Trovent MDR
(Managed Detection & Response)

Erfüllung des

Mindeststandards des BSI zur Protokollierung und Detektion von Cyber-Angriffen

(nach § 8 Absatz 1 Satz 1 BSIG – Version 2.1 vom 11.11.2024)

Inhaltsverzeichnis

1 Einleitung

Im Mindestandard vom 11.11.2024 beschreibt das BSI den Standard mit folgenden einleitenden Worten:

„Der Mindeststandard ‚Protokollierung und Detektion von Cyber-Angriffen' (MST PD) definiert gemäß § 8 Abs. 1 BSIG das **Mindestniveau für die Informationssicherheit des Bundes im Bereich der Protokollierung von Ereignissen und in der Detektion von daraus folgenden sicherheitsrelevanten Ereignissen** (SRE), um ein zielgerichtetes und einheitliches Vorgehen zur Erkennung und Abwehr von Cyber-Angriffen auf die Kommunikationstechnik des Bundes (§ 2 Abs. 3 S. 1 BSIG) zu etablieren. Der Mindeststandard beschreibt den dazu notwendigen Rahmen und eine strategische Vorgehensweise, die situationsunabhängig für eine angemessene Protokollierung und Detektion im jeweiligen Kontext angewendet werden muss."

Das vorliegende Dokument beschreibt in den folgenden Kapiteln inwieweit eine Organisation durch den Einsatz von Trovent MDR (Managed Detection & Response) in die Lage versetzt wird, die spezifischen Anforderungen des BSI Mindeststandards für Protokollierung und Detektion von Cyber-Angriffen zu erfüllen. In tabellarischer Form werden folgende Anforderungssammlungen behandelt:

- Anforderungen aus dem Mindeststandard *Protokollierung und Detektion von Cyber-Angriffen* selbst
- Anforderungen aus den dem Mindeststandard zugrundeliegenden IT-Grundschutz-Bausteinen *OPS.1.1.5 Protokollierung* und *DER.1 Detektion von sicherheitsrelevanten Ereignissen*

2 Trovent MDR: Erfüllung BSI Mindeststandard Protokollierung und Detektion

Die nachfolgende Tabelle enthält jede im BSI Mindeststand erwähnte Anforderung. Für jede Anforderungen führt die Tabelle folgende Informationen:

- eine Klassifikation als MUSS-, SOLLTE- oder KANN-Anforderung
- einen Querverweis auf jeweils zutreffende IT-Grundschutz-Bausteine
- eine Kennzeichnung, ob die jeweilige Anforderung durch den Einsatz von Trovent MDR erfüllt wird
- eine Kennzeichnung, ob die jeweilige Anforderung auch im Falle des Einsatzes von Trovent MDR im Verantwortungsbereich des Auftraggebers (AG) verbleibt
- ergänzende Anmerkungen zur Umsetzung der Anforderung

Die Nummerierung der Anforderungen ist in unveränderter Form dem Mindestandard vom 11.11.2024 entnommen. Die Querverweise auf IT-Grundschutz-Bausteine sind den Fußnoten des Mindeststandards entnommen worden und beziehen sich fast ausschließlich auf *OPS.1.1.5 – Protokollierung* und *DER.1 Detektion von sicherheitsrelevanten Ereignissen.*

Nr.	Art	Anforderung	IT-GS Baustein	Erfüllung durch Trovent MDR	Aufgabe des AG	Anmerkungen
2.1	**ALLGEMEINE ANFORDERUNGEN**					
PD.2.1.01	**Aufgabenbereiche**					
PD.2.1.01	MUSS	Zuständigkeit und Verantwortung für die Aufgabenbereiche Operative IT-Sicherheit, IT-Betrieb und Revision MÜSSEN gemäß Kapitel 1.1.3 verbindlich festgelegt werden, zum Beispiel unter Zuhilfenahme des Geschäftsverteilungsplans der Einrichtung.		Nein	X	
PD.2.1.02	**Sensibilisierung der Mitarbeitenden**					
PD.2.1.02	MUSS	Es MUSS eine Sensibilisierung der Mitarbeitenden in Bezug auf die Protokollierung und Detektion erfolgen.	DER.1.A4	Nein	X	Sensibilisierung der Mitarbeiter muss seitens des AG stattfinden.
PD.2.1.03	**Grundlegende Anforderungen**					
PD.2.1.03	MUSS	Einrichtungen MÜSSEN die Basis- und Standardanforderungen der IT-Grundschutz-Bausteine **OPS.1.1.5 Protokollierung** und **DER.1 Detektion von sicherheitsrelevanten Ereignissen** umsetzen.	OPS.1.1.5 DER.1	Ja	X	Siehe Kap. 3 - Trovent MDR: Erfüllung der Anforderungen des IT-Grundschutz-Bausteins OPS.1.1.5 – Protokollierung Siehe Kap. 4 - Trovent MDR: Erfüllung der Anforderungen des IT-Grundschutz-Bausteins DER.1 – Detektion von sicherheitsrelevanten Ereignissen
PD.2.1.03	MUSS	Es MUSS Personal speziell damit beauftragt werden, alle Protokoll- und Protokollierungsdaten zu überwachen.	DER.1.A6 DER.1.A7 DER.1.A14	Ja		Die Überwachung der Daten ist Bestandteil des Trovent MDR Lösung (Managed Service).
PD.2.1.03	MUSS	Das beauftragte Personal MUSS die notwendigen Fachkenntnisse für diese Aufgabe erhalten.		Ja		
PD.2.1.03	MUSS	Ein Personenkreis MUSS benannt werden, der für das Thema Auswertung von Protokoll- und Protokollierungsdaten verantwortlich ist.		Ja		
PD.2.1.03	MUSS	Komponenten an zentraler Stelle innerhalb der Infrastruktur MÜSSEN eingesetzt werden, um sicherheitsrelevante Ereignisse zu erkennen und auszuwerten.	DER.1.A6 DER.1.A15	Ja		
PD.2.1.03	MUSS	Zentrale, automatisierte Analysen mit Softwaremitteln MÜSSEN eingesetzt werden.		Ja		
PD.2.1.03	MUSS	Mit diesen zentralen, automatisierten Analysen MÜSSEN alle in der Systemumgebung anfallenden Ereignisse ermittelt und ggfs. in Bezug zueinander gesetzt werden.		Ja		
PD.2.1.03	MUSS	Alle eingelieferten Daten MÜSSEN lückenlos einsehbar und auswertbar sein.		Ja		
PD.2.1.03	MUSS	Die eingelieferten Daten MÜSSEN permanent ausgewertet werden.		Ja		
PD.2.1.03	MUSS	Werden definierte Schwellwerte überschritten oder bestätigte Verdachtsfälle erkannt, MUSS automatisch alarmiert werden.		Ja		
PD.2.1.03	MUSS	Das Personal MUSS sicherstellen, dass bei einem Alarm unverzüglich eine qualifizierte und dem Bedarf entsprechende Reaktion eingeleitet wird.		Ja		Die hierfür notwendigen Melde- und Eskalationswege zwischen Trovent und AG müssen klar definiert sein.
PD.2.1.03	MUSS	In diesem Zusammenhang MÜSSEN die Zuständigen und die Beteiligten des Kommunikationsvorgangs sofort informiert werden.		Ja		Ansprechpartner / Systemverantwortliche auf AG-Seite müssen definiert sein.

