passwortänderunge)..., Falls ja diese auch sperren, Passwortänderung des GlassbreakAdmins gemeinsam mit Kunde | nicht zutreffend | nicht zutreffend | nicht zutreffend |
| | Honeytoken Activity(von Server | nicht zutreffend | Mit Kunde Abstimmen ob der Alert | nicht zutreffend | nicht zutreffend |

# BASE-IT 24X7 SERVICES

## INKLUSIVE SOC



# SCHRITT FÜR SCHRITT
## ZUR LÜCKENLOSEN IT-SICHERHEIT

**Reifegradanalyse**

1

*Gründliches Assessment der IT-Securitylandschaft zur Identifizierung von Schwachstellen.*

*Implementierung oder Upgrade moderner Microsoft Security-Lösungen.*

2

**Prüfung der Lizenzen**

**Anbindung an das SOC**

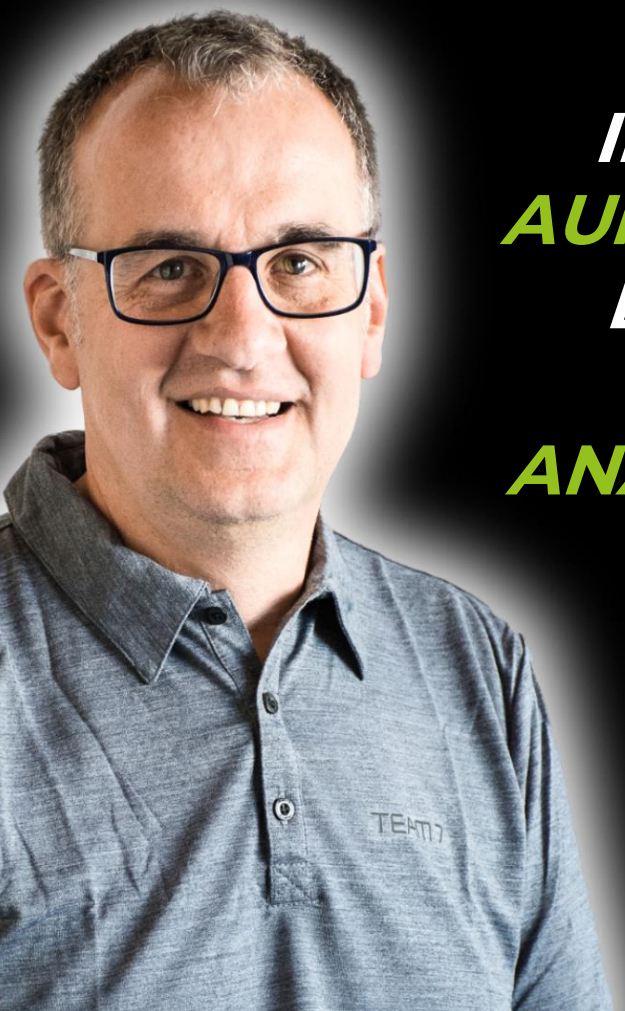
3

*24x7 Überwachung und umgehende Reaktion auf potenzielle Bedrohungen.*

*Kontinuierliche Überwachung und Betrieb der IT-Sicherheit durch Managed Service Security.*

