glueck kanja

Christopher Brumm

Clickbait vs. Reality: Die Cyber Threats, um die Sie sich wirklich sorgen sollten

glueck kanja

Protecting your assets around the globe 24/7

50+

Countries

5

Years in Service

15+

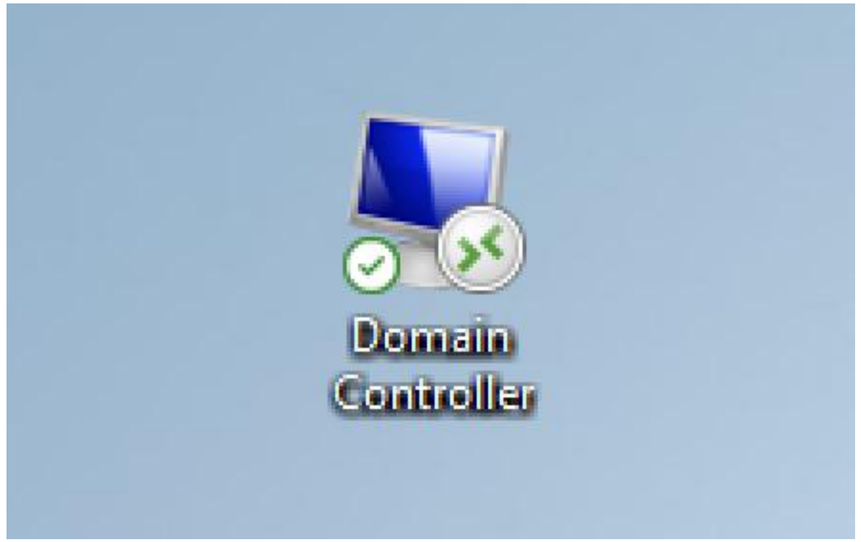
Industries

glueck kanja

Thermal Attacks & AI supported Attacks

RDP

Bad Citrix Password, RDP File with saved creds on desktop.



glueck kanja

Adverts

User:
Hey helpdesk, could you install a printer driver for me?

Google download hp printer driver

Ad • www.really-not-malicious.com

Official HP® Printer Drivers and Software Download

Download the latest **drivers**, **software**, firmware, and diagnostics for your **HP printers** from the official **HP** Support website.

SQL Server

Service Provider on a Maintenance Saturday:

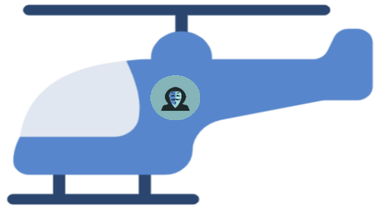
Shit, I forgot to ask for the SQL Server Password

