



Author	Dipl.-Ing. Daniel Mrskos, BSc
Funktion	CEO von Security mit Passion, Penetration Tester, Mentor, FH-Lektor, NIS Prüfer
Datum	14. Juni 2024
	
Zertifizierungen	CSOM, CRTL, eCPTXv2, eWPTXv2, CCD, eCTHPv2, CRTE, CRTO, eCMAP, PNPT, eCPPTv2, eWPT, eCIR, CRTP, CARTP, PAWSP, eMAPT, eCXD, eCDFP, BTL1 (Gold), CAPEN, eEDA, OSWP, CNSP, Comptia Pentest+, ITIL Foundation V3, ICCA, CCNA, eJPTv2, Developing Security Software (LFD121), CAP, Checkmarx Security Champion
LinkedIn	https://www.linkedin.com/in/dipl-ing-daniel-mrskos-bsc-0720081ab/
Website	https://security-mit-passion.at

Richtlinie für das Security Operations Center (SOC)

Datum: [Heutiges Datum]

Einleitung

Diese Richtlinie für das Security Operations Center (SOC) definiert die Anforderungen und Maßnahmen zur Sicherstellung der Sicherheit und des Schutzes der IT-Infrastruktur von [Unternehmen] durch das SOC. Diese Richtlinie basiert auf den Best Practices und Empfehlungen von Check Point, Solink, dem Canadian Centre for Cyber Security, ISACA und RSISecurity sowie auf den Standards ISO 27001:2022, ISO 27002:2022, CIS Controls v8, BSI C5:2020, der Cloud Controls Matrix (CCM), dem NIST Cybersecurity Framework, dem NIS2 Draft, der OH SZA für KRITIS, dem European Cyber Resilience Act, DORA und den OWASP Best Practices.

Geltungsbereich

Diese Richtlinie gilt für alle Mitarbeiter, Auftragnehmer, Berater, Zeitarbeitskräfte, Praktikanten und mit Dritten verbundene Personen, die im Security Operations Center (SOC) von [Unternehmen] tätig sind.

Compliance Matrix

Die Compliance Matrix dient dazu, die Konformität dieser Richtlinie für das SOC mit den relevanten Sicherheitsstandards und -richtlinien zu gewährleisten. Sie zeigt die Zuordnung der einzelnen Policy-Komponenten zu den spezifischen Anforderungen der Standards wie ISO 27001:2022, CIS Controls V8, BSI C5:2020, der Cloud Controls Matrix (CCM), dem NIST Cybersecurity Framework, dem NIS2 Draft, der OH SZA für KRITIS, dem European Cyber Resilience Act und DORA. Dies erleichtert die Nachverfolgung und Überprüfung, dass alle notwendigen Sicherheitsmaßnahmen implementiert sind und ermöglicht eine klare, transparente Dokumentation unserer Compliance-Verpflichtungen.

Policy-Komponente	ISO 27001:2022 / 27002:2022	TISAX	CIS Controls V8	BSI C5:2020	CCM	NIST CSF	NIS2	OH SzA	European CRA	DORA
SOC Policy und Programmmanagement	8.26.1, 8.26.2	1.1.1, 1.2.1	4.1, 4.2	ORP1, ORP2	IAM-01, IAM-02	PR.IP-1, PR.IP-2	Artikel 5, 6.1	Abschnitt 2.3	Artikel 23	Artikel 4
Sicherheitsüberwachung und Bedrohungserkennung	8.26.1, 8.26.2	2.1.1, 2.1.2	6.1, 6.2	ORP3, ORP4	IAM-03, IAM-04	DE.CM-1, DE.CM-2	Artikel 5, 6.2	Abschnitt 2.4	Artikel 23	Artikel 4
Incident Response und Management	8.27.1, 8.27.2	3.1.1, 3.1.2	11.1, 11.2	ORP5, ORP6	IVS-01, IVS-02	RS.RP-1, RS.RP-2	Artikel 6.3	Abschnitt 2.5	Artikel 23	Artikel 4
Kontinuierliche Verbesserung und Lessons Learned	8.26.1, 8.26.2	4.1.1, 4.1.2	17.1, 17.2	OPS3, OPS4	IVS-03, IVS-04	PR.IP-3, PR.IP-4	Artikel 6.4	Abschnitt 2.6	Artikel 23	Artikel 4
Schulung und Bewusstsein	8.26.1, 8.26.2	3.2.1, 3.2.2	13.1, 13.2	ORP7, ORP8	IAM-05, IAM-06	PR.AT-1, PR.AT-2	Artikel 6.5	Abschnitt 2.7	Artikel 23	Artikel 4
Zusammenarbeit und Kommunikation	8.26.1, 8.26.2	2.2.1, 2.2.2	13.4, 13.5	ORP9, ORP10	IVS-03, IVS-04	PR.IP-5, PR.IP-6	Artikel 6.8	Abschnitt 2.9	Artikel 23	Artikel 4
Technologien und Tools	8.26.1, 8.26.2	3.3.1, 3.3.2	5.4, 5.5	ORP11, ORP12	DSI-01, DSI-02	PR.PT-1, PR.PT-2	Artikel 6.10	Abschnitt 2.11	Artikel 23	Artikel 4
Physische Sicherheit des SOC	8.26.1, 8.26.2	3.4.1, 3.4.2	8.1, 8.2	ORP13, ORP14	DSI-03, DSI-04	PR.IP-7, PR.IP-8	Artikel 6.12	Abschnitt 2.13	Artikel 23	Artikel 4