4

**Rundum-Schutz**

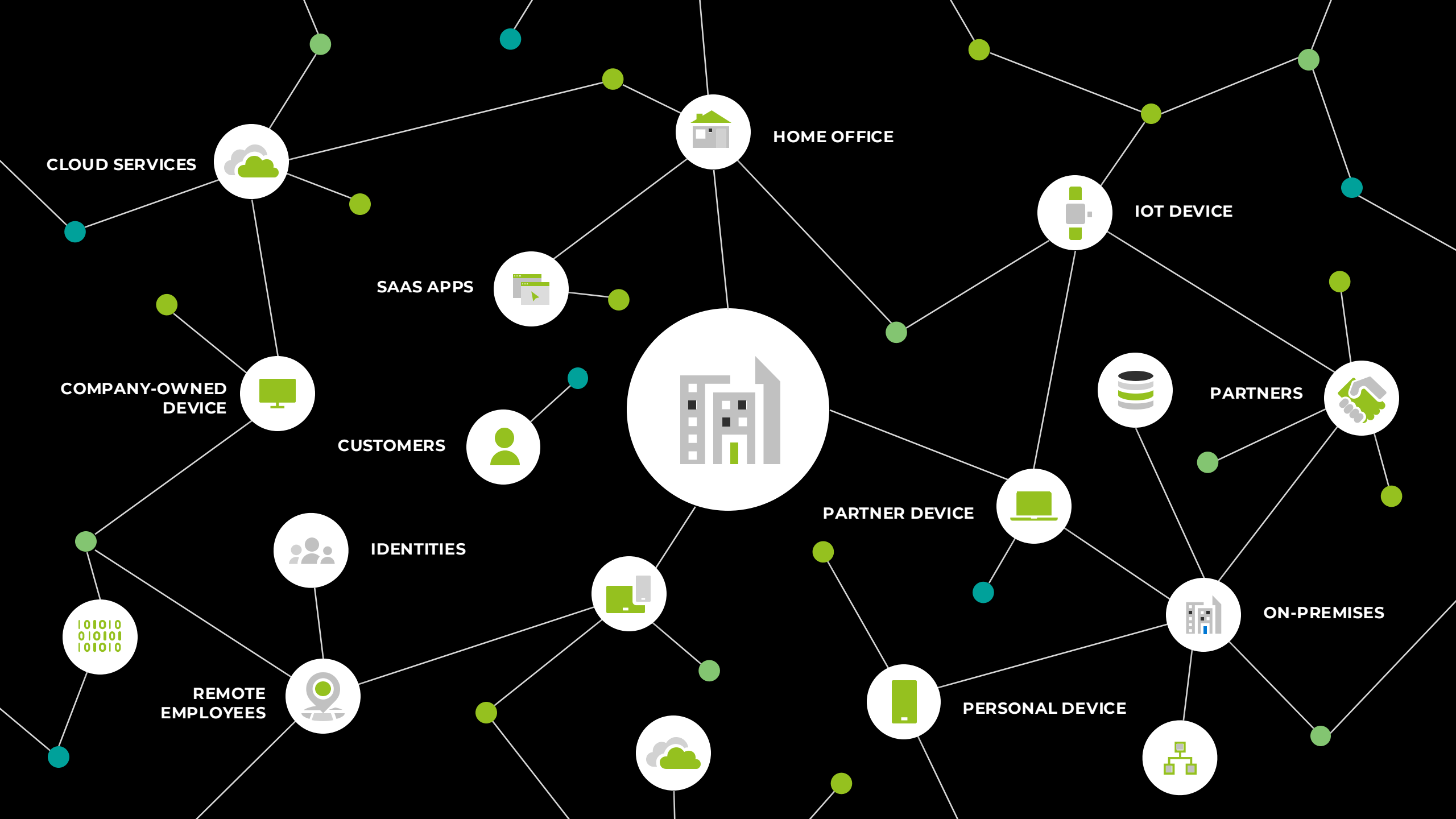


„DANK DER 24X7-BETREUUNG DURCH BASE-IT VERFÜGEN WIR ÜBER EINE MODERNE, LEISTUNGSFÄHIGE IT-SICHERHEITSLANDSCHAFT, DIE UNSERE INFRASTRUKTUR ZUVERLÄSSIG SCHÜTZT – AUCH AUßERHALB DER GESCHÄFTSZEITEN. POTENZIELLE BEDROHUNGEN WERDEN FRÜHZEITIG ERKANNT UND ABGEWEHRT. REGELMÄßIGE AUDITS, ANALYSEN UND OPTIMIERUNGEN STELLEN SICHER, DASS DAS SICHERHEITSNIVEAU STETS AKTUELL BLEIBT. ZIEL IST ES, BEI EVENTUELLEN ANGRIFFEN EFFEKTIV ZU REAGIEREN."

**- Karl-Heinz Voglsperger**
IT-Koordinator Technik bei TEAM 7 Österreich GmbH

base it

# MICROSOFT SECURITY LÖSUNGEN


CLOUD SERVICES
HOME OFFICE
IOT DEVICE
SAAS APPS
COMPANY-OWNED DEVICE
CUSTOMERS
PARTNERS
PARTNER DEVICE
IDENTITIES
ON-PREMISES
REMOTE EMPLOYEES
PERSONAL DEVICE

# ZERO TRUST
## SCHÜTZEN SIE IHR UNTERNEHMEN

VERIFY EXPLICITLY | USE LEAST-PRIVILEGED ACCESS | ASSUME BREACH

# MICROSOFT SECURITY TECHNOLOGIE

## 4 LÖSUNGSBEREICHE

### Identity and Access Management

Sicherer Zugriff für eine vernetzte Welt

### Threat Protection

Stoppen Sie Angriffe mit integriertem, automatisiertem SIEM und XDR

### Information Protection

Schützen Sie sensible Daten und minimieren Sie Insider-Risiken mit intelligenter Technologie.

