base it

professional.
fast.
secure.

WER WIR SIND

Base-IT auf einen Blick.

EXCELLENCE WIRD BEI UNS NEU DEFINIERT.

WIR

- Gründer:
  Gregor Dedl
  Christoph Moser
- seit 2010
- 130 engagierte Mitarbeiter/innen (96 Consultants)
- Standorte:
  Ansfelden | Wien | Salzburg
- ISO/IEC 27001-2013 zertifiziert
- FY 2021/22 Umsatz:
  23,52 M€

UNSERE WERTE

Der Kunde steht im Mittelpunkt unseres Handelns.

Knowhow & individueller Service sind unsere Markenzeichen.

UNSERE KUNDEN

Über 300 zufriedene Kunden in Österreich & in angrenzenden Ländern

KMUs, Konzerne, alle Branchen

Consulting & Beratung | Managed Service & Betreuung | Cloud Services | On Premise-Datacenter

UNSER PORTFOLIO

Was wir anbieten.

Microsoft 365 / Office 365
Microsoft Azure
Security (M365 & Azure)
Compliance (M365)

Cloud Services

On Premise Datacenter

Server / Storage
Virtualisierung
Backup
Network & Security
Management & Monitoring
Automatisierung

Projektumsetzungen
IST-Analyse & IT Strategie
Konzeption
Migrationsplanungen
Projektmanagement
Technische Schulungen
Lizenz-Beratung (CSP)

Consulting

Operations Support Managed Service

Datacenter Support
Datacenter Outsourcing
Managed Service
Security Operation Center
Client Service Desk
11x5 / 24x6 / 24x7

MICROSOFT PARTNER

Base-IT – Ihr CSP Partner

Microsoft Solutions Partner
Modern Work

Microsoft Solutions Partner
Security

Microsoft Gold Partner

- jahrelange Erfahrung in der Umsetzung und im Betrieb von Microsoft Produkten
- professionelle Beratung & Unterstützung durch unsere Base-IT Experten für eine optimale Lizenzstrategie & ein ideales Wachstum
- Zahlreiche Kompetenzen und gut ausgebildete Consultants
- bestehende & fortlaufende Zertifizierungen

Microsoft Competencies:

- Cloud Productivity
- Application Integration
- Enterprise Mobility Management
- Datacenter
- Windows & Devices
- Cloud Platform
- Small & Midmarket Cloud Solutions
- Collaboration and Content
- Security
- Application Development

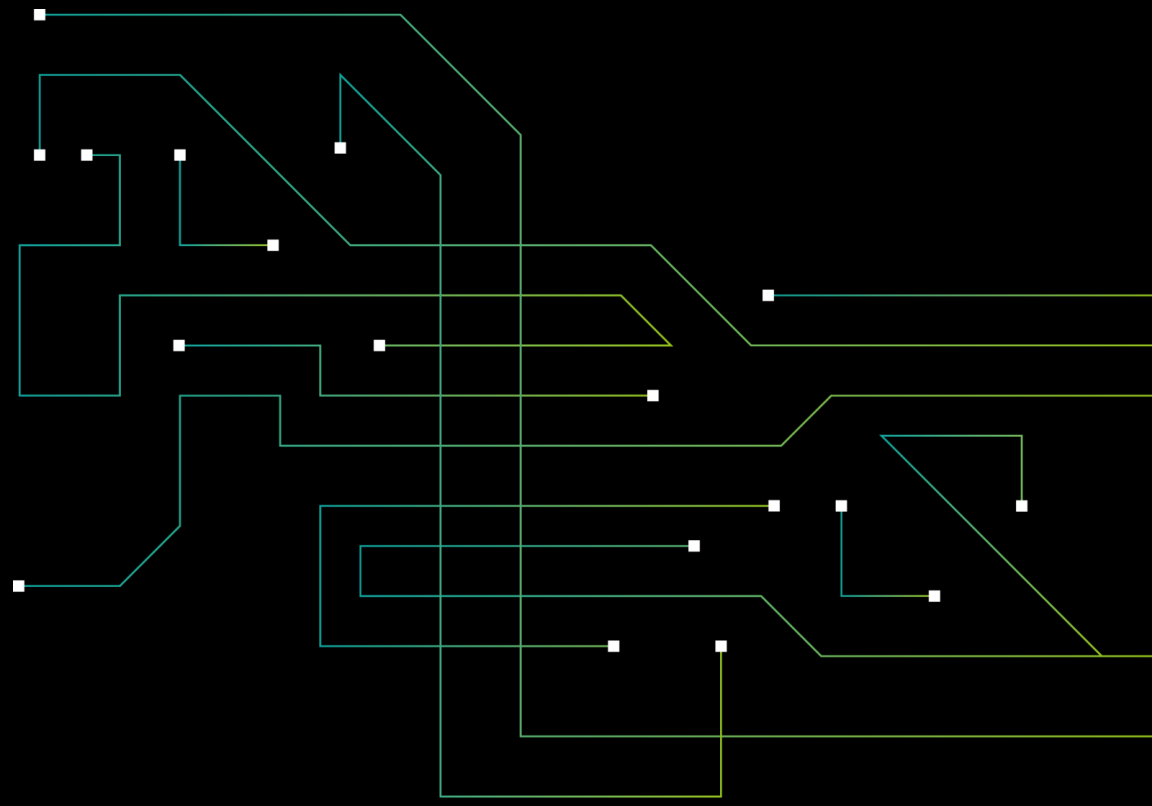
REFERENZEN

Viele zufriedene Kunden.

basg it

base it

BASE-IT MANAGED SERVICE SECURITY & SOC



Vollumfassende IT-Sicherheit für Ihre Microsoft 365 Cloud-Dienste

professional.
fast.
secure.