Richtlinien und Anforderungen

SOC Policy und Programmmanagement

Ein umfassendes SOC-Programm muss entwickelt und implementiert werden, um die Sicherheit der IT-Infrastruktur von [Unternehmen] zu gewährleisten (ISO 27001: 8.26.1, 8.26.2). Dies umfasst die Entwicklung einer Policy, die Rollen und Verantwortlichkeiten definiert, sowie die regelmäßige Überprüfung und Aktualisierung der Policy (CIS Controls 4.1, 4.2, TISAX 1.1.1, 1.2.1). Regelmäßige Schulungen und Sensibilisierungsmaßnahmen sind notwendig, um sicherzustellen, dass alle Mitarbeiter die Policy verstehen und umsetzen können (NIST CSF PR.IP-1, PR.IP-2, BSI C5: ORP1, ORP2, CCM IAM-01, IAM-02).

Sicherheitsüberwachung und Bedrohungserkennung

Eine kontinuierliche Überwachung der IT-Infrastruktur und die Erkennung von Bedrohungen sind wesentliche Bestandteile eines effektiven SOC (ISO 27001: 8.26.1, 8.26.2). Dies umfasst die Implementierung von Sicherheitsüberwachungssystemen und Bedrohungsanalysewerkzeugen (CIS Controls 6.1, 6.2, TISAX 2.1.1, 2.1.2). Regelmäßige Überprüfungen und Tests der Überwachungssysteme sind notwendig, um ihre Wirksamkeit sicherzustellen (NIST CSF DE.CM-1, DE.CM-2, BSI C5: ORP3, ORP4, CCM IAM-03, IAM-04).

Incident Response und Management

Ein effektiver Incident-Response- und Management-Prozess muss implementiert werden, um auf Sicherheitsvorfälle schnell und effektiv reagieren zu können (ISO 27001: 8.27.1, 8.27.2). Dies umfasst die Identifizierung, Analyse und Behebung von Sicherheitsvorfällen sowie die Dokumentation und Berichterstattung der Vorfälle (CIS Controls 11.1, 11.2, TISAX 3.1.1, 3.1.2). Regelmäßige Übungen und Überprüfungen des Incident-Response-Plans sind notwendig, um sicherzustellen, dass alle Beteiligten auf Vorfälle vorbereitet sind (NIST CSF RS.RP-1, RS.RP-2, BSI C5: ORP5, ORP6, CCM IVS-01, IVS-02).

Kontinuierliche Verbesserung und Lessons Learned

Ein Prozess zur kontinuierlichen Verbesserung und zur Nutzung von Lessons Learned muss implementiert werden, um die Effektivität des SOC kontinuierlich zu steigern (ISO 27001: 8.26.1, 8.26.2). Dies umfasst die Analyse vergangener Vorfälle, die Implementierung von Verbesserungsmaßnahmen und die regelmäßige Überprüfung der Prozesse (CIS Controls 17.1, 17.2, TISAX 4.1.1, 4.1.2). Regelmäßige Überprüfungen und Anpassungen der SOC-Prozesse sind notwendig, um ihre Wirksamkeit sicherzustellen (NIST CSF PR.IP-3, PR.IP-4, BSI C5: OPS3, OPS4, CCM IVS-03, IVS-04).

Schulung und Bewusstsein

Alle Mitarbeiter müssen regelmäßig Schulungen zur sicheren Überwachung und Verwaltung der IT-Infrastruktur durchlaufen (ISO 27001: 8.26.1, 8.26.2). Diese Schulungen müssen die aktuellen Bedrohungen, Sicherheitsmaßnahmen und Best Practices abdecken (CIS Controls 13.1, 13.2, TISAX 3.2.1, 3.2.2). Sensibilisierungsmaßnahmen müssen implementiert werden, um sicherzustellen, dass alle Mitarbeiter über die aktuellen Sicherheitsanforderungen informiert sind (NIST CSF PR.AT-1, PR.AT-2, BSI C5: ORP7, ORP8, CCM IAM-05, IAM-06).