### Cloud Security

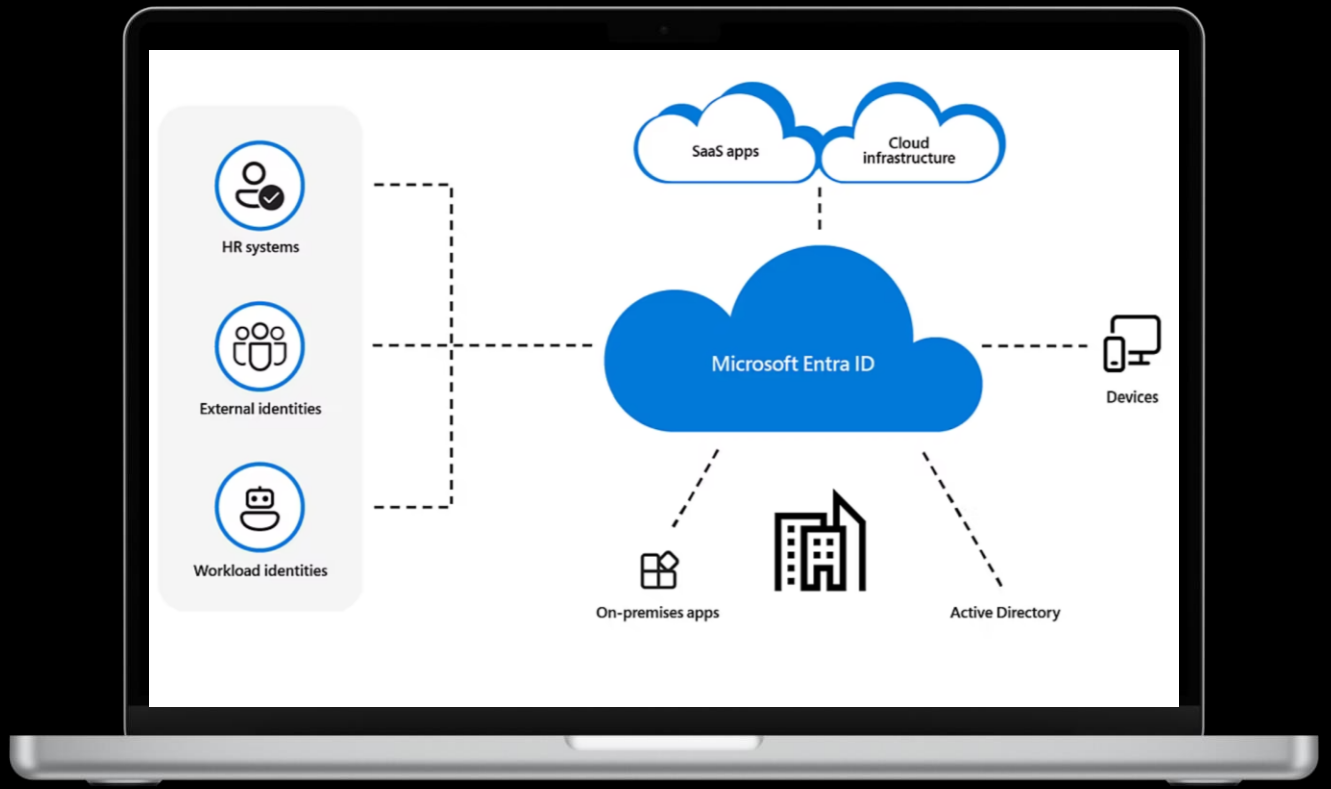
Schützen Sie Ihre Multi-Cloud-Ressourcen.

# MICROSOFT ENTRA ID
## DIE WICHTIGSTEN FUNKTIONEN ERKLÄRT

- **Conditional Access (CA):** der Zugriff auf Unternehmensressourcen wird nur unter bestimmten Bedingungen erlaubt. Automatisierte Richtlinienreduzieren den Verwaltungsaufwand und erleichtern gleichzeitig die Einhaltung von Compliance-Vorgaben. Zudem ermöglicht es eine flexible Anpassung an unterschiedliche Sicherheitsanforderungen.