SICHER VOR CYBERKRIMINALITÄT

PROAKTIVE und PROFESSIONELLE Betreuung, auf Wunsch Rund-um-die-Uhr

Für jedes Unternehmen ist ein exzellenter Schutz von eigenen Kommunikations- und Datennetzwerken, Unternehmens-Ressourcen, sensiblen Daten und vielem mehr essentiell. Besonders in Zeiten, in denen die Cyberbedrohungen steigen und einzelne Angriffe zum Teil sehr professionell umgesetzt werden, ist eine umfassende IT-Sicherheit unabdingbar.

Das betrifft jedes Unternehmen, jede Branche, jede Unternehmensgröße – die digitale Welt birgt Risiken, aber wir wissen, wie wir Sie vor diesen Cyberbedrohungen schützen können!

IHRE HERAUSFORDERUNGEN

- Cyberbedrohungen
- Ressourcenmangel
- IT-Security Awareness
- Skalierbarkeit
- Kostentransparenz
- …

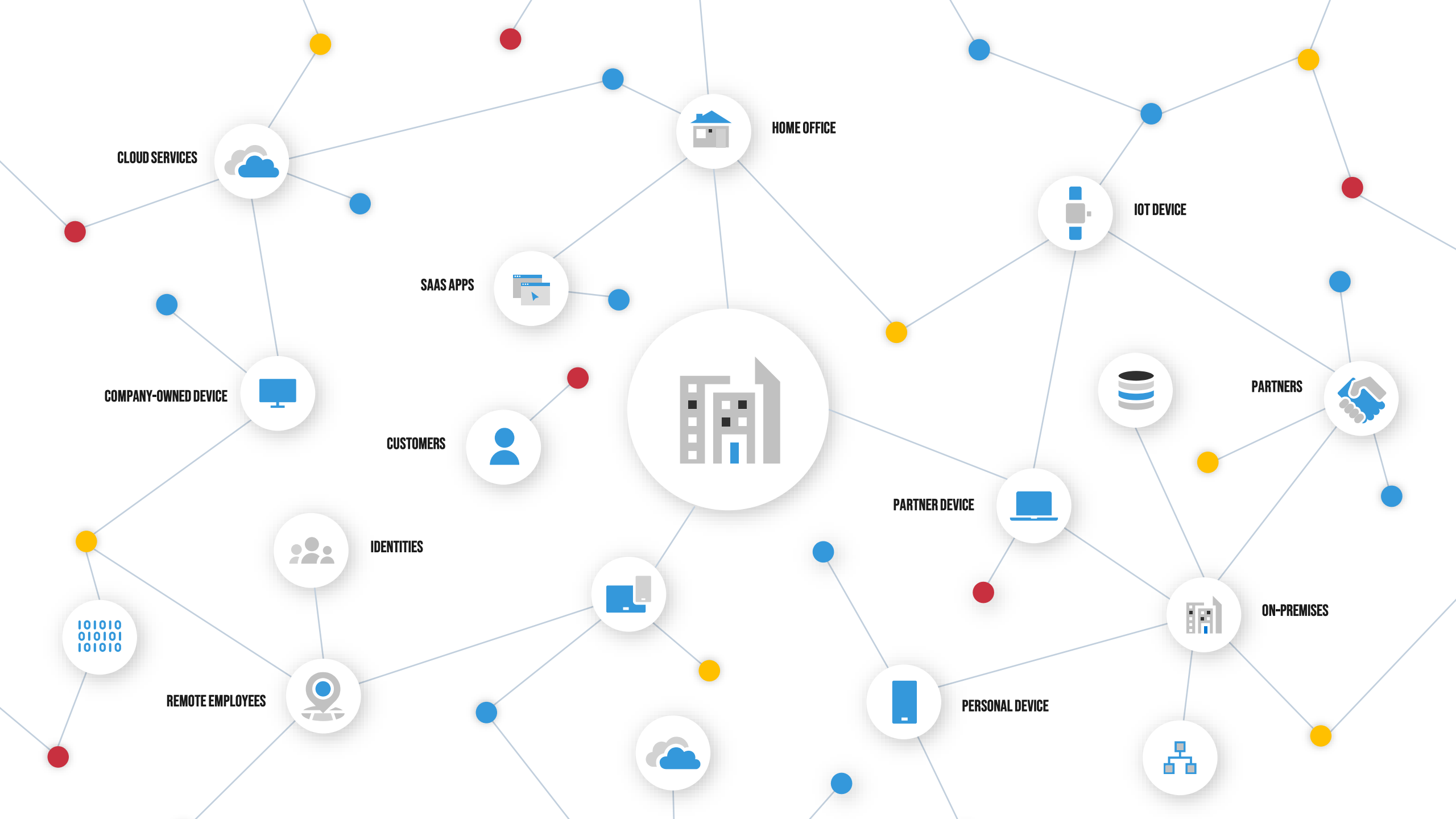
UNSERE BASE-IT LÖSUNG

- Base-IT
  Managed Service Security & SOC
  24x7 | 24x6 | 11x5
- M365 E3 | E5 | Defender for Cloud | Microsoft Sentinel | Complete
- Verwendung von innovativen Security-Lösungen der Microsoft

IHRE BENEFITS

- IT-Sicherheit auf höchsten Niveau
- Ideale Skalierbarkeit
- Absolute Kostentransparenz
- Operativer Betrieb durch uns und Betreuung auf Basis von Microsoft Security Lösungen

Schützen Sie Ihre Microsoft 365-Umgebung mit Base-IT Managed Service Security & SOC!


