

TeleTrust-interner Workshop

Berlin, 01.07.2025

Unabhängige europäische Bedrohungslageninformation

Thomas Hemker, DCSO

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

What Maps users will see



in the U.S.



in Mexico



in the rest of the world

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

MISP: Standard in Europa

Home

Event Actions

Dashboard

Galaxies

Input Filters

Global Actions

Sync Actions

Logs

API

Bookmarks

★

MISP

Thomas Hemker

Log out

List Events

Add Event

Import from...

REST client

List Attributes

Search Attributes

View Proposals

Events with proposals

View delegation requests

View periodic summary

Export

Automation

Blocklists Event

Manage Event Blocklists

Events

« previous

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

next »

Q

My Events

Org Events

+

Enter value to search

Event info

Filter

☐	Creator	org	ID	Clusters	Tags	#Attr.	#Corr.	Date	Info	Distribut
☐	✓	DCSO	5578		tip:green dcso-sharing:event-type="Analysis" DCSO-TIE:source="DCSO" DCSO-TIE:category="malware" DCSO-TIE:category="cybercrime" Cybercrime veris:actor:motive="Financial"	61	3	2024-08-16	Analysis: Leaked Environment Variables Allow Large-Scale Extortion Operation of Cloud Environments	All
☐	✓	DCSO	5577	Attack Pattern Q	tip:green dcso-sharing:event-type="Analysis" DCSO-TIE:source="DCSO" DCSO-TIE:category="malware" DCSO-TIE:category="cybercrime" Cybercrime veris:actor:motive="Financial"	38		2024-08-16	Analysis: Disrupting a Covert Iranian Influence Operation	All
				Web Protocols - T1071.001 Q						
☐	✓	DCSO	5576	Attack Pattern Q	tip:green dcso-sharing:event-type="Analysis" DCSO-TIE:source="DCSO" DCSO-TIE:category="malware" misp-galaxy:mitre-attack-pattern="Man in the Browser - T1185" Adware DCSO-TIE:category="cybercrime" Cybercrime veris:actor:motive="Financial"	64	1	2024-08-18	Analysis: HotPage - Story of a Signed, Vulnerable, Ad-Injecting Driver	All
				Software Packing - T1027.002 Q						
				System Owner/User Discovery - T1033 Q						
				Dynamic-link Library Injection - T1055.001 Q						
				File Deletion - T1070.004 Q						
				Web Protocols - T1071.001 Q						
				Deobfuscate/Decode Files or Information - T1140 Q						
				Malicious File - T1204.002 Q						
				Code Signing - T1553.002 Q						
				Transmitted Data Manipulation - T1565.002 Q						
				Service Execution - T1569.002 Q						
				Symmetric Cryptography - T1573.001 Q						
				Code Signing Certificates - T1588.003 Q						
☐	✓	DCSO	5575	Attack Pattern Q	tip:green dcso-sharing:event-type="Analysis" DCSO-TIE:source="DCSO" DCSO-TIE:category="malware" veris:action:malware:variety="Password dumper" DCSO-TIE:category="espionage" APT veris:actor:motive="Espionage"	43	4	2024-08-14	Analysis: EastWind Campaign - New CloudSorcerer Attacks on Government Organizations in Russia	All
				OS Credential Dumping - T1003 Q						
				Query Registry - T1012 Q						
				Remote System Discovery - T1018 Q						
				Data Encrypted - T1022 Q						
				Obfuscated Files or Information - T1027 Q						
				Masquerading - T1036 Q						
				Scheduled Task/Job - T1053 Q						
				Input Capture - T1056 Q						
				Command and Scripting Interpreter - T1059 Q						
				Ingress Tool Transfer - T1105 Q						
				Supply Chain Compromise - T1195 Q						
				Threat Actor Q						
				APT31 Q						



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
- Qualitätssicherung
- Digitale Souveränität
- Redundanz

Arbeitshypothese(n)

TeleTrust als Plattform

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

TeleTrust als Interessenvertretung

- EU Vernetzung
- Grundlage für Souveränität schaffen
- Mittelbeschaffung