- **Multi Faktor Authentication (MFA):** Microsoft Entra bietet verschiedene Authentifizierungsmethoden, darunter kennwortlose Optionen wie Windows Hello, Passkeys (FIDO2), Zertifikate und die Microsoft Authenticator-App.

- **Global Secure Access (GSA):** bietet einen sicheren und flexiblen Zugriff auf Unternehmensressourcen. Es integriert Zero Trust Network Access und Secure Web Gateway, um Bedrohungen effektiv zu erkennen und abzuwehren. Zudem ermöglicht es eine zentrale Verwaltung und Überwachung von Sicherheitsrichtlinien.



# MICROSOFT ENTRA ID
## ALLE FUNKTIONEN

### Entra ID P1

- Advanced Security Reports & Alerts
- App Proxy incl. PingAccess
- Cloud App Discovery
- Conditional Access
- Custom Security Attributes
- Customized Sign-in-Page
- Dynamic Groups
- Enterprise State Roaming
- External ID & Verified ID
- Entra ID Connect Health
- Microsoft Identity Manager
- Password Protection
- Administrative Units
- Multi-Factor Auth. (MFA)
- Passwordless Authentication
- 3rd Party MFA Integration
- Self-Service Group Management
- Self-Service Password Reset in AD
- Self-Service Activity Reports
- Service Level Agreements (SLA)
- Shared Account Password Rollover
- Single-Sign-On to other SaaS
- SMS Sign-In
- Temporary Access Pass
- Terms of Use
- Windows Autopilot

### Entra ID P2

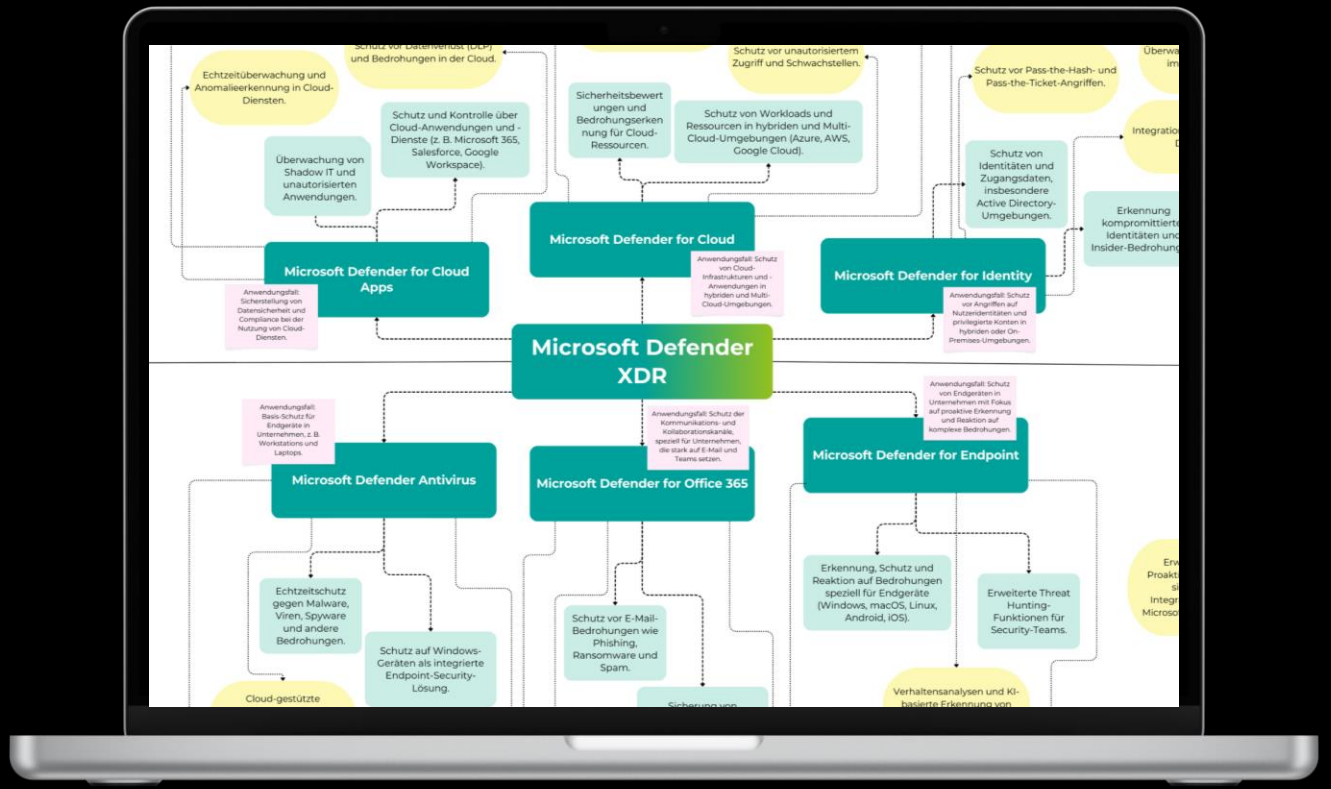
Zusätzlich zu P1:

