TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

TeleTrusT-interner Workshop

Berlin, 01.07.2025

Unabhängige europäische Bedrohungslageninformation

Thomas Hemker, DCSO

Cyber Threat Intelligence

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

3.2.27 Cyber Threat Intelligence

Cyber Threat Intelligence ist ein wichtiger Grundbaustein moderner Verteidigungsstrategien und liefert Indikatoren, Reports und Dienstleistungen, um sich über das aktuelle Angriffsgeschehen zu informieren, Cyber-Angriffe zu erkennen, deren mutmaßliche Urheber zu bestimmen und Gegenmaßnahmen abzuleiten.

Cyber Threat Intelligence gliedert sich in drei Anwendungsbereiche:

- Taktische Cyber Threat Intelligence umfasst Malware-Analyse und den Import von einzelnen, statischen und verhaltensrelevanten Bedrohungsindikatoren in defensive IT-Sicherheitslösungen wie Netzwerk-, Endpoint- und Applikationssicherheitslösungen, um deren Effektivität zu erhöhen. Durch Cyber Threat Intelligence gewonnene Indikatoren können bei Maßnahmen wie System-Patching eine wichtige Rolle spielen.
- Operative Cyber Threat Intelligence dient der Verbesserung des Wissens über einen Angreifer, seine Fähigkeiten, Infrastrukturen und Angriffstaktiken, sowie Techniken und Prozeduren (TTPs). Anhand dieser Informationen lassen sich deutlich zielgerichteter Cyber-Sicherheitsmaßnahmen wie Vorfalls-Analysen, Incident Response und proaktives Threat Hunting umsetzen. Die Leistungsfähigkeit von Cyber-Sicherheitsmitarbeitern (z.B. aus dem Security Operation Center oder CERT) wie Threat Hunting Experten, Vulnerability Managern, Incident Response Analysten und Experten zur Abwehr von Insider-Bedrohungen wird dadurch verbessert.
- Strategische Threat Intelligence ermöglicht ein besseres Verständnis über die aktuelle Bedrohungslage (Threat Assessment), die Ableitung von Trends und die Motivation einzelner Angreifergruppen. Sie unterstützt bei strategischen Geschäftsentscheidungen zur Verbesserung der Cyber-Sicherheit.

Gegen welche Bedrohung(-en) der IT-Sicherheit wird die Maßnahme eingesetzt?

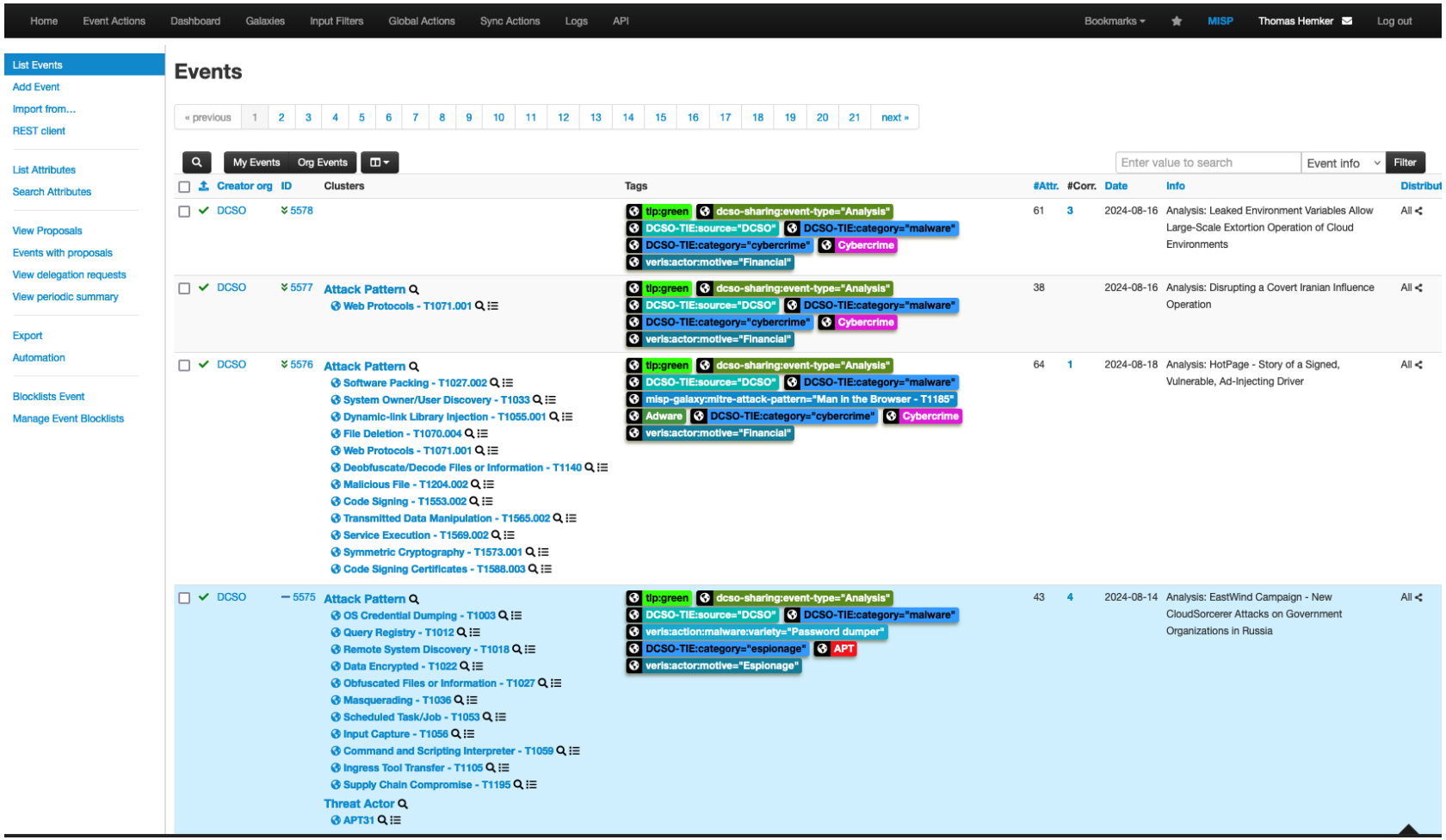
Cyber Threat Intelligence informiert über alle Arten von aktuellen und potenziellen Cyber-Bedrohungen und hilft bei deren Abwehr.