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

SECURING YOUR ORGANIZATION WITH ZERO TRUST

VERIFY EXPLICITLY | USE LEAST-PRIVILEGED ACCESS | ASSUME BREACH

MICROSOFT SECURITY TECHNOLOGY

IDENTITY AND ACCESS MANAGEMENT

SECURE ACCESS FOR A CONNECTED WORLD

THREAT PROTECTION

STOP ATTACKS WITH INTEGRATED, AUTOMATED SIEM AND XDR

INFORMATION PROTECTION

PROTECT SENSITIVE DATA AND MANAGE INSIDER RISKS WITH INTELLIGENCE

CLOUD SECURITY

SAFEGUARD YOUR MULTI-CLOUD RESOURCES

ESSENTIAL PARTS OF MANAGED SERVICE SECURITY

reactive Alerthandling
24x7

proactive Operations
& Servicing

Forensic Analysis
& centralized Logging

MANAGED SERVICE SECURITY OVERVIEW

base it

Managed Services Security Products

Azure AD Premium
Defender AV

Defender for Endpoint
Defender for Identity
Defender for O365
Defender for Cloud Apps

Defender for Cloud
Microsoft Sentinel

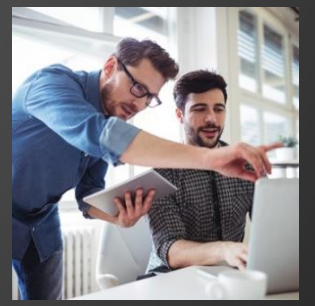
To be extended…

Security Operation Center

24x7
24x6
11x5

Managed Service Bundles

M365 Security E3 / E5
Azure Security
complete



MANAGED SERVICE SECURITY PRODUCTS
M365 E3/E5 SECURITY

basc it

Managed Service Security Products

Azure AD Premium P1

- Advanced Security Reports & Alerts
- App Proxy, inc. PingAccess
- Azure AD B2B
- Azure AD Connect Health
- Azure AD Password Protection
- Cloud App Discovery
- Conditional Access
- Multi-Factor Auth. (MFA)
- Self-Service Password Reset in AD
- Self-Service Group Management
- Shared Account Password Roll-Over
- Single-Sign-On to other SaaS
- Terms of Use
- 3rd Party MFA Integration

Azure AD Premium P2

- Access Reviews
- Azure Identity Protection
- Entitlement Management
- Privileged Identity Management
- Risk-Based Conditional Access

Defender for AV

- “Windows Defender Anti-Virus”
- Pattern-based virus protection
- Basic protection

Defender for Endpoint

- Adv. functionalities as Windows Defender
- Analyzes of behavior in order to recognize anomalies
- Ability of detecting new viruses/zero Day
- Threat & Vulnerability Management
- Endpoint Detection & Response

MANAGED SERVICE SECURITY PRODUCTS
M365 E3/E5 SECURITY

basg it

Managed Service Security Products

Defender for Identity

- Detection of abnormal Logon behavior
- Control of logins, VPN connections, etc.
- Honeytoken activities

Defender for O365

- Protection from phishing and zero-day-malware through analyzes of e-mails, files on OneDrive, Teams and SharePoint
- Safe links, safe attachments
- Protect all Office 365 Data

Defender for Cloud Apps

- Control over cloud apps & files within SaaS application in the cloud
- Detection of threats
- analyzes of behavior
- Block & Control usage of SaaS applications

MANAGED SERVICE SECURITY PRODUCTS
AZURE SECURITY

basc it

Managed Service Security Products

Defender for Cloud

- SQL
- Storage
- Cosmos Database
- Network Layer
- Key Vault
- ARM – Management APIs
- Azure App Service
- Database for MySQL/PostgreSQL

Defender for Cloud

- Recommendations & Assessments
- Secure Score & Benchmarks
- Coverage (Onpremise & Azure)
- Threat Protection
- Vulnerability assessment

Defender for Cloud

- Kubernetes Service
- Host level
- Container Registry - Images

Microsoft Sentinel (SIEM)

- Collection and analyses of data of users, applications, server, network devices from several sources such as on-premise and cloud
- AI and machine learning analyze data

MANAGED SERVICE MICROSOFT 365 E3 / E5

M365 E3

- Azure AD Premium P1
- MS Defender AV
- MS Defender for Endpoint P1

M365 E5

- Azure AD Premium P1
- Azure AD Premium P2
- MS Defender AV
- MS Defender for Endpoint
- MS Defender for Identity
- MS Defender for O365
- MS Defender for Cloud Apps

To be extended to future product / bundle updates.