- Access Reviews
- Entra ID Protection
- MFA Registration Policy
- Entitlement Management
- Privileged Identity Management
- Risk-Based Conditional Access

# MICROSOFT DEFENDER XDR

## DIE WICHTIGSTEN FUNKTIONEN ERKLÄRT

- **Defender for Endpoint (MDE)**: umfassenden Schutz vor modernen Bedrohungen durch fortschrittliche Erkennung und Abwehrmechanismen. Zudem nutzt es KI, um Bedrohungen zu identifizieren und zu bekämpfen.
- **Defender for Identity (MDI):** umfassenden Schutz vor Identitätsbedrohungen, indem es Verhaltensanalysen nutzt, um ungewöhnliche Aktivitäten und Anomalien in **Benutzerkonten** zu erkennen.
- **Defender for Office (MDO)**: Schutz vor Bedrohungen in E-Mails, Links und Dateianlagen, indem es fortschrittliche Filter- und Erkennungstechnologien nutz. Es integriert sich nahtlos in Microsoft 365 und schützt nicht nur E-Mails, sondern auch Tools wie Microsoft Teams und SharePoint vor Cyberangriffen.
- **Defender for Cloud Apps**: überwacht und schützt Cloud-Anwendungen durch die Erkennung und Abwehr von Bedrohungen sowie die Verwaltung von Sicherheitsrichtlinien.



# MICROSOFT DEFENDER
## ALLE FUNKTIONEN

### MS Defender for Endpoint P1

- Block at First Sight
- Centralized Management
- Cross-Platform Support
- Enhanced ASR
- Manual Response Actions
- Mobile Threat Defence
- Next Gen Protection
- Tamper Protection
- Web Content Filtering

### MS Defender for Endpoint P2

Zusätzlich zu P1:

- Advanced Hunting
- Automated Investigations
- Defender for Cloud App Integration
- Endpoint Attack Notifications
- Endpoint Detection & Response
- Evaluation Lab
- MIP Integration
- Threat Analytics
- Vulnerability Management

### MS Defender Antivirus

- Pattern-based virus protection
- Basic protection

# MICROSOFT DEFENDER
## ALLE FUNKTIONEN

### MS Defender for Identity

- Erkennung abnormaler Anmeldeverhalten
- Kontrolle von Anmeldungen, VPN-Verbindungen usw.
- Honeytoken Aktivitäten

### MS Defender for Office 365

- Schutz vor Phishing und Zero-Day-Malware durch Analyse von E-Mails, Dateien in OneDrive, Teams und SharePoint
- Sichere Links, sichere Anhänge
- Schutz aller Office 365-Daten

### MS Defender for Cloud Apps

- Kontrolle über Cloud-Apps und Dateien innerhalb von SaaS-Anwendungen in der Cloud
- Erkennung von Bedrohungen
- Analyse des Nutzerverhaltens
- Kontrolle über die Nutzung von SaaS-Anwendungen

### MS Defender for Cloud

- SQL
- Storage
- Cosmos Database
- Network Layer
- Key Vault
- Management APIs
- Azure App Service
- Database for MySQL / PostgreSQL
- Kubernetes Service
- Host level
- Container Registry – Images
- Recommendations & Assessments
- Secure Score & Benchmarks
- Coverage (Onpremise & Azure)
- Threat Protection
- Vulnerability assessment

# MICROSOFT SENTINEL (SIEM)
## DIE WICHTIGSTEN FUNKTIONEN IM DETAIL

- **Skalierbare Datenerfassung:** Sammelt Daten von Benutzern, Geräten, Anwendungen und Infrastrukturen, sowohl lokal als auch in mehreren Clouds.
- **Bisher unentdeckte Bedrohungen ermitteln** und fälschlicherweise positive Ergebnisse mithilfe von Analysefunktionen und der unvergleichlichen Threat Intelligence von Microsoft minimieren.
- **Bedrohungen mit KI untersuchen** und verdächtige Aktivitäten nach Bedarf verfolgen – profitieren Sie dabei von der jahrzehntelangen Erfahrung von Microsoft in Sachen Cybersicherheit.
- **Mit integrierter Orchestrierung und Automatisierung** häufiger Aufgaben schnell auf Vorfälle reagieren.

