Problem: Defender Security Gap

Microsoft Defender for Endpoint kann URLs in Nicht-Microsoft-Browsern (z. B. Chrome, Firefox, Safari) nicht zuverlässig blockieren.

> **Die Auswirkungen:**
>
> - Blockierte Indicators of Compromise (IOCs) greifen nur zuverlässig in Microsoft Edge.
> - Vollständige URLs bleiben in Dritt-Browsern für SOC-Teams unsichtbar.
> - Security-Analysen sehen häufig nur Domains statt konkreter Angriffspfade.
> - Vorhandene Defender-Intelligence wird nicht vollständig durchgesetzt.

Referenz: Microsoft Defender Web Protection Overview

Die Ursache

TLS-Verschlüsselung verhindert die Sichtbarkeit kompletter URLs auf Netzwerkebene. Endpoint-Network-Protection kann deshalb außerhalb des Browsers nicht zuverlässig greifen.

Lösung: Cybereinforce Threat Enforcement

Cybereinforce erweitert Defender um deterministische URL-Durchsetzung direkt im Browser.

- **Browser-Nativ:** Erkennt entschlüsselte URLs direkt im Browser.
- **Präzise:** Blockiert vollständige URL-Pfade zuverlässig.
- **Integriert:** Übernimmt automatisch Defender-IOCs und integriert sich in Microsoft Sentinel.
- **Universell:** Chrome, Firefox, Safari, Edge und Chromium-basierte Browser.

SOC-Mehrwert

Cybereinforce liefert die fehlende Transparenz, um Detection in Enforcement zu verwandeln:

- Vollständige URL-Transparenz
- Automatische IOC-Synchronisation
- Incident-Generierung in Sentinel
- Audit-fähige Block-Events

Compliance-Unterstützung

ISO 27001	NIS2	DORA
A.8.20, A.8.15, A.5.23, A. 5.9	Angriffserkennung, Prävention & Monitoring	Risk Reduction & Threat Detection

Ressourcen & Proof of Concept

- PoC Demonstration: **Video ansehen**
- Produktvorstellung: **Video ansehen**
- Threat-Intel Beispiel 1: **Video ansehen**
- Threat-Intel Beispiel 2: **Video ansehen**

ISO/IEC 27001 ZERTIFIZIERT

Cybereinforce Threat Enforcement ist ISO/IEC 27001 zertifiziert für den Betrieb der SaaS-Plattform.