Proactive Operation and Servicing

- Weekly system-check off all solutions
- Handling of alerts in weekly system-check
- Continuous discussion with customer to guarantee service quality
- Adopting new features and functionality
- Service reports
- working on defined goals to reach secure score targets

Security Operation Center (11x5 / 24x6 / 24x7)

- High Alerts - Alerting to base-IT SoC
- Alert-handling based on customer agreement
- monthly alert reports
- SLA for Alert Handling

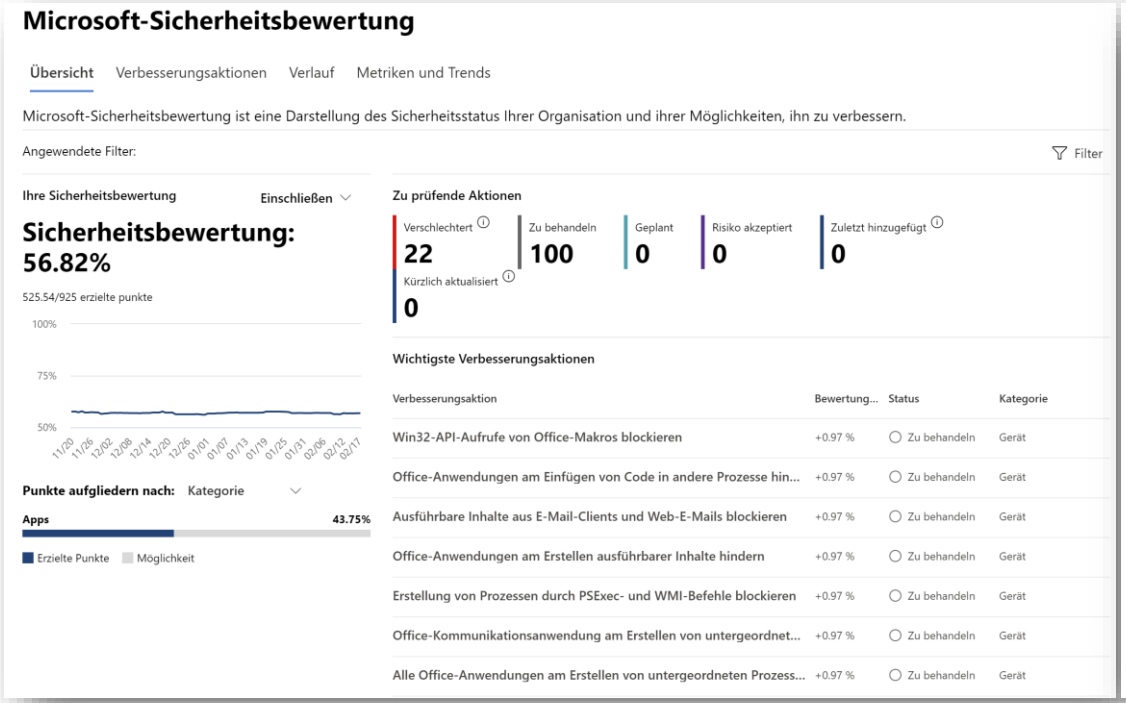
SECURITY OPERATION CENTER
REACTION CATALOG

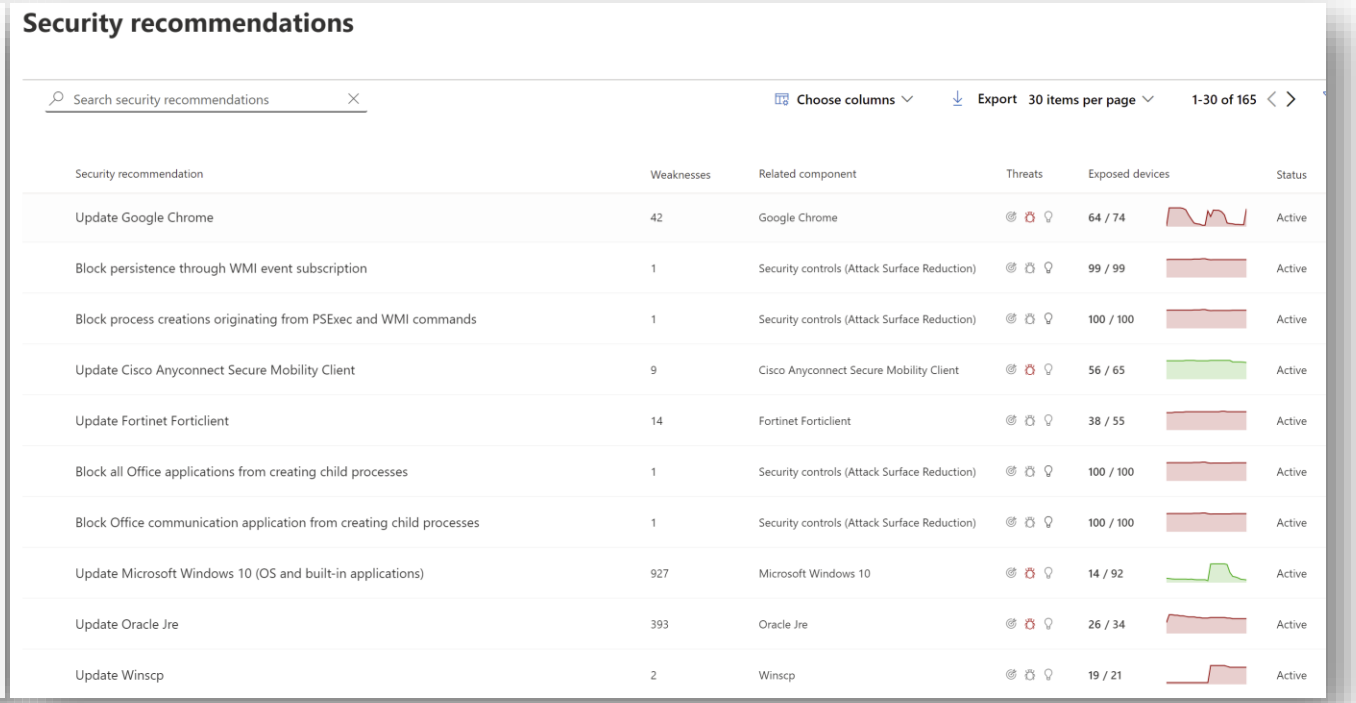
base it

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
Defender for Identity	Honeytoken Activity(von Server aus)	nicht zutreffend	Mit Kunde Abstimmen ob der Alert durch eine Software (LDAP-Abfrage) gemacht wurde	nicht zutreffend	nicht zutreffend
Defender for Identity	Honeytoken Activity(von Client	nicht zutreffend	Client im Defender for Endpoint prüfen, Falls Auffälligkeiten vorhanden - Prüfen ob bereits eine Automatic Investiagtion	nicht zutreffend	nicht zutreffend

