DCSO
Engineering Security.
Together.

Warum Managed Detection über den Endpunkt hinausgehen muss

Thomas Hemker

2022-10-26

DCSO Booth: Hall 6, Nr. 430

TLP: White

Let’s get to know each other
Who we are

Thomas Hemker, CISSP, CISM, CISA
Director Cyber Defense

- 27 Jahre Cyber-Security
- Threat Intelligence & Advisory Board
- ENISA ETL Stakeholder Group
- ISACA, (ISC)2, TeleTrust, (prev. ISF Advisory Council)
- Speaker, Author, Associate Lecturer
- NAI, PGP, SYMC
- Hamburg

researchgate.net/profile/Thomas_Hemker3

Cyber Security … … by Design or by Counterplay?

linkedin.com/in/themker

xing.com/profile/Thomas_Hemker/cv

Deutsche Cyber-Sicherheitsorganisation

Aus der Wirtschaft – für die Wirtschaft

Connect

Leverage the expertise of the DCSO Community, connect with industry peers, our experts and law enforcement.

DCSO Community

Advisory Board

Defend

Strengthen cyber defense with measures to identify, investigate and remediate threats.

Threat Intelligence

Threat Detection & Hunting

Incident Response

Improve

Continuously evaluate and mature your security posture along technical and organizational capabilities.

Security Assessments

Security Technology

Security Consulting

Warum fokussiert jeder auf Endpoint Security?

Maximale Sichtbarkeit	▪ Jeder Prozess, jede Netzwerkverbindung ▪ Datenhaltung erlaubt Threat Hunting
Kein Perimeter	▪ Direktes Routing ins Internet ohne VPN ▪ Home Office, private Nutzung von Geräten
Maximaler Durchgriff	▪ Root auf dem System ▪ Isolation, Quarantäne, händische Ausführung von Prozessen

Welche Probleme hat Endpoint Security?

Kein Agent = kein Schutz	▪ Embedded Geräte (Drucker, Meeting-Displays, Produktion) ▪ Unbekannte Geräte (private Handys, etc.)
Sichtbar für den Angreifer	▪ Permanente Entwicklung von Umgehungen [1] ▪ Regelmäßige Schwachstellen in bekannten Produkten [2]

[1] https://heise.de/-6160551
[2] https://security.paloaltonetworks.com/CVE-2017-7408

McAfee Total Protection: Angreifer könnten Daten löschen

Ein wichtiges Sicherheitsupdate schließt eine Schwachstelle in der Anti-Viren-Software von McAfee.

14. März 2022, 09:21 Uhr 12

McAfee Agent könnte als Schlupfloch für Schadcode dienen

Ein wichtiges Sicherheitsupdate schließt eine Schwachstelle in McAfee Agent.

29. Juli 2022, 11:38 Uhr 18

Angreifer könnten sich über Lücken in McAfee Agent in Windows einnisten

Eigentlich soll McAfee Agent Computer schützen. Doch zwei nun gepatchte Schwachstellen könnten Angreifer auf Computer lassen.

21. Januar 2022, 11:31 Uhr 38

Einige Eset-Produkte könnten Angreifern System-Rechte verschaffen

Es gibt wichtige Sicherheitsupdates für verschiedene Windows-Schutzlösungen von Eset.

03. Februar 2022, 09:52 Uhr 12

Jetzt aktualisieren! Angriffe auf Sicherheitslücke in Trend Micro Apex Central

Trend Micro warnt vor Angriffen auf eine Sicherheitslücke in zentralen Verwaltungssoftware Apex Central. Zum Abdichten des Lecks stehen Updates bereit.

30. März 2022, 09:25 Uhr 5

Angreifer könnten Scan-Engine von F-Secure und WithSecure crashen lassen

Patches schließen mehrere Lücken in Sicherheitsprodukten von WithSecure ehemals F-Secure.

25. Juli 2022, 13:50 Uhr 4

Fortinet dichtet mehrere Schwachstellen in zahlreichen Produkten ab

Der IT-Sicherheitsanbieter Fortinet hat in diversen Produkten Sicherheitslücken aufgespürt. Updates stehen bereit, die die Schwachstellen abdichten.

06. Juli 2022, 15:42 Uhr 9

Patchvorgang von Bitdefender Endpoint Security Tools manipulierbar

Sicherheitsupdates schließen unter anderem eine kritische Sicherheitslücke in der Schutzsoftware Endpoint Security Tools von Bitdefender.