Nr.	Art	Anforderung	IT-GS Baustein	Erfüllung durch Trovent MDR	Aufgabe des AG	Anmerkungen
PD.2.1.03	MUSS	Die Systemverantwortlichen MÜSSEN regelmäßig die Analyseparameter auditieren und anpassen, falls dies erforderlich ist.		Ja		Bestandteil der Trovent MDR-Lösung.
PD.2.1.03	MUSS	Zusätzlich MÜSSEN bereits überprüfte Protokoll- und Protokollierungsdaten regelmäßig hinsichtlich sicherheitsrelevanter Ereignisse automatisch untersucht werden.		Ja		
PD.2.1.03	KANN	Die Umsetzung der Detektion KANN ausgelagert werden.		N/A	X	Diese Möglichkeit wird durch den AG durch Einsatz von Trovent MDR (Managed Service) genutzt.
PD.2.1.03	SOLLTE	IT-Dienstleister und andere Einrichtungen, die über erhöhte Ressourcen für die Detektion verfügen, SOLLTEN eine eigenständige Protokollierungs- und Detektionsinfrastruktur konzipieren und nutzen.		Ja		Trovent MDR kann „on-premise“ als eigenständige Protokollierungs- und Detektionsinfrastruktur betrieben werden.
PD.2.1.04	**Bestimmung und Einhaltung rechtlicher und vertraglicher Rahmenbedingungen**					
PD.2.1.04	MUSS	Es MUSS eine Bestimmung der rechtlichen und vertraglichen Rahmenbedingungen im Zusammenhang mit der Protokollierung und Detektion durchgeführt werden	OPS.1.1.5.A5 DER.1.A2	Ja	X	Ein Vertrag wird im Einzelfall zwischen AG und Trovent abgestimmt. Hierbei werden u.a. Regelungen hinsichtlich der Pseudonymisierung von Daten und Aufbewahrungsfristen geklärt.
PD.2.1.04	MUSS	Die Anforderungen aus den Ergebnissen der Bestimmung rechtlicher und vertraglicher Rahmenbedingungen MÜSSEN bei der Festlegung der Sichtbarkeiten zur Auswahl von Datenquellen eingehalten werden.		Ja		
PD.2.1.04	DARF NUR	Es DÜRFEN NUR die Daten erhoben werden, für die die Legitimität geprüft worden ist.		Ja		
PD.2.1.04	MUSS	Aus den geltenden rechtlichen und vertraglichen Rahmenbedingungen MUSS eine konforme Speicherfrist für die Protokollierung identifiziert und angewendet werden.	OPS.1.1.5.A8	Ja		Speicherfristen können quellenspezifisch konfiguriert werden.
PD 2.1.04	SOLLTE	Die Speicherdauer aller Protokoll- und Protokollierungsdaten SOLLTE, je nach Ergebnis der internen Prüfung der rechtlichen und vertraglichen Rahmenbedingungen, auf bspw. 90 Tage festgelegt werden		Ja		Speicherfristen können quellenspezifisch konfiguriert und mit dem AG abgestimmt werden.
PD.2.1.04	MUSS	Es MUSS sichergestellt werden, dass die Protokoll- und Protokollierungsdaten nach Ablauf der Speicherfrist gelöscht werden.		Ja		
PD 2.1.04	KANN	Sicherheitsrelevante Ereignisse (sofern keine personenbeziehbaren Informationen enthalten sind) und allgemeine Ereignisse, die nachweislich einem Cyberangriff zugeordnet wurden, KÖNNEN von dieser Löschung ausgenommen werden.		Ja		
PD.2.1.05	**Protokollierung und Detektion bei Bezug von IT-Dienstleistungen**					
PD.2.1.05	MUSS	Einrichtungen, die Teile ihrer IT bei einem Dienstleister ausgelagert haben, MÜSSEN sicherstellen, dass die Anforderungen dieses Mindeststandards auch im Rahmen der Auslagerung berücksichtigt werden.		Ja	X	Es besteht die Möglichkeit Protokolldaten auch von Dienstleistern (z.B. auch über abgesetzte Log-Kollektoren) einzusammeln. Die rechtlichen / organisatorischen Voraussetzungen hierfür sind hier aber vom AG mit dem Dienstleister zu klären.
PD.2.1.05	MUSS	Alle Aspekte der Protokollierung und Detektion, die im Rahmen der Dienstleistungserbringung gemäß dieses Mindeststandards festgelegt werden, MÜSSEN schriftlich zwischen den Parteien geregelt werden.		Ja	X	Der AG muss entsprechende Vereinbarungen mit seinen Dienstleistern treffen.

Nr.	Art	Anforderung	IT-GS Baustein	Erfüllung durch Trovent MDR	Aufgabe des AG	Anmerkungen
PD.2.1.05	SOLLTE	Es SOLLTE sichergestellt werden, dass die Einrichtung Zugriff auf die Protokoll- und Protokollierungsdaten sowie auf die Sekundär-SRE der ausgelagerten Systeme erhält.		Ja	X	
PD.2.1.05	SOLLTE	Dies SOLLTE über eine kontinuierliche Datenübertragung der Protokoll- und Protokollierungsdaten sowie der Sekundär-SRE zu einem zentralen System realisiert werden.		Ja	X	
PD.2.1.05	KANN	Wenn eine Datenübertragung nicht möglich ist, KANN alternativ eine unmittelbare Meldung des Dienstleisters bei sicherheitsrelevanten Ereignissen mit der Möglichkeit zur nachfolgenden Übersendung der Protokoll- und Protokollierungsdaten sowie der Sekundär-SRE etabliert werden.		Nein	X	Falls dies zutreffend ist, müssen durch den AG entsprechende organisatorische Voraussetzungen getroffen werden.
PD.2.1.05	MUSS	Sollten einer Partei Erkenntnisse über einen Angriff in Bezug auf die ausgelagerten Infrastrukturen vorliegen, MUSS sichergestellt sein, dass die jeweils andere Partei unmittelbar informiert wird, um gemeinsam reaktive Maßnahmen zu etablieren.		Ja	X	Organisatorische Voraussetzungen müssen durch den AG geschaffen werden, so dass der Informationsfluss zwischen Dienstleister und dem Trovent MDR SOC gewährleistet ist.
2.2	**PROTOKOLLIERUNG**					
PD.2.2.01	**Organisatorische und personelle Rahmenbedingungen zur Protokollierung**					
PD.2.2.01	MUSS	Die organisatorischen und personellen Rahmenbedingungen für die effektive Umsetzung des oben definierten Protokollierungsprozesses, der sich daraus ergebenen Aufgaben für Planen, Sammeln und Dokumentieren sowie für die Umsetzung der Anforderungen dieses Mindeststandards MÜSSEN geschaffen werden.	ISMS.1.A6	Ja	X	Im Rahmen der Leistungserbringung von Trovent MDR sind die entsprechenden organisatorischen und personellen Rahmenbedingungen gegeben. AG-seitig muss sichergestellt werden, dass die notwendigen Kommunikations- und Eskalationswege zur Verfügung stehen und der Zugriff auf die Log-Quellen gegeben ist.
PD.2.2.02	**Planungs- und Dokumentationsphase der Protokollierung**					
PD.2.2.02	SOLLTE	Die Erschließung von Datenquellen SOLLTE auf Basis der Schutzbedarfsfeststellungen im Informationsverbund priorisiert erfolgen.		Ja	X	In Zusammenarbeit mit dem AG.
PD.2.2.02	MUSS	Sollten für die im Einsatz befindlichen oder geplanten Detektoren und Detektionssysteme zusätzliche Sichtbarkeiten notwendig sein, MÜSSEN diese erschlossen werden		Ja	X	In Zusammenarbeit mit dem AG.
PD.2.2.02	KANN	Es KÖNNEN „Quick-Wins“ in der Protokollierung berücksichtigt werden.		Ja		Mit Beginn der Inbetriebnahme von Trovent MDR stehen eine Vielzahl von Log-Konnektoren und Log-Parsern zur Verfügung, um entsprechende „Quick-Wins“ zu erzielen.
PD.2.2.02	MUSS	Es MUSS sichergestellt werden, dass trotz der Protokollierung die Betriebssicherheit gewährleistet bleibt.		Ja	X	Die Betriebssicherheit wird durch den Einsatz von Trovent MDR nicht beeinträchtigt. Die Gewährleistung der Betriebssicherheit verbleibt unverändert im Verantwortungsbereich des AG.
PD.2.2.02	SOLLTE	Das anfallende Protokoll- und Protokollierungsdatenaufkommen SOLLTE anhand eines repräsentativen Systems pro IT-Systemgruppe bestimmt werden.		Ja		
PD.2.2.02	MUSS	Bei der Erschließung von Datenquellen MUSS geprüft werden, ob sich das Datenformat für die Detektionssysteme eignet.	OPS.1.1.5.A9	Ja		