MANAGED SERVICE SECURITY
SECURE SCORE – PROACTIVE TARGETS

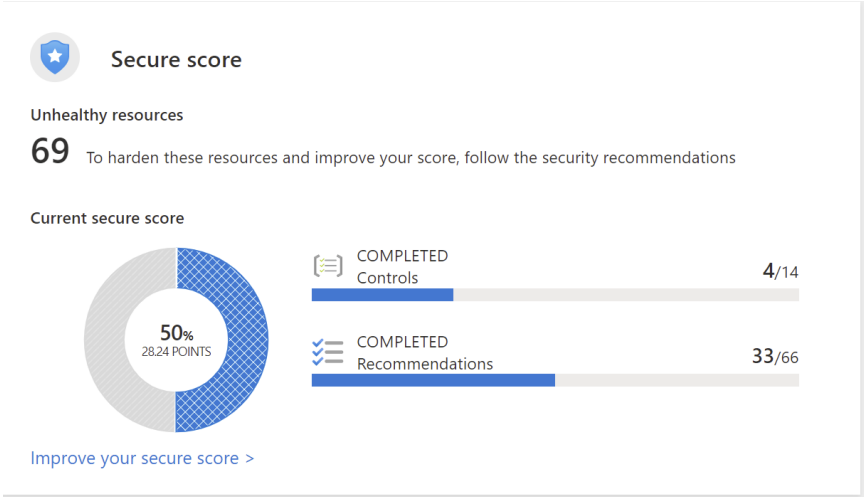
basg it

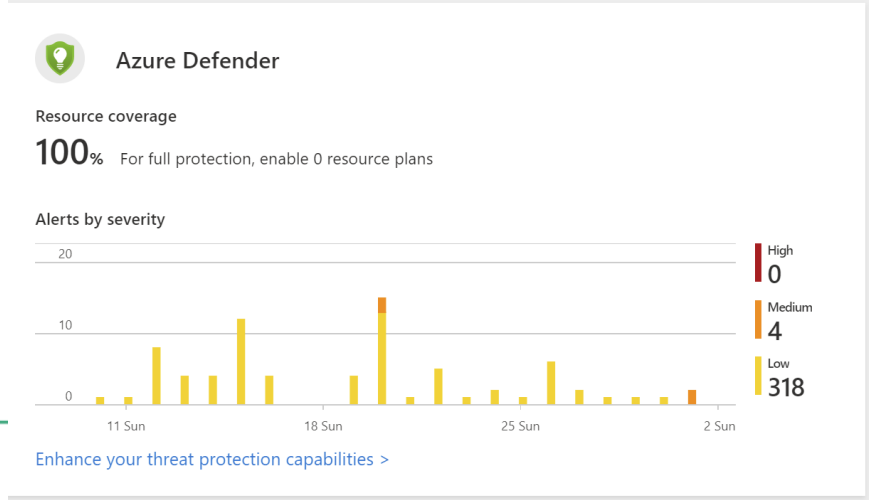




In proactive operations management, the recommendations from the Microsoft Security solutions are continuously analyzed and coordinated with the customer. Depending on the scope, topics for optimizing security are implemented at short notice in the course of the managed service or defined as a separate project and released by the customer.

MANAGED SERVICE SECURITY
SECURE SCORE – PROACTIVE TARGETS





Controls	Max score	Current Score	Potential score increase	Unhealthy resources	Resource health
Enable MFA	10	0	+ 18% (10 points)	1 of 1 resources	
Secure management ports	8	3.64	+ 8% (4.36 points)	6 of 12 resources	
Remediate vulnerabilities	6	1.09	+ 9% (4.91 points)	9 of 14 resources	
Apply system updates	6	5.43	+ 1% (0.57 points)	2 of 22 resources	
Remediate security configurations	4	0.57	+ 6% (3.43 points)	18 of 24 resources	
Enable encryption at rest	4	1.82	+ 4% (2.18 points)	6 of 15 resources	
Restrict unauthorized network access	4	2.91	+ 2% (1.09 points)	3 of 12 resources	

Im proaktiven Betriebsmanagement werden die Empfehlungen aus den Microsoft Security-Lösungen kontinuierlich analysiert und mit dem Kunden abgestimmt. Je nach Umfang werden Themen zur Optimierung der Sicherheit kurzfristig im Rahmen des Managed Service umgesetzt oder als eigenes Projekt definiert und vom Kunden freigegeben.

