

CSOC

Cloud Security Operation Center

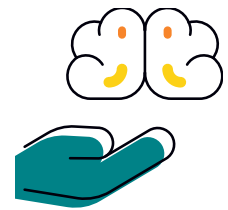
Protect // Detect // Respond // Improve



We see your trouble coming.

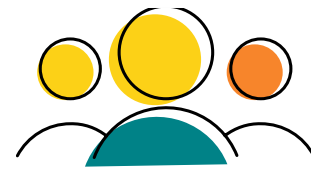
Who we are...

Years of Experience



30+

Employees



200+

Microsoft Designations & Specializations



14

Partner of the Year Awards



8





Bundesamt
für Sicherheit in der
Informationstechnik

Qualifizierter
APT Response Anbieter

Microsoft Intelligent
Security Association



Microsoft Verified
Managed XDR Solution



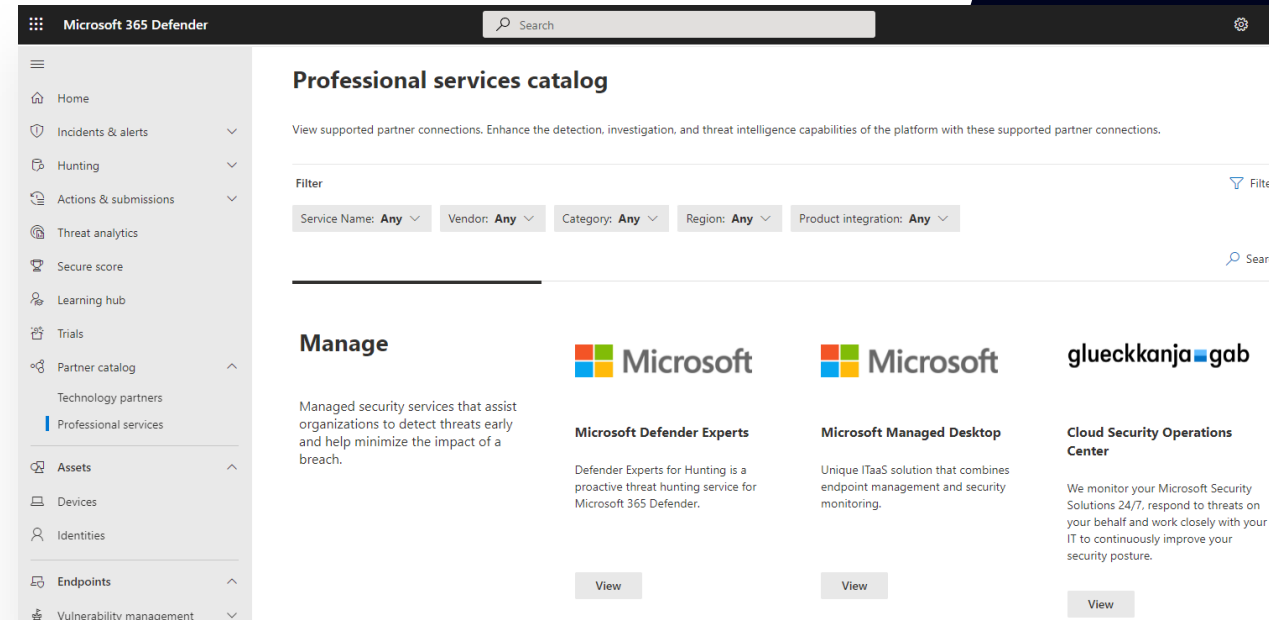
 **Microsoft**
Solutions Partner
Data & AI
Azure

 **Microsoft**
Solutions Partner
Digital & App Innovation
Azure

 **Microsoft**
Solutions Partner
Modern Work

 **Microsoft**
Solutions Partner
Security

 **Microsoft**
Solutions Partner
Infrastructure
Azure



What Microsoft says

glueckkanja



With malicious attacks on the rise, we understand security is front and center for our customers. That is why I am excited to congratulate glueckkanja on achieving Microsoft Verified: Managed Extended Detection and Response solution status. Their solution closely integrates with Microsoft 365 Defender and Microsoft Sentinel and has been verified by Microsoft Security engineering to ensure that it provides comprehensive service coverage across the Microsoft Security portfolio.