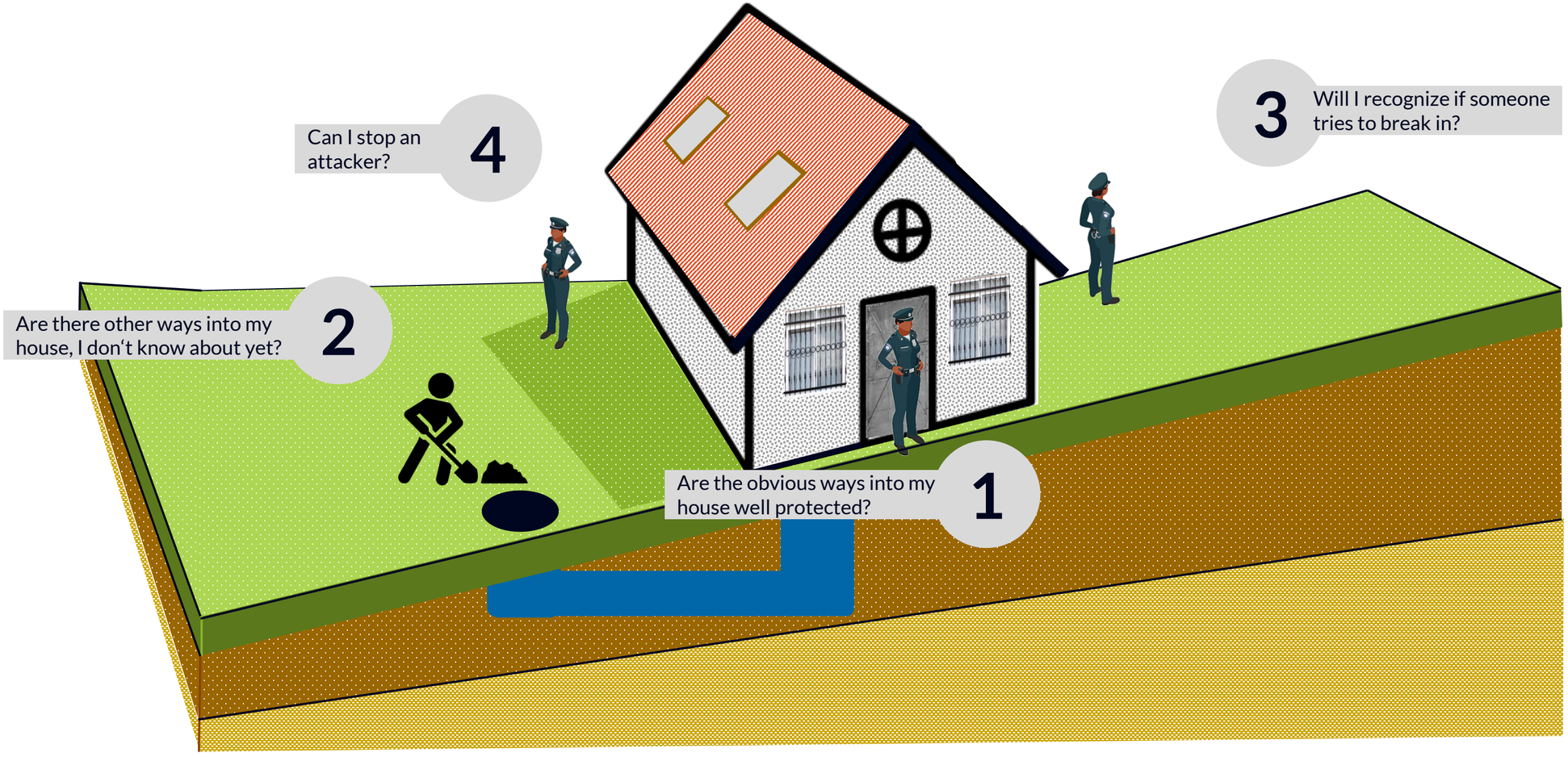
Hashcat

glueck kanja

The sorrows of a CISO

Are we safe enough?





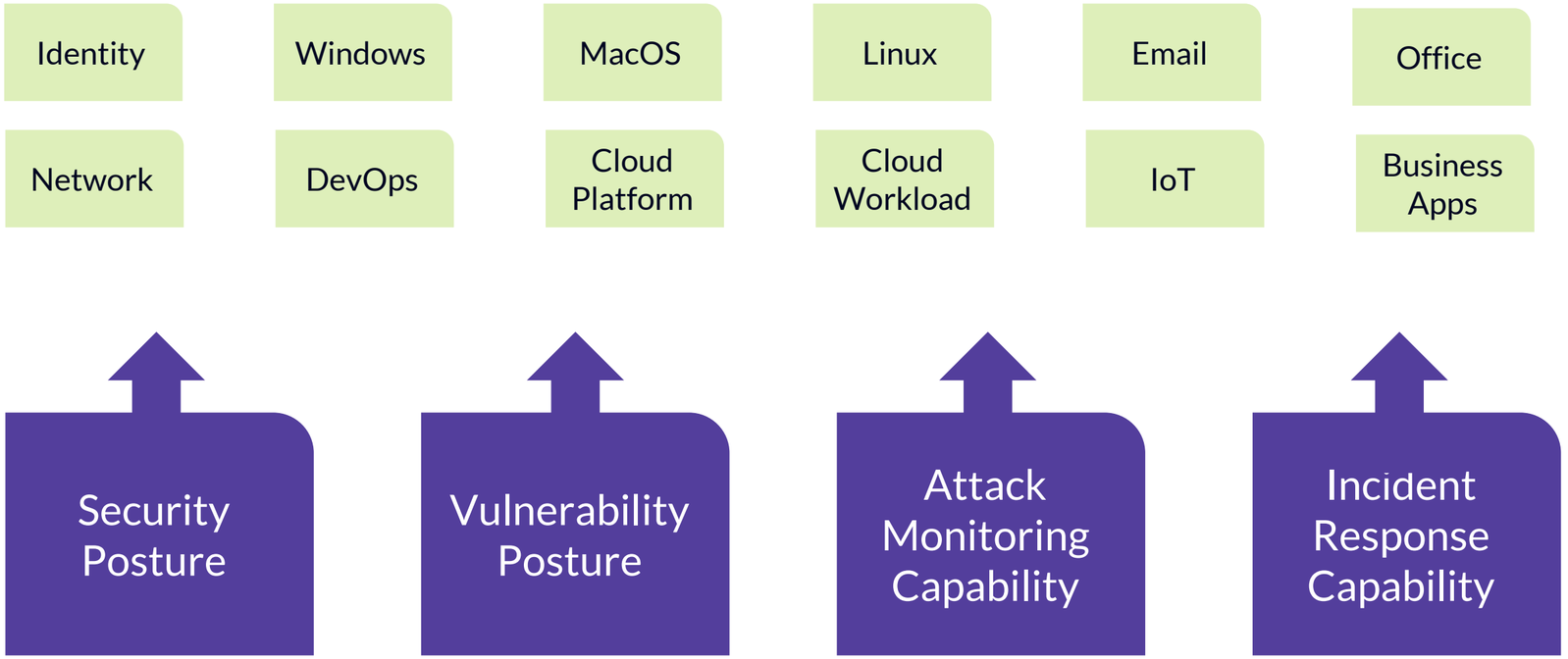
glueck kanja

Are you safe?