MANAGED SERVICE SECURITY
SECURE SCORE – PROACTIVE TARGETS

basg it

Microsoft-Sicherheitsbewertung – Microsoft 365 Security

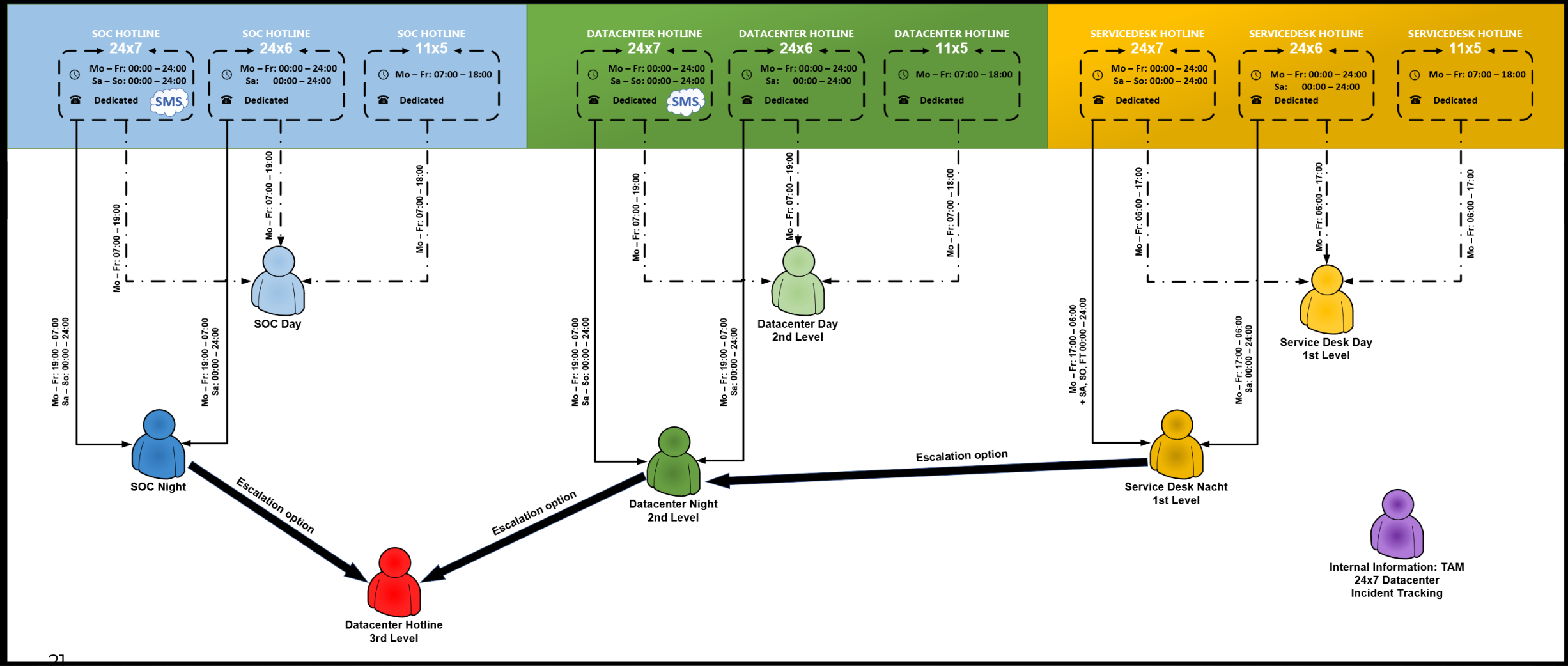
Security recommendations – Microsoft 365 Security

Identity Secure Score - Microsoft Azure

Security Center - Microsoft Azure

BASE-IT 24X7 SERVICES (INCLUDING SOC)

base it



MANAGED SERVICE AZURE SECURITY

To be extended to future product / bundle updates.

Defender for Cloud

(Azure Defender for Server + Azure Security Center)

Azure Defender for Services | Azure Defender for IoT | Azure Defender for Container Registries | Azure Defender for App Service | Azure Defender for Storage | Azure Defender for Kubernetes | Azure Defender for Key Vault | Azure Defender for SQL

Microsoft Sentinel

Proactive Operation and Servicing

- Weekly system-check off all solutions
- Handling of alerts in weekly system-check
- Continuous discussion with customer to guarantee service quality
- Adopting new features and functionality
- Service reports
- working on defined goals to reach secure score targets

Security Operation Center (11x5 / 24x6 / 24x7)

- High Alerts - Alerting to base-IT SoC
- Alert-handling based on customer agreement
- Monthly alert reports
- SLA for Alert handling

MANAGED SERVICE SECURITY COMPLETE

To be extended to future product / bundle updates.

Proactive Operation and Servicing

- Weekly system-check off all solutions
- Handling of alerts in weekly system-check
- Continuous discussion with customer to guarantee service quality
- Adopting new features and functionality
- Service reports
- working on defined goals to reach secure score targets

Security Operation Center (11x5 / 24x6 / 24x7)

- High Alerts - Alerting to base-IT SoC
- Alert-handling based on customer agreement
- Monthly alert reports
- SLA for Alert Handling

MANAGED SERVICE SECURITY SUMMARY

Managed Service Security	M365 E3	M365 E5	Azure Defender	Azure Sentinel	Security complete
Offer except licenses & travel expenses for services on-site					
Azure AD Premium P1	*	*			*
Microsoft Defender AV	*	*			*
Azure AD Premium P2		*			*
MS Defender for Endpoint		*			*
MS Defender for Identity		*			*
MS Defender for O365		*			*
MS Defender for CloudApps		*			*
MS Defender for Cloud			*		*
Microsoft Sentinel				*	*

Response time / on-call time		
Default response time - best effort	€	n/a
11x5 - 60min response time	€	350,00
24x6 - 60min response time	€	800,00
24x7 - 60min response time	€	1.300,00