https://www.teletrust.de/fileadmin/user_upload/2025-06_TeleTrusT-Handreichung_Stand_der_Technik_in_der_IT-Sicherheit_DE.pdf

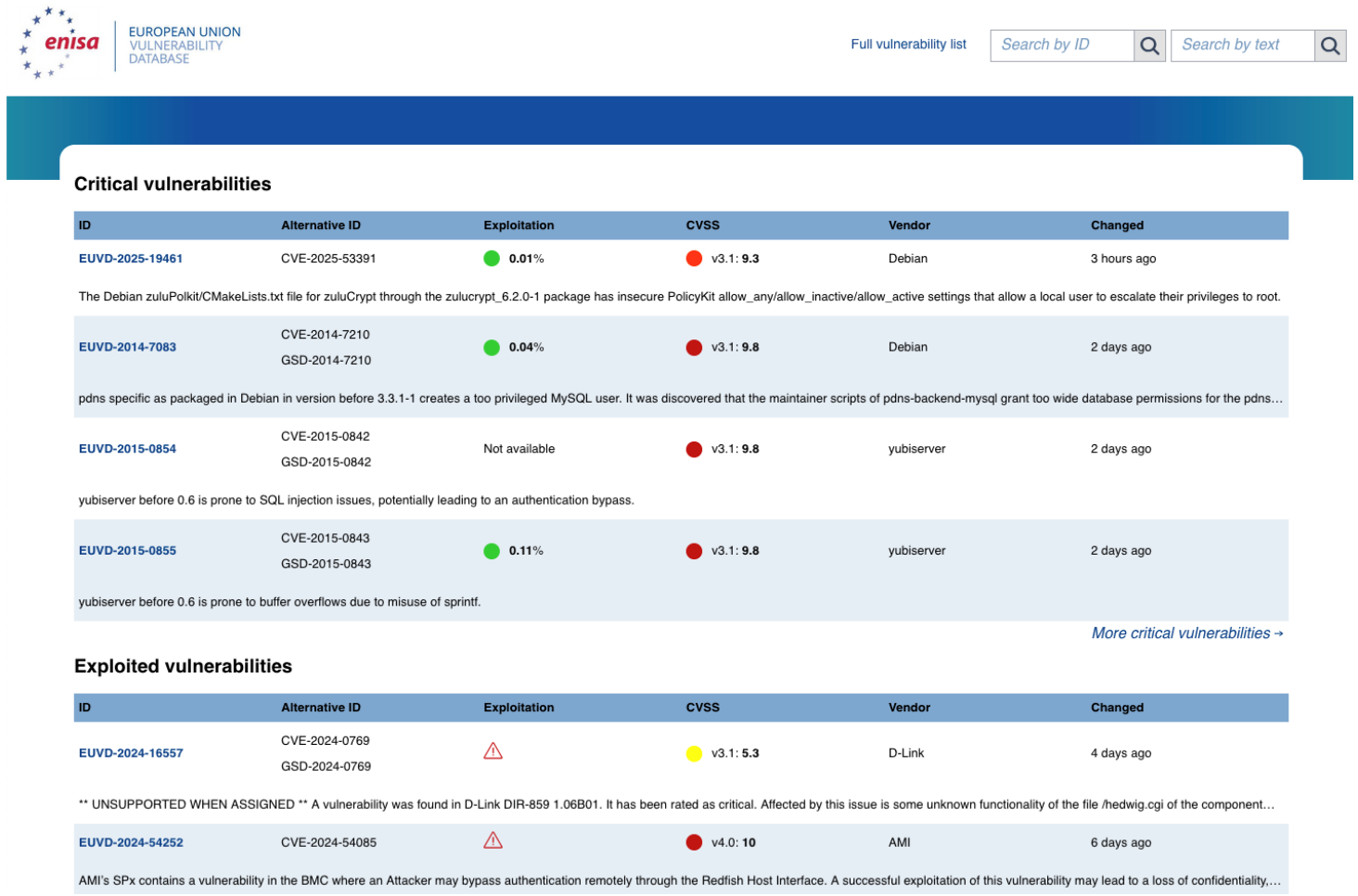
Warum?