# CSP LICENSING
## OPTIONEN

| PRODUKT | Option #1 | Option #2 | Option #3 |
|---|---|---|---|
| Entra ID P1 | Jährliche Bindung und Vorauszahlung | Jährliche Bindung und monatliche Zahlung | Monatliche Bindung und monatliche Zahlung |
| Entra ID P2 | | | |
| MS Defender for Endpoint P1 | | | |
| MS Defender for Endpoint P2 | | | |
| MS Defender for Identity | | | |
| MS Defender for Office 365 | | | |
| MS Defender for Cloud Apps | | | |
| Microsoft 365 E5 Security | | | |
| Enterprise Mobility & Security E3 (EMS E3) | | | |
| Upgrade auf EMS E5 (bei vorhandener EMS E3 Lizenz) | | | |
| Upgrade auf Microsoft 365 E5 (bei vorhandener M365 E3 Lizenz) | | | |
| MS Defender for Cloud | Verrechnung nach Aufwand durch das Azure Plan-Abonnement | | |
| MS Sentinel | Verrechnung nach Aufwand durch das Azure Plan-Abonnement | | |

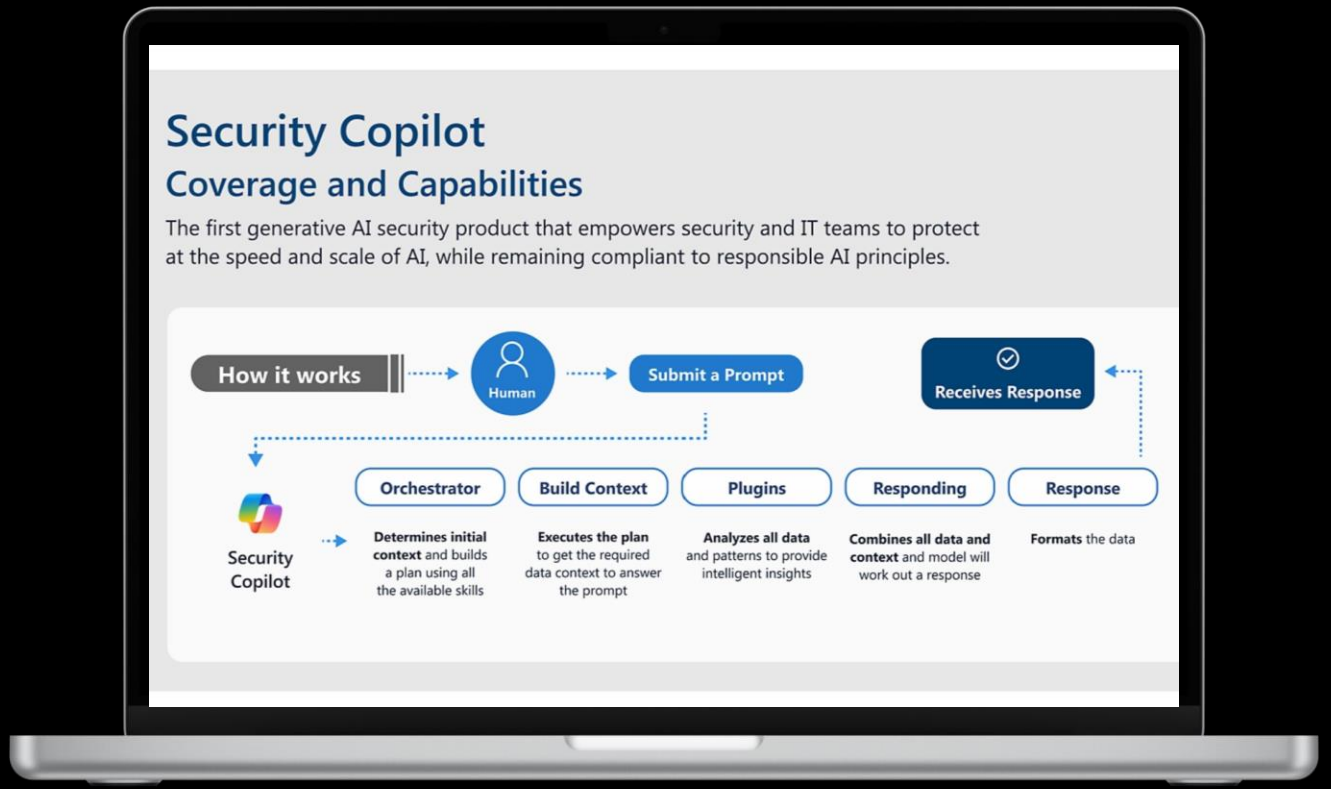
*Stand September 2025

base it

# SECURITY COPILOT

# SECURITY COPILOT
## SICHER MIT KI

- **KI-gestützte Sicherheitsanalysen**: Security Copilot nutzt generative KI, um Sicherheitsanalysen zu unterstützen und Bedrohungen schneller zu erkennen und zu bewältigen.
- **Integration mit Microsoft-Diensten:** Es lässt sich nahtlos in andere Microsoft-Sicherheitsdienste und Drittanbieterdienste integrieren, was eine umfassende Sicherheitslösung ermöglicht.
- **Echtzeit-Einblicke:** Es bietet Echtzeit-Einblicke und detaillierte Beschreibungen von Angriffen, betroffenen Systemen und Ereigniszeitlinien, um schnelle und gezielte Maßnahmen zu ermöglichen.
- **Benutzerfreundlichkeit:** Security Copilot ist darauf ausgelegt, Sicherheits- und IT-Experten durch eine intuitive Benutzeroberfläche und klare, umsetzbare Schritte zu unterstützen



base it