Enterprise Security Status

1 Are the obvious ways into my house well protected?	2 Are there other ways into my house, I don't know about yet?	3 Will I recognize if someone tries to break in?	4 Can I stop an attacker?
Security Posture	**Vulnerability Posture**	**Attack Monitoring Capability**	**Incident Response Capability**
Infrastructure Architecture	Vulnerability Monitoring	XDR Monitoring	24/7 IR Resources
As-Is Configuration Quality	External Attack Surface Monitoring	Sentinel Monitoring	Preparation of Emergency Incident
Best Practices Feature Comparison	Pen Testing / Red Teaming	Maintained Detection Repository	Processes

Applying it to your Org



glueck kanja

Customer Maturity Levels (CML)

	Security Posture	Vulnerability Posture	Attack Monitoring Capability	Incident Response Capability
CML 1	– USER MFA – ASR Rules	– Vulnerability Monitoring – Critical Patch Workflow	– MDE deployed on Clients – MDI deployed	– Internal or External SOC for Defender XDR
CML 2	– Role based just in time Access – Pingcastle Result X	– External Attack Surface Monitoring	– Sentinel Maturity Level 1	– AzERE

glueck kanja

Security Services

Preventive Services

Preperation for the worst case in combination with gap analysis

- Active Directory
- Entra ID
- Azure Infrastructure

AzERE

Your Life Net for the worst case: Secure Environment for AD Backup and Recovery

Managed Red Tenant

Managed privileged administration environment

Security Consulting

Deeply skilled experts that help you implement cutting edge security technology

APT Response

Incident Response in case of an Emergency

CSOC

24/7 Managed SOC, based on Microsoft Security Technology

Data Security Services

Prevent sensitive data from traveling into the unknown. Your Purview managed service

glueckkanja

glueckkanja ❤ Microsoft

Bundesamt
für Sicherheit in der
Informationstechnik

Qualifizierter
APT Response Anbieter

Microsoft Intelligent
Security Association

Microsoft

Microsoft Verified
Managed XDR Solution

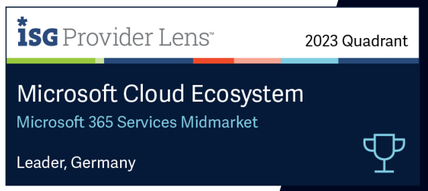
Microsoft
Solutions Partner
Data & AI
Azure

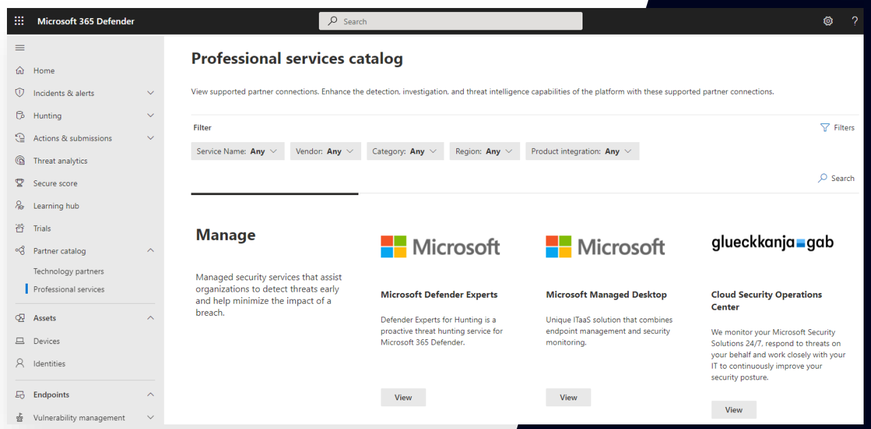
Microsoft
Solutions Partner
Digital & App Innovation
Azure

Microsoft
Solutions Partner
Modern Work

Microsoft
Solutions Partner
Security

Microsoft
Solutions Partner
Infrastructure
Azure





2x
Finalist
Security MSSP of the Year
Microsoft Security

8x
Winner / Finalist
Partner of the Year Award
Microsoft

ISO 27001

100 Microsoft Focus

glueck kanja

Our Approach to Modern Security

Microsoft sponsored

Implementation

Managed CSOC

CSOC Wide
Microsoft XDR

- Defender for **Endpoint**
- Defender for **Identity**
- Entra ID **Identity Protection**
- Defender for **Office 365**
- Defender for **Cloud Apps**
- **Defender XDR Custom Detections + Entra ID Sentinel Basic Detections** (GK Detection Engineering)