Nr.	Art	Anforderung	IT-GS Baustein	Erfüllung durch Trovent MDR	Aufgabe des AG	Anmerkungen
PD.2.2.02	MUSS	Es MUSS geprüft werden, ob die Daten normalisiert und, falls erforderlich, durch zusätzliche Informationen angereichert werden müssen. Daraus KÖNNEN sich Normalisierungsregeln für Logformate ableiten.		Ja		
PD.2.2.02	MUSS	Die Ergebnisse der Planungsphase MÜSSEN in einer geeigneten Dokumentation zusammengefasst werden.		Teilweise	X	Dokumentation der Planungsphase liegt im Verantwortungsbereich des AG; Trovent kann hierbei nach Bedarf unterstützen.
PD.2.2.02	SOLLTE	Eine geeignete Abstraktion SOLLTE sicherstellen, dass die Dokumentation keinen ständigen Änderungen unterliegt.		Teilweise	X	
PD.2.2.02	MUSS	Die Dokumentation MUSS alle Netzbereiche, die Datenquellen, deren Beziehungen untereinander und den Datenfluss der Protokoll- und Protokollierungsdaten sowie der Sekundär-SRE im Informationsverbund umfassen.		Teilweise	X	
PD.2.2.02	MUSS	Darüber hinaus MUSS für jedes System dokumentiert werden, welche Ereignisse dieses protokolliert.		Teilweise	X	
PD.2.2.02	SOLLTE	Es SOLLTE eine Gruppierung gleicher Systemgruppen innerhalb der Dokumentation erfolgen.		Teilweise	X	
PD.2.2.02	MUSS	Es MUSS ein Prozess eingerichtet werden, der sicherstellt, dass die Planungsphase bei grundlegenden Veränderungen im Informationsverbund, die Auswirkung auf die Protokollierung und Detektion haben, erneut durchlaufen wird.		Teilweise	X	In Zusammenarbeit mit dem AG.
PD.2.2.02	MUSS	Jede Einrichtung bzw. im Auftrag der jeweilige IT-Dienstleister des Bundes MUSS eine auf den konkreten Informationsverbund abgestimmte spezifische Sicherheitsrichtlinie für die Protokollierung erstellen.	OPS.1.1.5.A1	Nein	X	Liegt im Verantwortungsbereich des AG.
PD.2.2.03	**Umsetzungsphase der Protokollierung**					
PD.2.2.03	MUSS	Jede Einrichtung MUSS die Protokoll- und Protokollierungsdaten in einer zentralisierten Protokollierungsinfrastruktur speichern.	DER.1.A11 OPS.1.1.5.A6 OPS.1.1.5.A10	Ja		
PD.2.2.03	SOLLTE	Die Protokollierungsinfrastruktur SOLLTE in einer physikalisch dedizierten Zone ohne Internetverbindung betrieben werden.		Teilweise		Der Zugriff des Trovent MDR SOC auf die Protokollierungsinfrastruktur erfolgt über eine Site-2-Site IPSEC VPN-Verbindung. Über diese Verbindung werden auch notwendige Systemupdates eingespielt.
PD.2.2.03	MUSS	Der Zugriff auf die Protokollierungsinfrastruktur sowie die Protokoll- und Protokollierungsdaten MUSS restriktiv konfiguriert und überwacht werden.		Ja		

Nr.	Art	Anforderung	IT-GS Baustein	Erfüllung durch Trovent MDR	Aufgabe des AG	Anmerkungen
PD.2.2.03	MUSS	Die Protokollierungsinfrastruktur MUSS derart dimensioniert werden, dass die protokollierten Ereignisse für die doppelte Dauer der identifizierten Speicherfrist (siehe PD.2.1.04) vorgehalten werden könnten.		Ja		Aufgrund der Komplexität heutiger Informationsverbünde und vielfältiger Angriffsszenarien ist ein stetiger Anstieg des Protokollierungsvolumens zu erwarten. Eine regelmäßige Überwachung der Logvolumina und verfügbarer Speicherkapazitäten stellt sicher, dass die Protokollierungsinfrastruktur für die aktuellen bzw. die zu erwartenden Volumina ausreichend dimensioniert ist und bei Bedarf erweitert werden kann.
PD.2.2.03	SOLLTE	Die verwaltungsinternen Angebote des Bundes zur Protokollierung SOLLTEN genutzt werden.		N/A		
PD.2.2.03	SOLLTE	Vorhandene Konfigurationsvorgaben des BSI SOLLTEN als Basiskonfiguration für die Protokollierung auf IT-System- und Netz-Sicht verwendet werden.		Nein	X	Die IT Systeme müssen vom AG selbst nach BSI-Vorgaben konfiguriert werden. Trovent kann bei Bedarf unterstützen.
PD.2.2.03	KANN	Sollten betriebliche Aspekte oder die Geschäftstätigkeit der Einrichtung durch diese Vorgaben eingeschränkt werden, KANN eine abweichende Konfiguration vorgenommen werden.		Nein	X	
PD.2.2.03	MUSS	Falls keine Konfigurationsvorgaben des BSI existieren oder abweichende Konfigurationen aufgrund der oben genannten Kriterien vorgenommen werden müssen, MÜSSEN die von den Systemen als sicherheitsrelevant ausgegebenen Ereignisse (Protokoll- und Protokollierungsdaten oder Sekundär-SRE) protokolliert werden.		Ja		Werden automatisch vom Trovent MDR-System protokolliert.
PD.2.2.03	DARF NICHT	Zusätzliche behördenspezifische Einstellungen KÖNNEN ergänzend vorgenommen werden. Diese Einstellungen DÜRFEN NICHT herstellerspezifische oder intern etablierte Vorgaben zur Protokollierung ersetzen, sondern erweitern diese.		Ja	X	In Zusammenarbeit zwischen AG und Trovent.
PD.2.2.03	MUSS	Nach erfolgreichem Abschluss der Umsetzungsphase MUSS geprüft werden, ob alle geplanten Datenquellen der Planungs- und Dokumentationsphase erschlossen wurden.	OPS.1.1.5.A4	Ja	X	In Zusammenarbeit zwischen AG und Trovent.
PD.2.2.03	MUSS	Die Kompatibilität der Datenformate, der angestrebte Informationsgehalt (vgl. Sichtbarkeit) sowie die Zeitsynchronisation der Daten MUSS überprüft werden.		Ja		
PD.2.2.03	MUSS	Sofern erforderlich, MUSS eine Aktualisierung der Dokumentation erfolgen.		Teilweise	X	Dokumentation liegt beim AG; Trovent kann unterstützen
PD.2.2.04	**Protokollierung aus IT-System-Sicht**					
PD.2.2.04	MUSS	Die Auslegung der Sichtbarkeiten für die Protokollierung aus IT-System-Sicht MUSS quellenspezifisch entschieden werden. Sollten Konfigurationsvorgaben vom BSI existieren, MÜSSEN diese berücksichtigt werden (siehe PD.2.2.03.b).	OPS.1.1.5.A3	Ja		
PD.2.2.04	SOLLTE	Um ein einheitliches Schutzniveau zu schaffen, SOLLTEN mindestens aus den folgenden Kategorien Ereignisse protokolliert werden:		Ja		Grundsätzlich können durch Trovent MDR alle Protokollierungsdaten

Nr.	Art	Anforderung	IT-GS Baustein	Erfüllung durch Trovent MDR	Aufgabe des AG	Anmerkungen
		• Anlegen und Änderungen von Rechten, Benutzenden und Gruppen				entgegengenommen und gespeichert werden. Die Protokollierung der genannten Kategorien ist jedoch abhängig von der entsprechenden Konfiguration der Quellsysteme. Diese liegt im Verantwortungsbereich der IT-Administratoren des AG. Trovent steht in diesem Zusammenhang unterstützend zur Verfügung.
		• Änderungen von Zugangsdaten				
		• Anmeldeversuche (erfolgreich und fehlgeschlagen), Abmeldungen und Zugriffe auf System-, Programm- und Dateiressourcen				
		• Systemstarts, Neustarts und Herunterfahren				
		• Ausführungen von Applikationen, Programmen und Skripten				
		• Installationen und Deinstallationen				
		• Konfigurations- und Systemänderungen				
		• Prozessinformationen (z. B. Start, Terminierung und Abhängigkeiten)				
		• System- / Datei-Integrität				
		• Sekundäre sicherheitsrelevante Ereignisse				
PD.2.2.04	SOLLTE	Je Datensatz SOLLTEN mindestens die folgenden Informationen erhoben werden, sofern dies möglich ist:		Ja		(siehe vorige Anmerkung)
		• Zeitstempel				
		• Quellsystem, ggf. Benutzer				
		• Event-IDs				
		• Ereignisinformationen				
PD.2.2.04	MUSS	Auf allen in der Planungs- und Dokumentationsphase identifizierten Systemen MUSS die Protokollierung aktiviert werden. Es SOLLTE dabei NICHT zwischen virtuellen und physischen Systemen unterschieden werden.		Ja		
PD.2.2.04	MUSS	Für Querschnittsdienste und Fachverfahren MUSS systemabhängig definiert werden, welche Ereignisse protokolliert werden und wie diese in die zentralisierte Protokollierung mit einzubinden sind.		Ja	X	
PD.2.2.04	SOLLTE	Die zu protokollierenden Ereignisse SOLLTEN über die Betriebssystemmittel und/oder über Agenten erfasst werden.		Ja		Trovent MDR sammelt die zu protokollierenden Ereignisse entweder über Syslog, NetFlow (Netzwerkverkehrsdaten) oder mittels Agenten ein (u.a. Winlogbeat, Auditbeat und Filebeat).
PD.2.2.04	SOLLTE	Ein Einsatz von Agenten SOLLTE vorab geprüft werden, um die Kompatibilität zur Protokollierungs- und Detektionsinfrastruktur zu gewährleisten.		Ja		
PD.2.2.04	MUSS	Die Zuordenbarkeit der Protokollierungsdaten zu deren Identitäten MUSS über die Gesamtheit der Speicherdauer gewährleistet werden.		Ja		
PD.2.2.04	SOLLTE	Auf IT-Systemebene SOLLTE es dazu eine eindeutige Bezeichnung (z. B. Hostname) geben, mit der die protokollierenden Systeme und deren Daten identifiziert werden können.		Ja	X	
PD.2.2.05	**Protokollierung aus Netz-Sicht**					
PD.2.2.05	MUSS	Die Auslegung der Sichtbarkeiten für die Protokollierung aus Netz-Sicht MUSS quellenspezifisch entschieden werden. Sollten Konfigurationsvorgaben vom BSI existieren, MÜSSEN diese berücksichtigt werden (siehe PD.2.2.03.b).	OPS.1.1.5.A3	Ja		
PD.2.2.05	SOLLTE	Um eine umfassende Sichtbarkeit zu schaffen, SOLLTEN mindestens die folgenden Bereiche protokolliert werden:		Ja		Grundsätzlich können durch Trovent MDR alle Protokollierungsdaten