# ZUFRIEDENE KUNDEN

# REFERENZEN
## MANAGED SERVICE SECURITY & SOC

**Daniel Emmrich [Mitglied der Geschäftsleitung | Dr. Wieselhuber & Partner GmbH]**
„Die Zusammenarbeit mit Base-IT – sowohl während des Projekts als auch in der fortlaufenden Betreuung – ist ausgezeichnet. Schnelle Reaktionszeiten, kompetente und zielgerichtete Lösungsvorschläge und Umsetzung dieser zeichnen unsere Zusammenarbeit aus. Base-IT ist – sofern wir es beurteilen können – absolut „State of the art“ und ist dadurch der perfekte Partner für uns im Bereich Cyber Security. Die Zusammenarbeit ist eine perfekte Mischung aus partnerschaftlichem Miteinander, Freude und Sensibilisierung für die Herausforderungen geprägt. Wir freuen uns auf die weitere Zusammenarbeit.“

**Matthias Klinski [Chief Information Security Officer | SWIETELSKY AG]**
„Bei der Auswahl des Managed Security Operation Center Services waren für uns zwei Dinge entscheidend: State-of-the-Art Technologien und Transparenz im erbrachten Service. Der Managed Service Security der Base-IT vereint diese zwei Aspekte perfekt, indem die neuesten Microsoft Security Produkte gemeinsam durch uns Swietelskys sowie Experten der Base-IT betreut werden. Mit dieser Basis und dem daraus resultierenden kontinuierlichen voneinander lernen, sind wir bestens gewappnet um das „moving target“ Cyber Security nachhaltig anzugehen.“

# REFERENZEN
## VIELE WEITERE AUF UNSERER WEBSITE

**Bernhard Oberndorfer**
**[Head of Workplace Service | Salzburg AG]**
„Um als interne IT-Abteilung das Unternehmen weiterhin bestmöglich unterstützen und vor Cyberangriffen schützen können, ist die Einführung neuer Technologien, insbesondere im Security-Bereich, absolut notwendig. Mit der base-IT haben wir einen Partner gefunden, der uns dabei bestens unterstützt und bei dringlichen Angelegenheiten immer zur Verfügung steht.“


www.baseit.at/referenzen

base it

Haider Straße 23 | 4052 Ansfelden | AT

+43 7229 87800 - 0 | office@baseit.at |

www.baseit.at

Base-IT GmbH (unserebroschuere.at)

Certified to ISO/IEC 27701:2019

Certified to ISO/IEC 27001:2022

Microsoft Solutions Partner