CSP LICENSING OPTIONS

CSP License Prices*			
Azure AD Premium P1	€	4.5	per user/month
Azure AD Premium P2	€	6.78	per user/month
Microsoft Defender for Endpoint	€	3.89	per user/month
Microsoft Defender for Identity	€	4.11	per user/month
Microsoft Defender for O365	€	1.5	per user/month
Microsoft Defender for Cloud Apps	€	2.62	per user/month
Microsoft 365 E5 Security	€	9	per user/month
Enterprise Mobility & Security E3 (EMS E3)	€	6.55	per user/month
Upgrade to EMS E5 (given best EMS E3 license)	€	4.55	per user/month
Upgrade to Microsoft 365 E5 (given best Microsoft 365 E3 license)	€	20.17	per user/month
Azure Defender		charged based on effort	through Azure Plan Subscription
Microsoft Sentinel		charged based on effort	through Azure Plan Subscription

* License prices as of February 2021

* License prices are subject to change

BASE-IT MANAGED SERVICE SECURITY & SOC

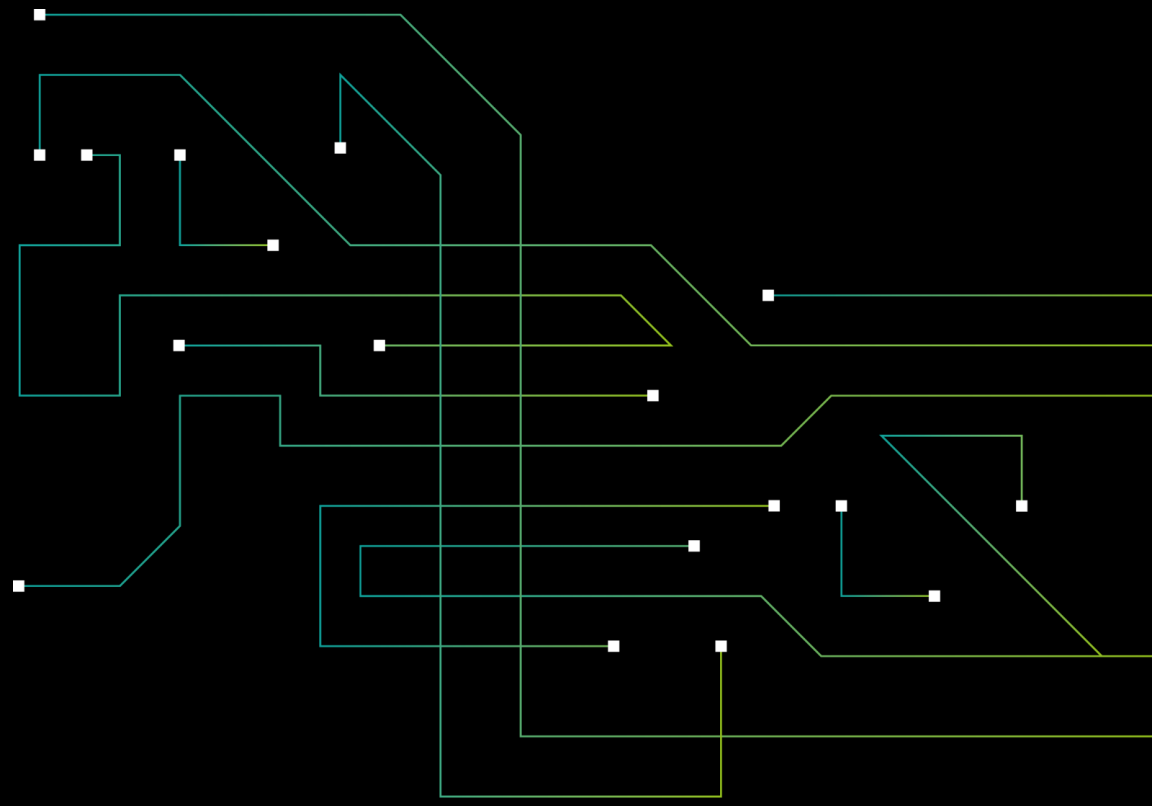
Perfektes Zusammenspiel zwischen Ihren Anforderungen und unseren Lösungen.

SUPPORT PACKAGES

Consulting & Beratung | Managed Service & Betreuung | Cloud Services | On Premise-Datacenter

base it

UNSERE REFERENZEN



professional.
fast.
secure.

BASE-IT MSS & SOC KUNDEN

Unsere Kunden verlassen sich auf unser Managed Service Security & SOC

Klaiton

SWIETELSKY

Dr. Wieselhuber & Partner GmbH
Unternehmensberatung

UND VIELE MEHR...

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."