29. November 2021, 11:31 Uhr 7

Sicherheitsupdate: Trend Micro Apex One und Worry-Free Business angreifbar

Angreifer könnten an einer Sicherheitslücke in Windows-Schutzlösungen von Trend Micro ansetzen.

29. Juli 2022, 10:49 Uhr 1

Sicherheitsupdate: Trend Micro Maximum Security könnte Angreifer auf PCs lassen

Wer Windows mit Trend Micro Maximum Security schützt, sollte die Anti-Viren-Anwendung auf den aktuellen Stand bringen.

05. Juli 2022, 10:19 Uhr 5

Schlupfloch in Trend Micro ServerProtect lässt Angreifer auf Server

Wichtige Sicherheitsupdates schließen unter anderem eine kritische Lücke in ServerProtect. Auch Worry-Free Business Security ist verwundbar.

24. Februar 2022, 17:18 Uhr 2

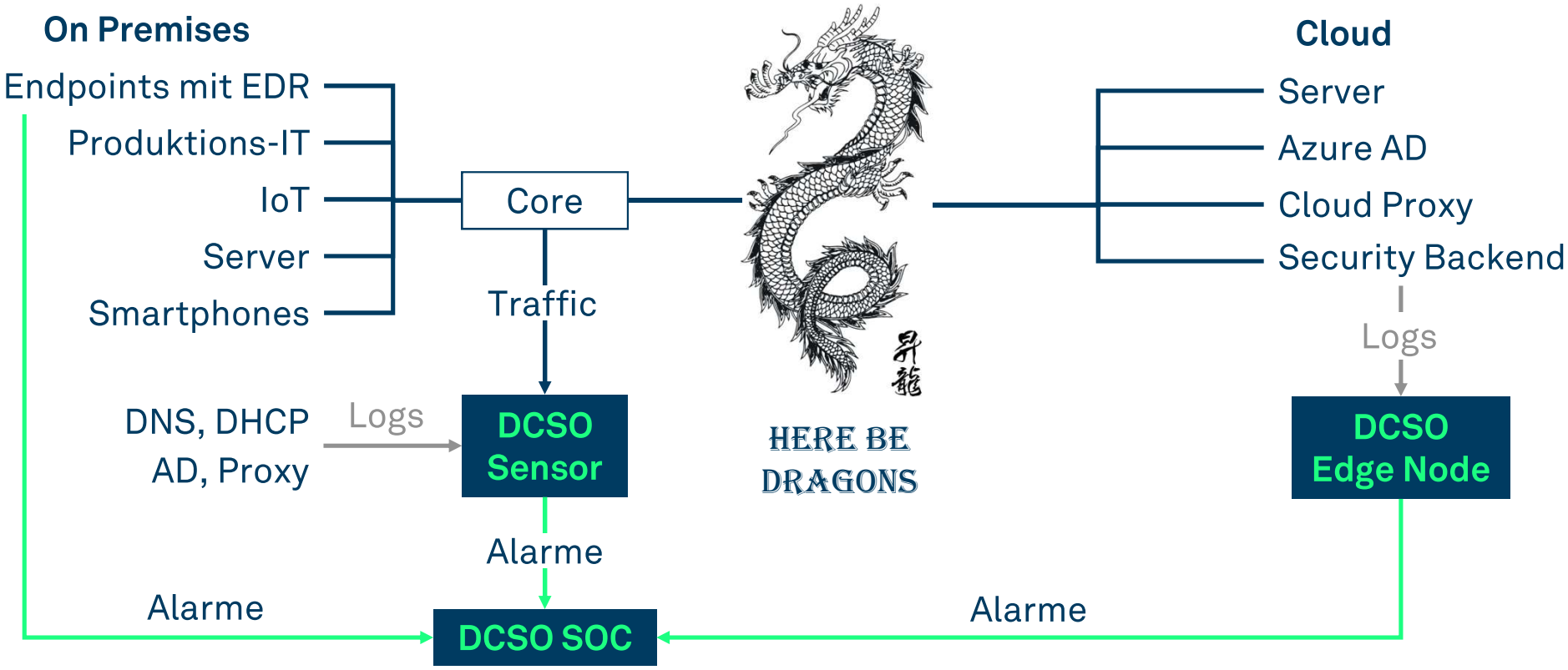
Trend Micro Apex One und Worry-Free Business Security gefährden Windows-PCs