Nr.	Art	Anforderung	IT-GS Baustein	Erfüllung durch Trovent MDR	Aufgabe des AG	Anmerkungen
		• Ein- und ausgehende Kommunikationen an allen Netzgrenzen (über entsprechende IT-Systeme, wie z. B., Proxies, Application Layer Gateways, Router; auch virtuelle Netzgrenzen) der relevanten Stufen aus Netz-Sicht				entgegengenommen und gespeichert werden. Die Protokollierung der genannten Kategorien ist jedoch abhängig von der entsprechenden Konfiguration der Quellsysteme. Diese liegt im Verantwortungsbereich der IT-Administratoren des AG. Trovent steht in diesem Zusammenhang unterstützend zur Verfügung.
		• Kommunikation innerhalb von Netzen und zwischen IT-Systemen der relevanten Stufen aus Netz-Sicht				
		• SRE der Netzwerkinfrastruktur				
PD.2.2.05	SOLLTE	Je Datensatz SOLLTEN mindestens die folgenden Informationen erhoben werden, sofern dies möglich ist:		Ja		(siehe vorige Anmerkung)
		• Zeitstempel				
		• Quellsystem				
		• Zielsystem				
		• Protokollinformationen				
PD.2.2.05	KANN	Es KÖNNEN zusätzlich Sensoriken eingesetzt werden, die zum Beispiel über Spiegelports (TAPs) die relevanten Protokolldaten aus Netz-Sicht protokollieren.		Ja		Für die Detektionsfunktionen von Trovent MDR sind NetFlow-Daten ausreichend; es erfolgt keine Analyse des Payloads von IP-Datenpaketen.
PD.2.2.05	MUSS	Die Zuordenbarkeit der Protokolldaten zu deren Identitäten MUSS über die Gesamtheit der Speicherdauer gewährleistet werden.		Ja		
PD.2.2.05	SOLLTE	Falls eine dynamische Zuordnung von IP-Adressen erfolgt, SOLLTEN zusätzliche Protokollierungsquellen (z. B. der DHCP-Server) erschlossen werden, um die Zuordenbarkeit über die Speicherdauer der Protokolldaten zu garantieren.		Ja		
PD.2.2.05	SOLLTE	Es SOLLTE mit geeigneten Maßnahmen (z. B. Reverse-DNS-Abfragen) sichergestellt werden, dass die Protokolldaten der Netz-Sicht den Protokollierungsdaten der IT-System-Sicht zuordenbar sind, sofern dies nicht durch die vorhergehende Maßnahme abgebildet werden kann.		Ja		Kann durch Trovent MDR umgesetzt werden.
2.3	**DETEKTION**					
PD.2.3.01	**Organisatorische und personelle Rahmenbedingungen zur Detektion**					
PD.2.3.01	MUSS	Die organisatorischen und personellen Rahmenbedingungen für die effektive Umsetzung des Detektionsprozesses , der sich daraus ergebenen Aufgaben für Planen, Kalibrieren, Detektieren, Auswerten und Dokumentieren sowie für die Umsetzung der Anforderungen dieses Mindeststandards MÜSSEN geschaffen werden.	DER.1.A7	Ja		Die organisatorischen und personellen Rahmenbedingungen (Kapazitäten) sind Bestandteil der Trovent MDR Dienstleistung.
PD.2.3.02	**Planungs- und Dokumentationsphase der Detektion**					
PD.2.3.02	MUSS	Die Einrichtung MUSS eine strategische Vorgehensweise für die Detektion festlegen. Folgende Kriterien sind bei der **Festlegung der Vorgehensweise zu berücksichtigen**:		Ja		

Nr.	Art	Anforderung	IT-GS Baustein	Erfüllung durch Trovent MDR	Aufgabe des AG	Anmerkungen
PD.2.3.02	SOLLTE	Zur Bestimmung der Abdeckung SOLLTE eine standardisierte Methodik angewendet werden, die es erlaubt Detektoren und Detektionssysteme zu den Vorgehensweisen von Cyber-Akteuren oder Arten von Cyber-Angriffen (z. B. über Matrizen zu Taktiken und Techniken von Cyber-Angriffen) zuzuordnen.		Ja		Alle von Trovent MDR eingesetzten Detektionsregeln / -methoden sind Taktiken bzw. Techniken des MITRE ATT&ACK Frameworks zugeordnet.
PD.2.3.02	MUSS	Es MUSS eine angemessene Abdeckung im Informationsverbund erzielt werden, die auf den theoretisch zu erkennenden Vorgehensweisen von Cyber-Akteuren oder Arten von Cyber-Angriffen basiert.	DER.1.A16	Ja		
PD.2.3.02	MUSS	Dazu MÜSSEN die Ergebnisse der Schutzbedarfsfeststellungen der Einrichtung in die Planung einbezogen werden.		Ja	X	Die Schutzbedarfsstellung muss vom AG geliefert werden, so dass diese Informationen in die Bewertung von SRE durch Trovent MDR (SOC Prozesse) einfließen können.
PD.2.3.02	SOLLTE	Bei der Produktauswahl, der Entwicklung oder dem Einsatz von Detektoren oder Detektionssystemen SOLLTE eine größtmögliche Abdeckung der Detektionsfähigkeit in Bezug auf die Bedrohungslandschaft der Einrichtung erzielt werden.		Ja	X	Trovent MDR bietet eine umfangreiche Detektionsabdeckung der Taktiken/Techniken des MITRE ATT&CK Frameworks.
PD.2.3.02	MUSS	Es MUSS eine auf den konkreten Informationsverbund abgestimmte spezifische Sicherheitsrichtlinie für die Detektion erstellt werden.	DER.1.A1	Nein	X	Liegt im Verantwortungsbereich des AG; Trovent kann unterstützen.
PD.2.3.02	SOLLTE	Die Einrichtung SOLLTE die verwaltungsinternen Detektionsangebote zur automatisierten Analyse der Protokoll- und Protokollierungsdaten auf sicherheitsrelevante Ereignisse nutzen. (Die zur Umsetzung verpflichteten Stellen können sich für Informationen zu den verwaltungsinternen Detektionsangeboten an das Bundes Security Operations Center (BSOC) des BSI wende)		N/A	X	
PD.2.3.02	MUSS	Informationen zu aktuellen technischen Schwachstellen und Angriffsmustern MÜSSEN fortlaufend für die im Informationsverbund eingesetzten Systeme eingeholt werden. Dazu MÜSSEN laufend Meldungen der Hersteller (Hard- und Software), Behörden und Medien geprüft werden.	DER.1.A12	Ja	X	Detektionsregeln/-methoden von Trovent MDR werden fortlaufend verbessert. Maßgeblich sind hierbei: - Neuerungen/Erweiterungen des MITRE ATT&CK Frameworks - Sigma Rule Repository - Elastic Detection Rules Ergebnisse aus bestehenden Schwachstellenscannern des AG können in das automatisch aufgebaute Kontextwissen über die IT-Infrastruktur (Trovent Context Engine) mit einbezogen werden, um so die Risikobewertung einzelner SRE zu präzisieren.
PD.2.3.03	**Umsetzungsphase der Detektion**					
PD.2.3.03	SOLLTE	Bei der Umsetzung von Maßnahmen zur Detektion SOLLTE initial eine Kalibrierung durchgeführt werden, um festzustellen, welche SRE im Normalzustand auftreten.		Ja		Das ist Bestandteil der Trovent MDR Dienstleistung. Ziel ist ein hohes Volumen an False Positives zu vermeiden.
PD.2.3.03	SOLLTE	Dazu SOLLTE bewertet werden, ob dieser Normalzustand hingenommen werden kann oder, ob die Feststellung genutzt werden sollte Änderungen durchzuführen, um das gewünschte Detektionsergebnis zu erzielen.		Ja		Das ist Bestandteil der fortlaufenden Trovent MDR Dienstleistung.