– Rob Lefferts, CVP, Modern Protection and SOC, Microsoft

glueckkanja



I am happy to work with the people at glueckkanja. They show always highest professionalism, constantly invest fully leveraging and extending security tools to provide the best levels of threat protection to customer organizations. They also provide important and insightful feedback and input that help shape and evolve security products.

Corina Feuerstein, Principal Program Manager, Microsoft

glueckkanja



Collaborating with glueckkanja, a Microsoft Security Provider, as a product manager has been a rewarding experience. Their early adoption of our features and valuable feedback have greatly impacted our product's design and roadmap, making them a crucial partner in our success.

Tali Ash, Senior Product Manager, Microsoft 365 Defender, Microsoft

glueckkanja



glueckkanja is a very active partner we constantly work with, especially through our Customer Connection Program (CCP). They contribute with deep knowledge and valuable feedback in various feature development cycles, helping make our products better.

Heike Ritter, Principal Product Manager, Microsoft

glueckkanja



glueckkanja's team has been valued partner for the Entra ID engineering team for several years. Their extensive experience deploying and managing our products has given them a unique perspective that has helped us form our approaches to new identity security capabilities related to risk-based Conditional Access and ID Protection.

– Etan Basseri, Security Product Management + AI, CISSP, Microsoft

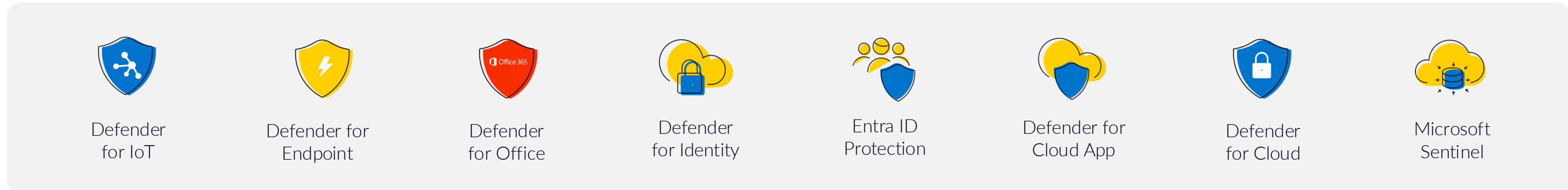
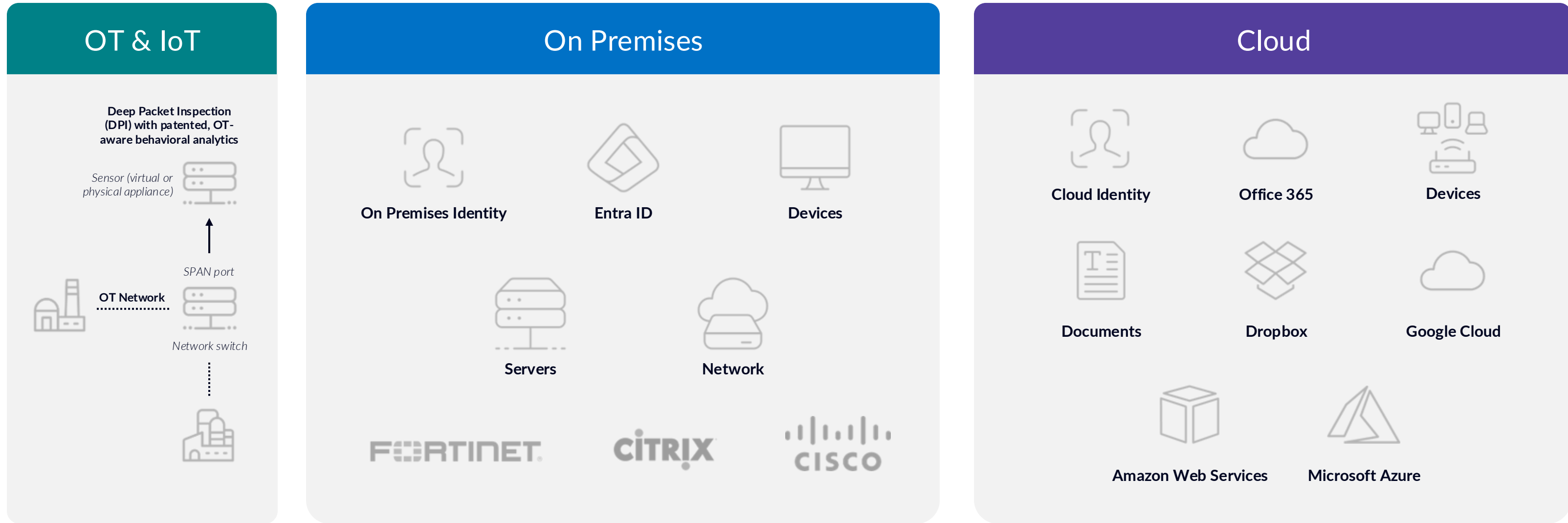
glueckkanja