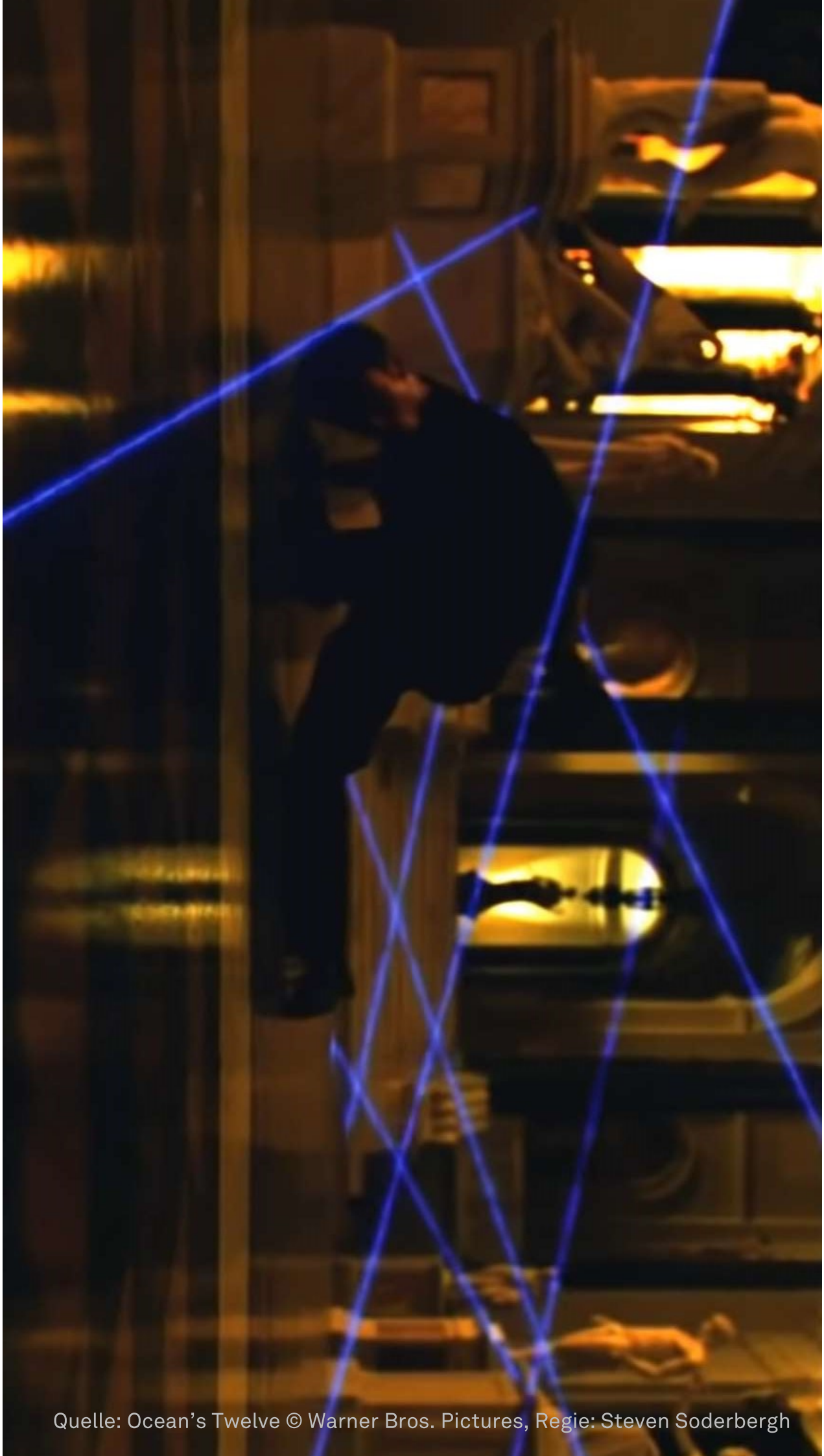
Es sind wichtige Sicherheitsupdates für die Schutzlösungen Apex One und Worry-Free Business Security von Trend Micro erschienen.

03. Januar 2022, 12:10 Uhr 8

Endpoint Security? **Ja!**
Nur Endpoint Security? **Nein.**

Überwachung auf mehreren Ebenen





Quelle: Ocean’s Twelve © Warner Bros. Pictures, Regie: Steven Soderbergh

DCSO
Engineering Security.
Together.

Let‘s meet!
Hall 6, Booth 430

DCSO Deutsche Cyber-Sicherheitsorganisation GmbH
EUREF-Campus 22
10829 Berlin

thomas.hemker@dcso.de

+49 151 18274832

Whitepaper: NDR für den Mittelstand

TLP: GREEN