Nr.	Art	Anforderung	IT-GS Baustein	Erfüllung durch Trovent MDR	Aufgabe des AG	Anmerkungen
PD.2.3.03	SOLLTE	Die Kalibrierung SOLLTE bei Änderungen innerhalb des Informationsverbunds oder der Bedrohungslage erneut durchgeführt werden.		Ja		
PD.2.3.03	MUSS	Die SRE MÜSSEN überprüft und dahingehend bewertet werden, ob sie auf einen Verdachtsfall (qualifizierter SRE) hindeuten.		Ja		
PD.2.3.03	SOLLTE	Die zur Detektion eingesetzten Systeme SOLLTEN in eindeutig zuordenbaren Fällen eine automatisierte Auswertung der SRE ermöglichen.		Ja		
PD.2.3.03	DARF	Nur Verdachtsfälle DÜRFEN den Prozess der Reaktion auslösen.		Ja		
PD.2.3.03	MUSS	Die Qualifizierung MUSS in automatisiert nicht eindeutig zuordenbaren Fällen manuell durch die Einrichtung vorgenommen werden.		Ja		Das ist Aufgabe des Trovent SOC-Teams bzw. Bestandteil der Trovent MDR Dienstleistung.
PD.2.3.03	KANN	Für die Qualifizierung KÖNNEN weitere Erkenntnisse aus Protokoll- und Protokollierungsdaten sowie anderen SRE notwendig sein.		Ja		
PD.2.3.03	MUSS	Basierend auf den gewonnenen Erkenntnissen der Auswertung MÜSSEN die Detektionsmechanismen nachjustiert werden.		Ja		
PD.2.3.03	SOLLTE	Es SOLLTEN geeignete Evaluierungsprozesse definiert werden, um aus erfolgreich detektierten Vorfällen die notwendigen Maßnahmen zur Vorbeugung derartiger Vorfälle abzuleiten.	DER.1.A12	Teilweise	X	Aus der Vorfallsbearbeitung können mögliche Verbesserungsmaßnahmen durch Trovent SOC-Analysten erarbeitet werden. Die technische/organisatorische Umsetzung der Verbesserungsmaßnahmen in der Infrastruktur und/oder Geschäftsprozessen des AG obliegt dem AG selbst.
PD.2.3.03	SOLLTE	Insbesondere die Aufarbeitung für die Verbesserung der Threat-Intelligence der Organisation SOLLTE berücksichtigt werden.		Ja		In die Aufarbeitung eines Vorfalls wird mit einbezogen, ob andere/zusätzliche Threat-Intel-Quellen zur früheren/besseren Detektion beigetragen hätten.
PD.2.3.03	SOLLTE	Es SOLLTEN geeignete Evaluierungsprozesse definiert werden, um die Funktionsweisen der Detektoren und Detektionssysteme fortlaufend zu überprüfen.	DER.1.A3 DER.1.A18	Teilweise	X	Die Detektionsregeln/-methoden von Trovent MDR werden fortlaufend in Trovent-Laborumgebungen überprüft. Eine vollständig aussagekräftige Evaluierung setzt jedoch eine Überprüfung in der Produktivumgebung des AG voraus, vorzugsweise im Rahmen eines strukturiert durchgeführten Red-Teamings (Angriffssimulation). Letzteres liegt im Verantwortungsbereich des AG.
PD.2.3.04	**Einsatz von Systemfunktionen zur Detektion**					
PD.2.3.04	MUSS	Der Einsatz von mitgelieferten Systemfunktionen zur Detektion MUSS (z. B. bei Schadcodescannern, Paketfiltern oder Firewalls) umgesetzt werden.	DER.1.A5	Ja	X	Die Konfiguration der Systemfunktionen muss durch den AG erfolgen. Trovent kann hierbei unterstützen. Die aus diesen erzeugten Protokollierungsdaten bzw. SRE können nachgelagert im Trovent MDR-System entgegengenommen und verarbeitet werden.

Nr.	Art	Anforderung	IT-GS Baustein	Erfüllung durch Trovent MDR	Aufgabe des AG	Anmerkungen
PD.2.3.04	MUSS	Insofern ein Sekundär-SRE festgestellt worden ist, MÜSSEN die protokollierten Ereignisse als zusätzliches Hilfsmittel im Rahmen der Auswertung hinzugezogen werden.		Ja		
PD.2.3.05	**Einsatz zusätzlicher Produkte zur Detektion**					
PD.2.3.05		Bei dem Einsatz zusätzlicher Produkte (z. B. Agenten) zur Detektion sind die folgenden Anforderungen bei der Produktauswahl zu berücksichtigen:				„Produkt“ ist in diesem Abschnitt mit **Trovent MDR** gleichzusetzen.
PD.2.3.05	MUSS	Es MUSS sichergestellt sein, dass das Produkt kompatibel zur bestehenden Protokollierungs- und Detektionsinfrastruktur ist.		Ja		Sofern Drittkomponenten im Rahmen der Gesamtlösung von Trovent MDR zum Einsatz kommen, obliegt es Trovent diese auf Kompatibilität und Wirksamkeit zu testen sowie die Integration dieser zu gewährleisten.
PD.2.3.05	MUSS	Das Produkt MUSS vollständig autonom auf einem IT-System agieren und Sekundär-SRE protokollieren und/oder die Protokoll- und Protokollierungsdaten zu einem zentralisierten IT-System versenden (analog zur zentralen Protokollierungsinfrastruktur) und dort SRE detektieren.		Ja		
PD.2.3.05	DARF KEINE	Das Produkt DARF KEINE Verbindung zu externen Netzen außerhalb des Regierungsnetzes, insbesondere dem Internet, benötigen, um Ergebnisse zu SRE zu kommunizieren.		Ja		
PD.2.3.05	DARF NUR	Produktaktualisierungen und der Abgleich von Indikatoren oder Klassifikationen DÜRFEN NUR unidirektional heruntergeladen werden.		Ja		
PD.2.3.05	KANN	Alternativ KÖNNEN diese auf einem vom Produkt unabhängigen Weg heruntergeladen und von der Einrichtung eingespielt werden.		Ja		
PD.2.3.06	**Festlegung der Meldewege und Reaktion**					
PD.2.3.06	MUSS	Es MÜSSEN geeignete Melde- und Alarmierungswege für die sicherheitsrelevanten Ereignisse umgesetzt werden.	DER.1.A3	Ja	X	Die Bewertung von SRE sowie die Erarbeitung angemessener Reaktionsmaßnahmen ist Bestandteil der fortlaufenden Trovent MDR Dienstleistung. Die Melde- und Alarmierungswege auf AG-Seite (außerhalb des Trovent SOC) liegen jedoch im Verantwortungsbereich des AG und müssen von diesem definiert werden. Des weiteren sind diese AG-seitigen Prozesse mit den Trovent SOC-Eskalations/-Alarmierungsprozessen abzustimmen.
PD.2.3.06	MUSS	Dazu MUSS ein geeigneter Prozess zur Reaktion auf begründete Verdachtsfälle geschaffen werden.	DER.1.A17	Ja	X	
PD.2.3.06	MUSS	Dieser MUSS erprobt und regelmäßig geprüft werden, insbesondere die Meldewege zwischen der Detektion und der Reaktion.		Ja	X	

3 Trovent MDR: Erfüllung der Anforderungen des IT-Grundschutz-Bausteins OPS.1.1.5 – Protokollierung

Die nachfolgende Tabelle enthält jede im IT-Grundschutz-Baustein OPS.1.1.5 – Protokollierung erwähnte Anforderung. Für jede Anforderungen führt die Tabelle folgende Informationen:

- eine Klassifikation als MUSS-, SOLLTE- oder KANN-Anforderung
- eine Kennzeichnung, ob die jeweilige Anforderung durch den Einsatz von Trovent MDR erfüllt wird
- eine Kennzeichnung, ob die jeweilige Anforderung auch im Falle des Einsatzes von Trovent MDR im Verantwortungsbereich des Auftraggebers (AG) verbleibt
- ergänzende Anmerkungen zur Umsetzung der Anforderung

Die Nummerierung der Anforderungen ist in unveränderter Form dem Dokument *OPS.1.1.5 – Protokollierung* entnommen.

