OPENKRITIS

Mapping Anforderungen Angriffserkennung (OH SZA) auf KRITIS, C5 und ISO 27002

Oktober 2022
1.0

OH SzA	Thema	BSI KRITIS	C5:2020	ISO 27001:2022
SZA-A	Allgemeine Anforderungen			
A1	Rahmenbedingungen	BSI-2 BSI-17	OIS-02 OIS-01 BCM-01	A.5.2 4-10 A.5.24 A.5.31
A2	Angriffsmuster	BSI-96 BSI-21 BSI-97	OPS-20 OPS-05 OIS-05	A.8.8 A.5.7
A3	Plattform	BSI-25	OPS-23	A.8.19 A.8.8
A4	Signaturen	BSI-21	OPS-05	A.8.7
A5	Konfiguration	BSI-93 BSI-91	OPS-15 OPS-13	A.8.9
SZA-G	Governance			
G1	Richtlinie Protokollierung	BSI-2 BSI-66 BSI-86	OIS-02 SP-02 COM-02	A.5.1 A.5.24
G2	Richtlinie Detektion	BSI-2 BSI-66 BSI-77 BSI-86	OIS-02 SP-02 SIM-01 COM-02	A.5.1 A.5.24
G3	Richtlinie Reaktion	BSI-2 BSI-66 BSI-77 BSI-86	OIS-02 SP-02 SIM-01 COM-02	A.5.1 A.5.24
G4	Verantwortlichkeiten Detektion	BSI-77	SIM-01	A.5.24
G5	Ressourcen Protokollierung	BSI-20	OPS-01	A.8.6
G6	Personal Detektion	BSI-20	OPS-01	A.8.6
G7	Verantwortlichkeiten Reaktion	BSI-17 BSI-77	BCM-01 SIM-01	A.5.24 A.5.29
G8	Meldewege	BSI-81	SIM-04	A.6.8
G9	Awareness	BSI-68 BSI-82	HR-03 SIM-05	A.6.3 A.5.27

OH SzA	Thema	BSI KRITIS	C5:2020	ISO 27001:2022
G10	Benachrichtigungen	BSI-100	OIS-05	A.5.5 A.5.31
G11	Meldungen	BSI-100	OIS-05	A.5.5
G12	Regulierung Protokollierung	BSI-85	COM-01	A.5.31 A.5.34 A.5.33
G13	Regulierung Detektion	BSI-85	COM-01	A.5.31 A.5.34 A.5.33
G14	Branchenstandards	BSI-16	OIS-01	A.5.31
SZA-P	**Protokollierung (Logging)**			
P1	Daten und Ereignisse	BSI-36 BSI-37	COS-01 OPS-10 OPS-12 OPS-14	A.8.20 A.8.16
P2	Planung	BSI-20 BSI-90	OPS-01 OPS-10	A.8.6
P3	Überprüfung	BSI-87 BSI-88	COM-02 COM-03	A.5.36
P4	Geltungsbereich	BSI-1 BSI-91 BSI-45	OIS-01 OPS-10 DEV-03	ISMS 4.2
P5	Infrastruktur	BSI-80	SIM-05 COS-01	A.8.15
SZA-D	**Erkennung (Detektion)**			
D1	Bedrohungen und Risiken	BSI-14	OIS-07	8.2 8.3
D2	Kontinuierliche Überwachung	BSI-90	OPS-13	A.8.16
D3	Systemfunktionen	BSI-36 BSI-91	COS-01 OPS-13	A.8.26 A.8.27 A.8.16
D4	Schadcode	BSI-21	OPS-04 OPS-05	A.8.7

OH SzA	Thema	BSI KRITIS	C5:2020	ISO 27001:2022
D5	Netze und IDS	BSI-36 BSI-37	COS-01 COS-02 COS-03	A.8.20 A.8.21 A.8.23
D6	Korrelation und Signaturen	BSI-80 BSI-21 SZA-A4	SIM-05 OPS-05	A.6.8
D7	Zentrale Detektion	BSI-80	COS-01 SIM-05	A.6.8
D8	Dauerhafte Auswertung	BSI-91	OPS-13	A.8.16
D9	Manuelle Verfahren	BSI-90 BSI-77	OPS-10	A.5.24
D10	Automatische Alarmierung	BSI-91 BSI-80	OPS-13 SIM-05	A.8.16
D11	Überprüfung	BSI-91	OPS-13	A.8.16
D12	Externe Quellen	BSI-97	OIS-05	A.5.5 A.5.6
D13	Angriffsmuster	BSI-96 BSI-97	OPS-20 OIS-05	A.5.7
D14	Sicherheitsrelevante Ereignisse	BSI-78 BSI-82	SIM-02 SIM-05	A.5.26 A.5.27
SZA-R	**Reaktion**			
R1	Definition	BSI-77	SIM-01	A.5.24 A.5.25
R2	Behebung	BSI-77 BSI-78	SIM-01 SIM-02	A.5.24 A.5.25 A.5.26
R3	Wiederherstellung	BSI-18	BCM-03	A.5.30
R4	Automatische Reaktion	BSI-36	COS-01 COS-02	A.8.21 A.8.22
R5	Behandlung Angriffe	BSI-78	SIM-02	A.5.26

Quelle: *Eigene Zusammenstellung, Entwurf, Oktober 2022*

OpenKRITIS

Das freie Informationsportal für Kritische Infrastrukturen

Mapping Angriffserkennung auf KRITIS, C5 und ISO 27001

Das OpenKRITIS-Mapping ist eine Gegenüberstellung der Anforderungen der Orientierungshilfe Angriffserkennung OH SzA mit Security-Standards und KRITIS:

OH SzA: Anforderungen der BSI Orientierungshilfe Systeme zur Angriffserkennung.
BSI KRITIS: Die 100 KRITIS-Anforderungen der BSI Konkretisierung für Betreiber.
C5:2020: Aktualisierter BSI Cloud Security Standard mit einigen Veränderungen.
ISO 27001: Informationssicherheit der ISO 27001/27002 der 2022er-Version.

Grundlage ist das KRITIS-Standards Mapping von OpenKRITIS und ist ohne Gewähr der Vollständigkeit und Korrektheit.

Quelle: OpenKRITIS Mapping KRITIS Angriffserkennung

Stand: 21. Oktober 2022
Version: 1.0

Impressum

Paul Weissmann c/o Insignals GmbH
Rheinwerkallee 6
53227 Bonn

https://www.openkritis.de · ISSN 2748-565X
info@openkritis.de · +49 176 58952135