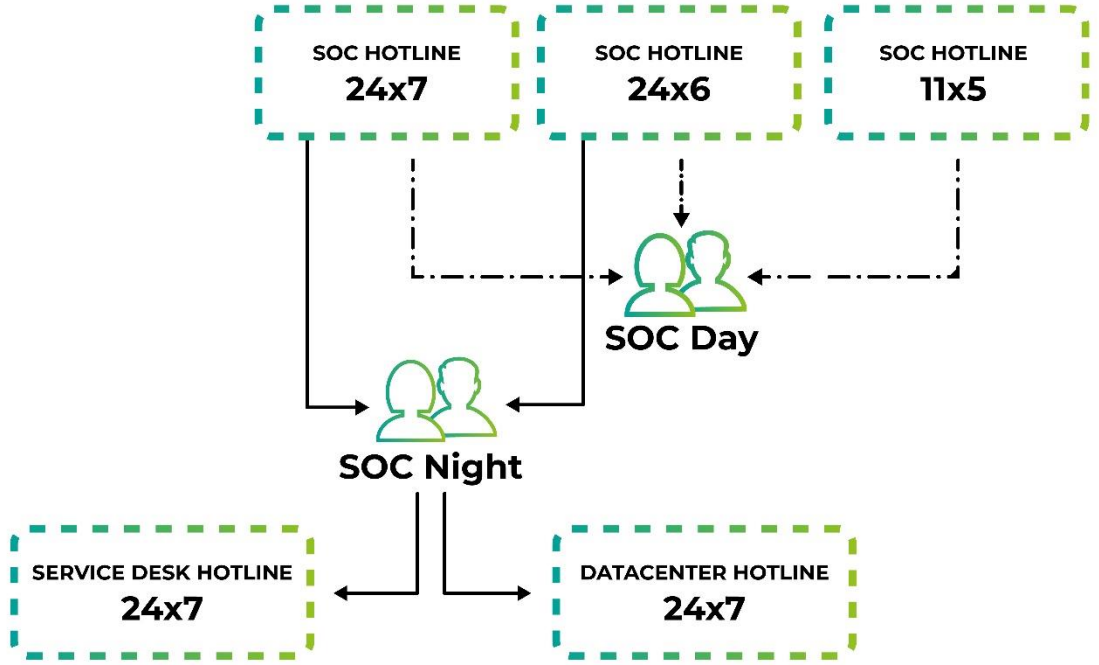
Matthias Klinski [Chief Information Security Officer | SWIETELSKY AG]
„Bei der Auswahl des Managed Security Operation Center Services waren für uns zwei Dinge entscheidend: State-of-the-Art Technologien und Transparenz im erbrachten Service. Der Managed Service Security der Base-IT vereint diese zwei 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."

SWIETELSKY AG

Base-IT Managed Service Security & Security Operations Center

SECURITY COMPLETE & SOC

- Azure AD Premium P1
- Microsoft Defender AV
- Azure AD Premium 2
- Defender for Endpoint (MDE)
- Defender for Identity (MDI)
- Defender for Office 365 (MDO)
- Defender for Cloud Apps
- Defender for Cloud
- Microsoft Sentinel



Forensic Analysis

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

PROACTIVE OPERATIONS & SERVICING

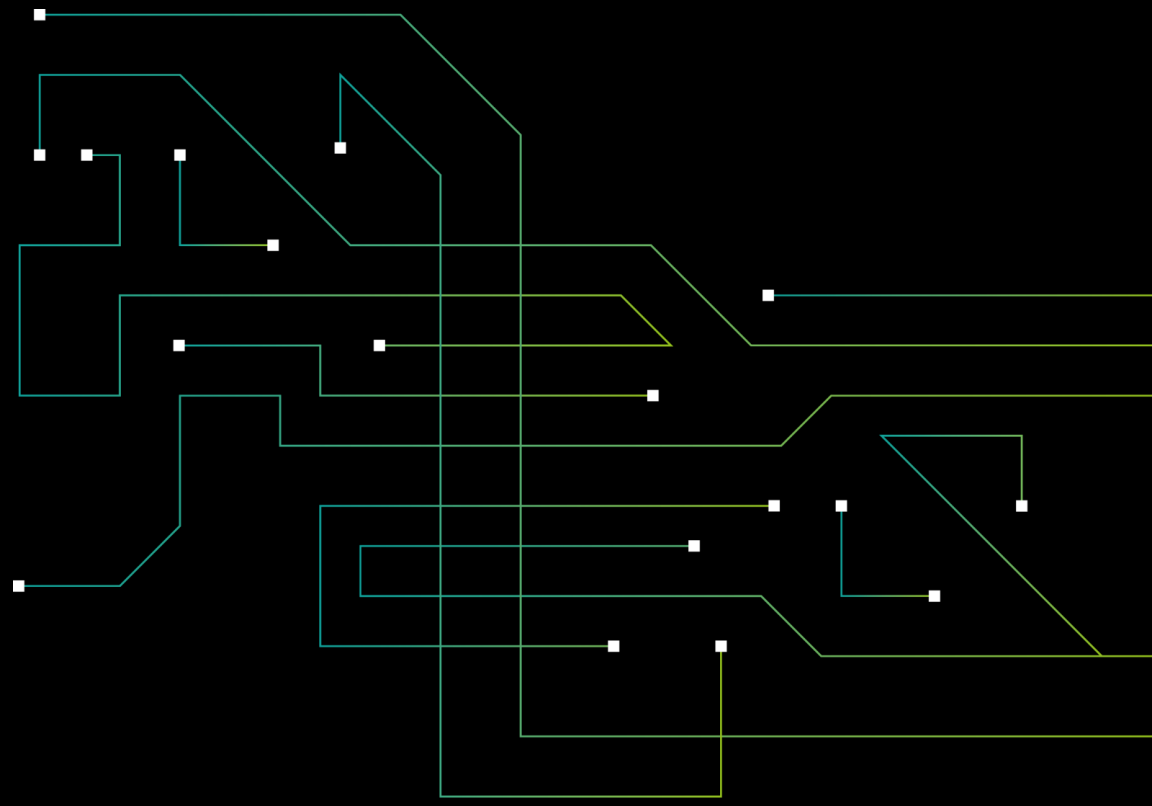
Betreuung von Microsoft Security Lösungen auf Basis des gewählten Base-IT Managed Service Pakets, bei SWIETELSKY „Security Complete“

Reactive Alert Handling

Betreuung durch das Base-IT Security Operations Center

base it

IHR PARTNER FÜR MODERN WORKPLACE



professional.
fast.
secure.

Base IT | Ihr Partner für Modern Workplace - YouTube

base it

Haider Straße 23 | 4052 Ansfelden | Austria

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