Nr.	Art	Anforderung	Erfüllung Trovent MDR	Aufgabe des AG	Anmerkungen
OPS.1.1.5.A1	**Erstellung einer Sicherheitsrichtlinie für die Protokollierung**				
OPS.1.1.5.A1	MUSS	Ausgehend von der allgemeinen Sicherheitsrichtlinie der Institution MUSS eine spezifische Sicherheitsrichtlinie für die Protokollierung erstellt werden.	Nein	X	Liegt im Verantwortungsbereich des AG. Trovent kann hierbei inhaltlich unterstützen, insbesondere bei: - der Festlegung, **wie** für das jeweilige Quellsystem zu protokollieren ist - der Definition des Protokollierungsumfangs (und der Einschätzung der sich daraus ergebenden Logdatenvolumina)
OPS.1.1.5.A1	MUSS	In dieser Sicherheitsrichtlinie MÜSSEN nachvollziehbar Anforderungen und Vorgaben beschrieben sein, wie die Protokollierung zu planen, aufzubauen und sicher zu betreiben ist.	Nein	X	
OPS.1.1.5.A1	MUSS	In der spezifischen Sicherheitsrichtlinie MUSS geregelt werden, wie, wo und was zu protokollieren ist.	Nein	X	
OPS.1.1.5.A1	SOLLTE	Dabei SOLLTEN sich Art und Umfang der Protokollierung am Schutzbedarf der Informationen orientieren.	Nein	X	
OPS.1.1.5.A1	MUSS	Die spezifische Sicherheitsrichtlinie MUSS vom ISB gemeinsam mit den Fachverantwortlichen erstellt werden	Nein	X	
OPS.1.1.5.A1	MUSS	Sie MUSS allen für die Protokollierung zuständigen Mitarbeitern bekannt und grundlegend für ihre Arbeit sein.	Nein	X	
OPS.1.1.5.A1	MUSS	Wird die spezifische Sicherheitsrichtlinie verändert oder wird von den Anforderungen abgewichen, MUSS dies mit dem ISB abgestimmt und dokumentiert werden.	Nein	X	
OPS.1.1.5.A1	MUSS	Es MUSS regelmäßig überprüft werden, ob die spezifische Sicherheitsrichtlinie noch korrekt umgesetzt ist.	Nein	X	
OPS.1.1.5.A1	MUSS	Die Ergebnisse der Überprüfung MÜSSEN dokumentiert werden.	Nein	X	
OPS.1.1.5.A3	**Konfiguration der Protokollierung auf System- und Netzebene**				
OPS.1.1.5.A3	MUSS	Alle sicherheitsrelevanten Ereignisse von IT-Systemen und Anwendungen MÜSSEN protokolliert werden.	Ja		
OPS.1.1.5.A3	MUSS	Sofern die in der Protokollierungsrichtlinie als relevant definierten IT-Systeme und Anwendungen über eine Protokollierungsfunktion verfügen, MUSS diese benutzt werden.	Ja		
OPS.1.1.5.A3	MUSS	Wenn die Protokollierung eingerichtet wird, MÜSSEN dabei die Herstellervorgaben für die jeweiligen IT-Systeme oder Anwendungen beachtet werden.	Ja		
OPS.1.1.5.A3	MUSS	In angemessenen Intervallen MUSS stichpunktartig überprüft werden, ob die Protokollierung noch korrekt funktioniert.	Ja		Die Trovent MDR Lösung verfügt über Monitoring-Funktionen, die automatisch alarmieren, wenn Logquellen ausfallen bzw. unzuverlässig Daten liefern.
OPS.1.1.5.A3	MUSS	Die Prüfintervalle MÜSSEN in der Protokollierungsrichtlinie definiert werden.	Ja	X	Die Protokollierungsrichtlinie liegt im Verantwortungsbereich des AG.
OPS.1.1.5.A3	MUSS	Falls betriebs- und sicherheitsrelevante Ereignisse nicht auf einem IT-System protokolliert werden können, MÜSSEN zusätzliche IT-Systeme zur Protokollierung (z. B. von Ereignissen auf Netzebene) integriert werden.	Ja		
OPS.1.1.5.A4	**Zeitsynchronisation der IT-Systeme**				
OPS.1.1.5.A4	MUSS	Die Systemzeit aller protokollierenden IT-Systeme und Anwendungen MUSS immer synchron sein.	Nein	X	NTP Server müssen kundenseitig zur Verfügung gestellt werden
OPS.1.1.5.A4	MUSS	Es MUSS sichergestellt sein, dass das Datums- und Zeitformat der Protokolldateien einheitlich ist	Ja		

Nr.	Art	Anforderung	Erfüllung Trovent MDR	Aufgabe des AG	Anmerkungen
OPS.1.1.5.A5	**Einhaltung rechtlicher Rahmenbedingungen**				
OPS.1.1.5.A5	MUSS	Bei der Protokollierung MÜSSEN die Bestimmungen aus den aktuellen Gesetzen zum Bundes- sowie Landesdatenschutz eingehalten werden (siehe CON.2 Datenschutz).	Ja	X	Trovent MDR bietet die Möglichkeit die in Protokollierungsdaten enthaltenen personenbezogenen Daten entsprechend zu pseudonymisieren. Die Pseudonymisierung kann für die jeweilige Logquelle granular konfiguriert werden. Die granulare Festlegung, welche Datenfelder zu pseudonymisieren sind, muss jedoch durch den AG bzw. seinen Datenschutzbeauftragten und Mitarbeitervertretungen festgelegt werden. Die technische Umsetzung der Pseudonymisierung erfolgt durch Trovent.
OPS.1.1.5.A5	MUSS	Darüber hinaus MÜSSEN eventuelle Persönlichkeitsrechte bzw. Mitbestimmungsrechte der Mitarbeitervertretungen gewahrt werden.	N/A	X	
OPS.1.1.5.A5	MUSS	Ebenso MUSS sichergestellt sein, dass alle weiteren relevanten gesetzlichen Bestimmungen beachtet werden.	Ja	X	
OPS.1.1.5.A5	MUSS	Protokollierungsdaten MÜSSEN nach einem festgelegten Prozess gelöscht werden.	Ja	X	Speicherfristen können quellenspezifisch konfiguriert werden. Die Festlegung der Aufbewahrungs- bzw. Löschfristen liegt im Verantwortungsbereich des AG.
OPS.1.1.5.A5	MUSS	Es MUSS technisch unterbunden werden, dass Protokollierungsdaten unkontrolliert gelöscht oder verändert werden.	Ja		
OPS.1.1.5.A6	**Aufbau einer zentralen Protokollierungsinfrastruktur**				
OPS.1.1.5.A6	SOLLTE	Vor allem in größeren Informationsverbünden SOLLTEN alle gesammelten sicherheitsrelevanten Protokollierungsdaten an einer zentralen Stelle gespeichert werden.	Ja		
OPS.1.1.5.A6	SOLLTE	Dafür SOLLTE eine zentrale Protokollierungsinfrastruktur im Sinne eines Logserver-Verbunds aufgebaut und in einem hierfür eingerichteten Netzsegment platziert werden (siehe NET.1.1 Netzarchitektur und -design).	Ja		
OPS.1.1.5.A6	SOLLTE	Zusätzlich zu sicherheitsrelevanten Ereignissen (siehe OPS.1.1.5.A3 Konfiguration der Protokollierung auf System- und Netzebene) SOLLTE eine zentrale Protokollierungsinfrastruktur auch allgemeine Betriebsereignisse protokollieren, die auf einen Fehler hindeuten.	Ja		
OPS.1.1.5.A6	SOLLTE	Die Protokollierungsinfrastruktur SOLLTE ausreichend dimensioniert sein.	Ja		
OPS.1.1.5.A6	SOLLTE	Die Möglichkeit einer Skalierung im Sinne einer erweiterten Protokollierung SOLLTE berücksichtigt werden.	Ja		Trovent MDR ermöglicht horizontale Skalierung.
OPS.1.1.5.A6	SOLLTE	Dafür SOLLTEN genügend technische, finanzielle und personelle Ressourcen verfügbar sein.	Ja		Wird durch Beauftragung des Trovent MDR-Dienstleistung sichergestellt.
OPS.1.1.5.A8	**Archivierung von Protokollierungsdaten**				
OPS.1.1.5.A8	SOLLTE	Protokollierungsdaten SOLLTEN archiviert werden.	Ja		Siehe OPS.1.1.5.A5