Zusammenarbeit und Kommunikation

Effektive Zusammenarbeit und Kommunikation sind wesentliche Bestandteile eines erfolgreichen SOC (ISO 27001: 8.26.1, 8.26.2). Dies umfasst die Implementierung von Kommunikationsprotokollen und die Förderung der Zusammenarbeit zwischen verschiedenen Teams und Abteilungen (CIS Controls 13.4, 13.5, TISAX 2.2.1, 2.2.2). Regelmäßige Überprüfungen und Tests der Kommunikationsprotokolle sind notwendig, um ihre Wirksamkeit sicherzustellen (NIST CSF PR.IP-5, PR.IP-6, BSI C5: ORP9, ORP10, CCM IVS-03, IVS-04).

Technologien und Tools

Die Auswahl und Implementierung geeigneter Technologien und Tools ist entscheidend für den Betrieb eines effektiven SOC (ISO 27001: 8.26.1, 8.26.2). Dies umfasst die Implementierung von SIEM-Systemen, Bedrohungsanalyse-Tools und Automatisierungswerkzeugen (CIS Controls 5.4, 5.5, TISAX 3.3.1, 3.3.2). Regelmäßige Überprüfungen und Aktualisierungen der Technologien und Tools sind notwendig, um sicherzustellen, dass sie den aktuellen Sicherheitsanforderungen entsprechen (NIST CSF PR.PT-1, PR.PT-2, BSI C5: ORP11, ORP12, CCM DSI-01, DSI-02).

Physische Sicherheit des SOC

Die physische Sicherheit des SOC muss gewährleistet sein, um unbefugten Zugriff und physische Bedrohungen zu verhindern (ISO 27001: 8.26.1, 8.26.2). Dies umfasst die Implementierung von Zugangskontrollsystemen, Überwachungskameras und anderen physischen Sicherheitsmaßnahmen (CIS Controls 8.1, 8.2, TISAX 3.4.1, 3.4.2). Regelmäßige Überprüfungen und Tests der physischen Sicherheitsmaßnahmen sind notwendig, um ihre Wirksamkeit sicherzustellen (NIST CSF PR.IP-7, PR.IP-8, BSI C5: ORP13, ORP14, CCM DSI-03, DSI-04).

Verantwortliche

Die Implementierung und Einhaltung dieser Richtlinie liegt in der Verantwortung des SOC-Leiters und des Security Operations Teams. Alle Mitarbeiter sind verpflichtet, sich an diese Richtlinie zu halten und jegliche Verstöße umgehend zu melden.

Quellen und Referenzen

Quelle	Zweck	Link
ISO27001:2022	Aufbau und Implementierung eines ISMS	ISO 27001:2022
CIS Controls v8	Sicherheitsmaßnahmen gegen Cyberangriffe	CIS Controls v8
BSI C5:2020	Cloud Security Standard	BSI C5:2020
Cloud Controls Matrix (CCM)	Sicherheitskontrollen für Cloud-Dienste	Cloud Controls Matrix
NIST Cybersecurity Framework	Rahmenwerk zur Verbesserung der Cybersicherheit	NIST CSF
NIS2 Draft	EU-Richtlinie zur Netz- und Informationssicherheit	NIS2 Draft
OH SzA für KRITIS	Orientierungshilfe Angriffserkennung für Kritische Infrastrukturen	OH SzA
European Cyber Resilience Act	EU-Verordnung zur Cyber-Resilienz	European CRA
Digital Operational Resilience Act (DORA)	EU-Verordnung zur digitalen operationellen Resilienz	DORA
Check Point: Security Operations Center (SOC) Best Practices	Best Practices für SOC	Check Point
Solink: Security Operations Center Best Practices	Best Practices für SOC	Solink
Canadian Centre for Cyber Security: Best Practices for Setting Up a SOC	Best Practices für SOC	Canadian Centre for Cyber Security
ISACA: Best Practices for Setting Up a Cybersecurity Operations Center	Best Practices für SOC	ISACA
RSISecurity: NIST Security Operations Center Best Practices	Best Practices für SOC	RSISecurity

Diese Quellen und Referenzen bieten umfassende Leitlinien und Best Practices für die Entwicklung und Implementierung von Sicherheitsmaßnahmen sowie für die Einhaltung der relevanten Standards und Richtlinien. Sie dienen als Grundlage und Unterstützung bei der Implementierung und Aufrechterhaltung eines effektiven Security Operations Center (SOC) bei [Unternehmen].

Dokumentinformationen

Titel: Richtlinie für das Security Operations Center (SOC)

Version: 1.0

Datum: [Heutiges Datum]

Verantwortlich: SOC-Leiter

Genehmigt von: [Name der genehmigenden Person]

Nächste Überprüfung: [Datum der nächsten Überprüfung]