Herzlich Willkommen zur

CYBER DEFENSE HORIZONS

08.10.2026



Unsere heutige Leitfrage:

Wie werden aus spezialisierten Technologien belastbare Sicherheits-abläufe gegen neue Bedrohungen?



Arne Vodegel
Head of SOC & Threat Intelligence
Cyber Samurai GmbH



Threat Landscape 2026

Die Angreifer sind vernetzt.
Sind wir es auch?

Fünf Dinge bleiben 2026 hochaktuell



SILOED ALERTS

EACH TOOL SEES ONLY A PIECE

SIEM — CRITICAL

Multiple failed login attempts

Source IP: 185.62.***.**
User: j.smith
10:21:15

EVENT COUNT

ENDPOINT DETECTION — HIGH

Malicious PowerShell execution detected

Host: WS-10234
User: j.smith
10:23:47

EVENT COUNT

EMAIL SECURITY — HIGH

Suspicious email delivered

Subject: Invoice details
From: billing@acme-service.com
10:20:11

EVENT COUNT

FIREWALL — MEDIUM

Unusual outbound connection

Destination: 104.21.***.**
Port: 443 (HTTPS)
10:24:02

EVENT COUNT

IAM SYSTEM — HIGH

New sign-in from unusual location

User: j.smith
Location: Eastern Europe
10:22:18

EVENT COUNT

CLOUD MONITORING — MEDIUM

Unusual API call pattern detected

Service: Microsoft Graph API
App: MailService
10:25:10

EVENT COUNT



Warum Silos Angreifern helfen

MANY ALERTS. NO CONTEXT.
NO STORY. NO PRIORITY.

CORRELATED ATTACK CHAIN

THE FULL PICTURE. ONE STORY.

INITIAL ACCESS
Spear phishing email delivered to user
10:20:11 — Email Security

CREDENTIAL ACCESS
User clicked link and entered credentials on fake page
10:21:15 — SIEM / IAM

ACCOUNT COMPROMISE
Successful login from unusual location
10:22:18 — IAM System

EXECUTION
Malicious PowerShell executed on endpoint
10:23:47 — Endpoint Detection

DISCOVERY & MOVEMENT
Internal reconnaissance and lateral movement
10:24:31 — Network / EDR

EXFILTRATION
Data staged and transferred to external server
10:25:10 — Cloud Monitoring

IMPACT
Ransomware deployment and encryption
10:27:32 — EDR / File Monitor

ONE INCIDENT. ONE STORY.
PRIORITIZED. ACTIONABLE. CONTAINABLE.

FÜNF PRIORITÄTEN FÜR 2026

1. IDENTITÄTEN WIE KRITISCHE INFRASTRUKTUR BEHANDELN
2. LIEFERANTENZUGRIFFE AKTIV ÜBERWACHEN
3. THREAT INTELLIGENCE OPERATIONALISIEREN
4. SECURITY-TOOLS KORRELIEREN STATT ISOLIEREN
5. INCIDENT RESPONSE REGELMÄSSIG ÜBEN

MERKSATZ:

RESILIENZ ENTSTEHT NICHT DURCH BESITZ VON TOOLS. RESILIENZ ENTSTEHT DURCH GEÜBTES ZUSAMMENSPIEL.



Ihr Kontakt:



Arne Vodegel
Head of SOC & Threat Intelligence
Tel.: +49 170 9080432
E-Mail: arne.vodegel@cyber-samurai.net