https://www.googlewatchblog.de/wp-content/uploads/google-maps-golf-von-amerika-golf-von-mexiko.jpg

MISP: Standard in Europa



euvd.enisa.europa.eu



enisa EUROPEAN UNION VULNERABILITY DATABASE

Full vulnerability list | Search by ID | Search by text

Critical vulnerabilities

ID	Alternative ID	Exploitation	CVSS	Vendor	Changed
EUVD-2025-19461	CVE-2025-53391	0.01%	v3.1: 9.3	Debian	3 hours ago
The Debian zuluPolkit/CMakeLists.txt file for zuluCrypt through the zulucrypt_6.2.0-1 package has insecure PolicyKit allow_any/allow_inactive/allow_active settings that allow a local user to escalate their privileges to root.					
EUVD-2014-7083	CVE-2014-7210 GSD-2014-7210	0.04%	v3.1: 9.8	Debian	2 days ago
pdns specific as packaged in Debian in version before 3.3.1-1 creates a too privileged MySQL user. It was discovered that the maintainer scripts of pdns-backend-mysql grant too wide database permissions for the pdns…					
EUVD-2015-0854	CVE-2015-0842 GSD-2015-0842	Not available	v3.1: 9.8	yubiserver	2 days ago
yubiserver before 0.6 is prone to SQL injection issues, potentially leading to an authentication bypass.					
EUVD-2015-0855	CVE-2015-0843 GSD-2015-0843	0.11%	v3.1: 9.8	yubiserver	2 days ago
yubiserver before 0.6 is prone to buffer overflows due to misuse of sprintf.					

More critical vulnerabilities →

Exploited vulnerabilities

ID	Alternative ID	Exploitation	CVSS	Vendor	Changed
EUVD-2024-16557	CVE-2024-0769 GSD-2024-0769	⚠	v3.1: 5.3	D-Link	4 days ago
** UNSUPPORTED WHEN ASSIGNED ** A vulnerability was found in D-Link DIR-859 1.06B01. It has been rated as critical. Affected by this issue is some unknown functionality of the file /hedwig.cgi of the component…					
EUVD-2024-54252	CVE-2024-54085	⚠	v4.0: 10	AMI	6 days ago
AMI's SPx contains a vulnerability in the BMC where an Attacker may bypass authentication remotely through the Redfish Host Interface. A successful exploitation of this vulnerability may lead to a loss of confidentiality,…					

Interessante Themen

- Anwenderaustausch
- Anbieteraustausch
- Meldesysteme
- Behördeninformation

- Austauschplattform
- Austausch-Regime
- Lagebilder

- Nutzbarkeit
- Qualitätsicherung

- Digitale Souveränität
- Redundanz

Arbeitshypothese(n)

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

TeleTrust als Plattform

- Definition von Regeln
- Austausch
- Gemeinsame Nutzung
- Zentraler Zugang

TeleTrust als Interessenvertretung

- EU Vernetzung
- Grundlage für Souveränität schaffen
- Mittelbeschaffung