Nr.	Art	Anforderung	Erfüllung Trovent MDR	Aufgabe des AG	Anmerkungen
OPS.1.1.5.A8	SOLLTE	Dabei SOLLTEN die gesetzlich vorgeschriebenen Regelungen berücksichtigt werden.	Ja		Speicherfristen können quellenspezifisch konfiguriert werden. Die Festlegung der Aufbewahrungs- bzw. Löschfristen liegt im Verantwortungsbereich des AG.
OPS.1.1.5.A9	**Bereitstellung von Protokollierungsdaten für die Auswertung**				
OPS.1.1.5.A9	SOLLTE	Die gesammelten Protokollierungsdaten SOLLTEN gefiltert, normalisiert, aggregiert und korreliert werden.	Ja		
OPS.1.1.5.A9	SOLLTE	Die so bearbeiteten Protokollierungsdaten SOLLTEN geeignet verfügbar gemacht werden, damit sie ausgewertet werden können.	Ja		
OPS.1.1.5.A9	SOLLTE	Damit sich die Daten automatisiert auswerten lassen, SOLLTEN die Protokollanwendungen über entsprechende Schnittstellen für die Auswertungsprogramme verfügen.	Ja		Mittels Trovent MDR gesammelte Protokolldaten werden durch dieses auch einer automatischen Auswertung unterzogen. Sowohl die Datensammlung als auch Datenauswertung findet auf dem gleichen System statt.
OPS.1.1.5.A9	SOLLTE	Es SOLLTE sichergestellt sein, dass bei der Auswertung von Protokollierungsdaten die Sicherheitsanforderungen eingehalten werden, die in der Protokollierungsrichtlinie definiert sind.	Ja		
OPS.1.1.5.A9	SOLLTE	Auch wenn die Daten bereitgestellt werden, SOLLTEN betriebliche und interne Vereinbarungen berücksichtigt werden.	Ja		Siehe Anmerkungen zu **OPS.1.1.5.A5**: Es besteht die Notwendigkeit der engen Abstimmung mit Mitarbeitervertretungen.
OPS.1.1.5.A9	SOLLTE	Die Protokollierungsdaten SOLLTEN zusätzlich in unveränderter Originalform aufbewahrt werden	Ja		
OPS.1.1.5.A10	**Zugriffsschutz für Protokollierungsdaten**				
OPS.1.1.5.A10	SOLLTE	Es SOLLTE sichergestellt sein, dass die ausführenden Administratoren selbst keine Berechtigung haben, die aufgezeichneten Protokollierungsdaten zu verändern oder zu löschen.	Ja	X	

4 Trovent MDR: Erfüllung der Anforderungen des IT-Grundschutz-Bausteins DER.1 – Detektion von sicherheitsrelevanten Ereignissen

Die nachfolgende Tabelle enthält jede im IT-Grundschutz-Baustein DER.1 – Detektion erwähnte Anforderung. Für jede Anforderungen führt die Tabelle folgende Informationen:

- eine Klassifikation als MUSS-, SOLLTE- oder KANN-Anforderung
- eine Kennzeichnung, ob die jeweilige Anforderung durch den Einsatz von Trovent MDR erfüllt wird
- eine Kennzeichnung, ob die jeweilige Anforderung auch im Falle des Einsatzes von Trovent MDR im Verantwortungsbereich des Auftraggebers (AG) verbleibt
- ergänzende Anmerkungen zur Umsetzung der Anforderung

Die Nummerierung der Anforderungen ist in unveränderter Form dem Dokument *DER.1 – Detektion* entnommen.

Nr.	Art	Anforderung	Erfüllung Trovent MDR	Aufgabe des AG	Anmerkungen
	BASIS-ANFORDERUNGEN				
DER.1.A1 Erstellung einer Sicherheitsrichtlinie für die Detektion von sicherheitsrelevanten Ereignissen					
DER.1.A1	MUSS	Ausgehend von der allgemeinen Sicherheitsrichtlinie der Institution MUSS eine spezifische Sicherheitsrichtlinie für die Detektion von sicherheitsrelevanten Ereignissen erstellt werden.	Nein	X	
DER.1.A1	MUSS	In der spezifischen Sicherheitsrichtlinie MÜSSEN nachvollziehbar Anforderungen und Vorgaben beschrieben werden, wie die Detektion von sicherheitsrelevanten Ereignissen geplant, aufgebaut und sicher betrieben werden kann.	Nein	X	Trovent kann hierbei unterstützen.
DER.1.A1	MUSS	Die spezifische Sicherheitsrichtlinie MUSS allen im Bereich Detektion zuständigen Mitarbeitern bekannt und grundlegend für ihre Arbeit sein.	Nein	X	Die Sicherheitsrichtlinie muss dem Trovent-SOC zur Verfügung gestellt werden, so dass spezifische Anforderungen aus der Richtlinie (sofern zutreffend) in SOC-Prozessen mit berücksichtigt werden können.
DER.1.A1	MUSS	Falls die spezifische Sicherheitsrichtlinie verändert wird oder von den Anforderungen abgewichen wird, dann MUSS dies mit dem verantwortlichen ISB abgestimmt und dokumentiert werden.	Nein	X	
DER.1.A1	MUSS	Es MUSS regelmäßig überprüft werden, ob die spezifische Sicherheitsrichtlinie noch korrekt umgesetzt ist.	Nein	X	
DER.1.A1	MUSS	Die Ergebnisse der Überprüfung MÜSSEN sinnvoll dokumentiert werden.	Nein	X	
DER.1.A2 Einhaltung rechtlicher Bedingungen bei der Auswertung von Protokollierungsdaten (B)					
DER.1.A2	MUSS	Wenn Protokollierungsdaten ausgewertet werden, dann MÜSSEN dabei die Bestimmungen aus den aktuellen Gesetzen zum Bundes- und Landesdatenschutz eingehalten werden.	Ja	X	Trovent MDR bietet die Möglichkeit die in Protokollierungsdaten enthaltenen personenbezogenen Daten entsprechend zu pseudonymisieren. Die Pseudonymisierung kann für die jeweilige Logquelle granular konfiguriert werden. Die granulare Festlegung, welche Datenfelder zu pseudonymisieren sind, muss jedoch durch den AG bzw. seinen Datenschutzbeauftragten und Mitarbeitervertretungen festgelegt werden. Die technische Umsetzung der Pseudonymisierung erfolgt durch Trovent.
DER.1.A2	MUSS	Wenn Detektionssysteme eingesetzt werden, dann MÜSSEN die Persönlichkeitsrechte bzw. Mitbestimmungsrechte der Mitarbeitervertretungen gewahrt werden.	Ja	X	
DER.1.A2	MUSS	Ebenso MUSS sichergestellt sein, dass alle weiteren relevanten gesetzlichen Bestimmungen beachtet werden, z. B. das Telemediengesetz (TMG), das Betriebsverfassungsgesetz und das Telekommunikationsgesetz	Ja	X	
DER.1.A3 Festlegung von Meldewegen für sicherheitsrelevante Ereignisse (B)					
DER.1.A3	MUSS	Für sicherheitsrelevante Ereignisse MÜSSEN geeignete Melde- und Alarmierungswege festgelegt und dokumentiert werden.	Ja	X	Die Melde- und Eskalationswege zwischen Trovent und AG müssen klar definiert sein. Diese werden im Vorfeld festgelegt – vor Beginn der Dienstleistungserbringung von Trovent MDR.
DER.1.A3	MUSS	Es MUSS bestimmt werden, welche Stellen wann zu informieren sind.	Ja	X	Ansprechpartner / Systemverantwortliche auf AG-Seite müssen definiert sein.
DER.1.A3	MUSS	Es MUSS aufgeführt sein, wie die jeweiligen Personen erreicht werden können.	Ja	X	Kontaktdaten sind vom AG zur Verfügung zu stellen.