When we started the development work for our Unified Security Operations Platform (USOP) we needed capable and quality focused customer who would be willing to work very closely with us, knowing that it would be a great, but bumpy ride. When I talked to the folks at glueckkanja AG they immediately were excited and willing to invest resources to help us to build a great service. The great team, led by Jan Geisbauer (Fabian Bader and Thomas Naunheim) were able to help us identify bugs, gaps and critical performance issues. They were and are critical to our success in achieving a great Ignite milestone and our journey to public preview and GA of USOP.

Tiander Turpijn, Principal Product Manager, Microsoft Sentinel, Microsoft

Asset Coverage



Who we are...



~50

CSOC Team Members

7 years

Average Company Affiliation

4 of 6

German Security MVPs

- Best in Class Analysts
- Detection Engineers
- APT Responders
- Purple Teamer
- TAMs
- Sentinel Experts
- Identity Experts
- OT / IoT Experts
- Defender Experts
- Threat Intel Researchers
- Linux Experts
- Firewall Experts

Threat & Vulnerability Management

- Based on Defender for Endpoint
- Ad-hoc Recommendations for new **critical** vulnerabilities
 - Through notification, member-only newsletter & monthly reports

glueckkanja

CSOC Security Update

Critical vulnerability in the Log4j Java library



A critical vulnerability in the **Log4j Java library** was recently disclosed. This allows attackers to execute arbitrary code (remote code execution) on applications that are

TOP 10 SOFTWARE VULNERABILITIES

Product	Machines	Vulnerabilities	Impact
Google Chrome	1809	891	12.09
Microsoft Edge Chromium-based	431	236	2.88
Microsoft Windows 10	191	1118	2.24
Cisco Ios	116	201	1.62
Zoom	290	3	1.43
Apache Log4j	172	7	1.42
Microsoft Office	182	52	1.22
Oracle Jre	117	605	0.85
Openbsd Openssh	88	50	0.77
Microsoft .NET Framework	109	6	0.63

Public Exploit

Windows Hyper-V Elevation of Privilege Vulnerability

CSOC Severity

- Critical (Now)
- High (4 Weeks)
- Medium (8 Weeks)

Vulnerability Index by glueckkanja

Search products

Vulnerability overview

Product	TenantName	Exposed Machines	Crit. Vulnerabilities	Public Exploit
Pulsesecure Pulse Secure		1	0	False
Pulsesecure Pulse Secure		1	0	False
Pulsesecure Pulse Secure		1	0	False
Pulsesecure Pulse Secure		1	0	False
Pulsesecure Pulse Secure		1	0	False
Pulsesecure Pulse Secure		2	0	False
Pulsesecure Pulse Secure		3	0	False
Pulsesecure Pulse Secure		1	0	False

glueck kanja

50+

Countries

5

Years in Service

15+

Industries

Protecting your assets around the globe 24/7