CSOC Deep
Microsoft Sentinel

- **Network Log Interaction** (e.g. Firewalls, Proxy, VPN, OT)
- **Windows Event Logs, Linux, Syslogs**
- **Defender for Cloud**
- **Entra ID Sentinel Advanced Directions**
- **Business Apps** (e.g. Power Platform, Dynamics, SAP)
- **Defender for IoT**
- **Office Activity, Cloud Platform** (Azure, AWS, GCP)**, Cloud Workload**
- **3rd Party Log Interaction** (e.g. Okta, Auth0, Qualys)
- **Self-Managed Threat Intelligence**

GK Detection Engineering

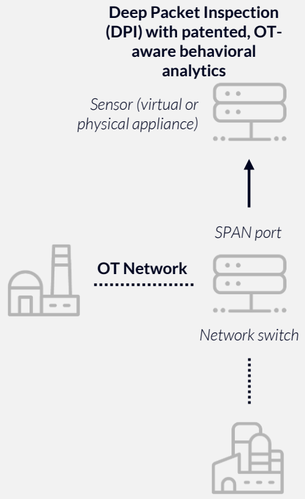
CSOC Foundation
GK Automation

- **CI / CD Deployment**
- **Playbook Manager**
- **Customer Enrichment**

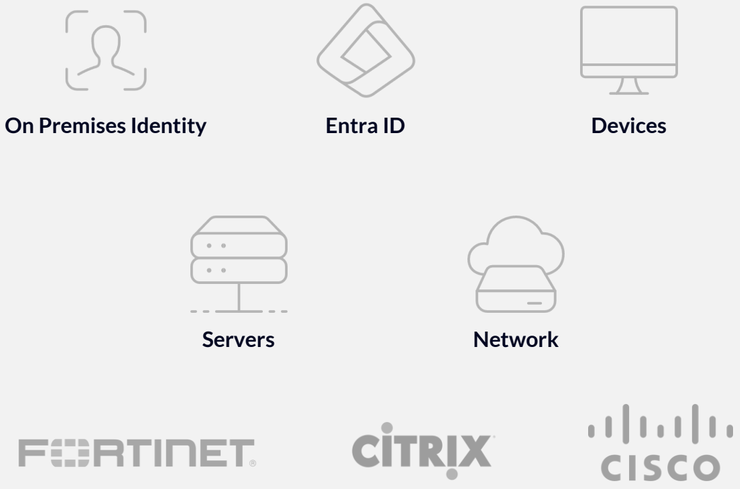
glueck kanja

Asset Coverage

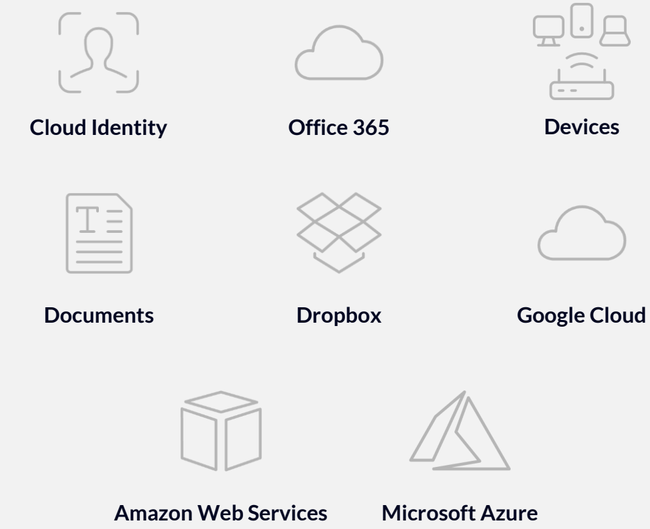
OT & IoT

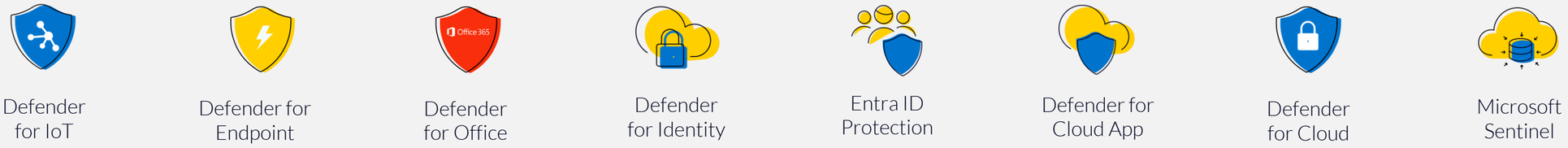


On Premises



Cloud





glueck kanja

THANK YOU!