Nr.	Art	Anforderung	Erfüllung Trovent MDR	Aufgabe des AG	Anmerkungen
DER.1.A3	MUSS	Je nach Dringlichkeit MUSS ein sicherheitsrelevantes Ereignis über verschiedene Kommunikationswege gemeldet werden.	Ja	X	Für den Fall der Eskalation/Alarmierung außerhalb der Kern-/Bürozeiten muss AG-seitig eine 24x7 Bereitschaft eingerichtet sein.
DER.1.A3	MUSS	Alle Personen, die für die Meldung bzw. Alarmierung relevant sind, MÜSSEN über ihre Aufgaben informiert sein.	Ja	X	Innerhalb des Trovent SOC sind Prozesse und Rollen im Alarmierungsfall klar definiert. Die damit in Verbindung stehenden AG-seitigen Alarmierungswege und Verantwortlichkeiten müssen AG-seitig eindeutig dokumentiert sein.
DER.1.A3	MUSS	Alle Schritte des Melde- und Alarmierungsprozesses MÜSSEN ausführlich beschrieben sein.	Ja	X	
DER.1.A3	SOLLTE	Die eingerichteten Melde- und Alarmierungswege SOLLTEN regelmäßig geprüft, erprobt und aktualisiert werden, falls erforderlich.	Ja	X	Gemeinsam durch AG und Trovent.
DER.1.A4 Sensibilisierung der Mitarbeiter [Vorgesetzte, Benutzer, Mitarbeiter] (B)					
DER.1.A4	MUSS	Jeder Benutzer MUSS dahingehend sensibilisiert werden, dass er Ereignismeldungen seines Clients nicht einfach ignoriert oder schließt.	Nein	X	
DER.1.A4	MUSS	Jeder Benutzer MUSS die Meldungen entsprechend der Alarmierungswege an das verantwortliche Incident Management weitergeben (siehe DER.2.1 Behandlung von Sicherheitsvorfällen).	Nein	X	
DER.1.A4	MUSS	Jeder Mitarbeiter MUSS einen von ihm erkannten Sicherheitsvorfall unverzüglich dem Incident Management melden.	Nein	X	
DER.1.A5 Einsatz von mitgelieferten Systemfunktionen zur Detektion [Fachverantwortliche] (B)					
DER.1.A5	MUSS	Falls eingesetzte IT-Systeme oder Anwendungen über Funktionen verfügen, mit denen sich sicherheitsrelevante Ereignisse detektieren lassen, dann MÜSSEN diese aktiviert und benutzt werden.	Ja	X	Die Konfiguration der Systemfunktionen muss durch den AG erfolgen. Trovent kann hierbei unterstützen. Die aus diesen erzeugten Protokollierungsdaten bzw. SRE können nachgelagert im Trovent MDR-System entgegengenommen und verarbeitet werden.
DER.1.A5	MUSS	Falls ein sicherheitsrelevanter Vorfall vorliegt, dann MÜSSEN die Meldungen der betroffenen IT- Systeme ausgewertet werden.	Ja		
DER.1.A5	MUSS	Zusätzlich MÜSSEN die protokollierten Ereignisse anderer IT-Systeme überprüft werden.	Ja		
DER.1.A5	MUSS	Auch SOLLTEN die gesammelten Meldungen in verbindlich festgelegten Zeiträumen stichpunktartig kontrolliert werden.	Ja		
DER.1.A5	MUSS	Es MUSS geprüft werden, ob zusätzliche Schadcodescanner auf zentralen IT-Systemen installiert werden sollen.	Nein	X	
DER.1.A5	MUSS	Falls zusätzliche Schadcodescanner eingesetzt werden, dann MÜSSEN diese es über einen zentralen Zugriff ermöglichen, ihre Meldungen und Protokolle auszuwerten.	Ja	X	Die aus diesen erzeugten Protokollierungsdaten bzw. SRE können nachgelagert im Trovent MDR-System entgegengenommen und verarbeitet werden.
DER.1.A5	MUSS	Es MUSS sichergestellt sein, dass die Schadcodescanner sicherheitsrelevante Ereignisse automatisch an die Zuständigen melden.	Ja	X	Die Konfiguration der Systemfunktionen muss durch den AG erfolgen. Trovent kann hierbei unterstützen.
DER.1.A5	MUSS	Die Zuständigen MÜSSEN die Meldungen auswerten und untersuchen.	Ja		

Nr.	Art	Anforderung	Erfüllung Trovent MDR	Aufgabe des AG	Anmerkungen
		STANDARD-ANFORDERUNGEN			
DER.1.A6 Kontinuierliche Überwachung und Auswertung von Protokollierungsdaten (S)					
DER.1.A6	SOLLTE	Alle Protokollierungsdaten SOLLTEN möglichst permanent aktiv überwacht und ausgewertet werden.	Ja		Die Überwachung und Auswertung der Daten ist Bestandteil des Trovent MDR Lösung (Managed Service).
DER.1.A6	SOLLTE	Es SOLLTEN Mitarbeiter benannt werden, die dafür zuständig sind.	Ja		
DER.1.A6	SOLLTE	Falls die zuständigen Mitarbeiter aktiv nach sicherheitsrelevanten Ereignissen suchen müssen, z. B. wenn sie IT-Systeme kontrollieren oder testen, dann SOLLTEN solche Aufgaben in entsprechenden Verfahrensanleitungen dokumentiert sein.	Ja		
DER.1.A6	SOLLTE	Für die Detektion von sicherheitsrelevanten Ereignissen SOLLTEN genügend personelle Ressourcen bereitgestellt werden.	Ja		
DER.1.A7 Schulung von Zuständigen [Vorgesetzte] (S)					
DER.1.A7	SOLLTE	Alle Zuständigen, die Ereignismeldungen kontrollieren, SOLLTEN weiterführende Schulungen und Qualifikationen erhalten.	Ja		Alle Mitarbeiter des Trovent SOC werden entsprechend gezielt geschult, um die protokollierten Daten und sicherheitsrelevanten Ereignisse der überwachten Systeme auswerten/bewerten zu können.
DER.1.A7	SOLLTE	Wenn neue IT-Komponenten beschafft werden, SOLLTE ein Budget für Schulungen eingeplant werden.	Ja		
DER.1.A7	SOLLTE	Bevor die zuständigen Mitarbeiter Schulungen für neue IT- Komponenten bekommen, SOLLTE ein Schulungskonzept erstellt werden.	Ja		
DER.1.A9 Einsatz zusätzlicher Detektionssysteme [Fachverantwortliche] (S)					
DER.1.A9	SOLLTE	Anhand des Netzplans SOLLTE festgelegt werden, welche Netzsegmente durch zusätzliche Detektionssysteme geschützt werden müssen.	Ja	X	Dokumentation der Netzwerkinfrastruktur muss durch den AG zur Verfügung gestellt werden. Auf Basis der Dokumentation kann entschieden werden, welchen Datenquellen und Detektionssysteme in Trovent MDR mit einbezogen werden sollten, um die Effektivität der Detektion insgesamt zu maximieren.
DER.1.A9	SOLLTE	Der Informationsverbund SOLLTE um zusätzliche Detektionssysteme und Sensoren ergänzt werden.	Ja	X	
DER.1.A9	SOLLTE	Schadcodedetektionssysteme SOLLTEN eingesetzt und zentral verwaltet werden.	Nein	X	Die Konfiguration der Systemfunktionen muss durch den AG erfolgen. Trovent kann hierbei unterstützen. Die aus diesen erzeugten Protokollierungsdaten bzw. SRE **können nachgelagert im Trovent MDR-System entgegengenommen und verarbeitet werden**.
DER.1.A9	SOLLTE	Auch die im Netzplan definierten Übergange zwischen internen und externen Netzen SOLLTEN um netzbasierte Intrusion Detection Systeme (NIDS) ergänzt werden.	Nein	X	Trovent MDR selbst setzt kein IDS ein, aber i**st in der Lage die SRE eines IDS entgegenzunehmen und in die Detektion (von komplexen Szenarien) mit einzubeziehen**. Darüber hinaus verwendet Trovent MDR Netzwerk-Flows (Netzwerkmetadaten) um Anomalien (Symptome von möglichen SRE) an Netzübergängen zu detektieren.

Nr.	Art	Anforderung	Erfüllung Trovent MDR	Aufgabe des AG	Anmerkungen
DER.1.A10 Einsatz von TLS-/SSH-Proxies [Fachverantwortliche] (S)					
DER.1.A10	SOLLTE	An den Übergängen zu externen Netzen SOLLTEN TLS-/SSH-Proxies eingesetzt werden, welche die verschlüsselte Verbindung unterbrechen und es so ermöglichen, die übertragenen Daten auf Malware zu prüfen.	Nein	X	Für die Detektionsfunktionen von Trovent MDR sind NetFlow-Daten ausreichend; es erfolgt keine Analyse des Payloads von IP-Datenpaketen.
DER.1.A10	SOLLTE	Alle TLS-/SSH-Proxies SOLLTEN vor unbefugten Zugriffen geschützt werden.	Nein	X	
DER.1.A10	SOLLTE	Auf den TLS-/SSH-Proxies SOLLTEN sicherheitsrelevante Ereignisse automatisch detektiert werden.	Nein	X	Die von den TLS-/SSH-Proxies erzeugten Protokollierungsdaten bzw. SRE können nachgelagert im Trovent MDR-System entgegengenommen und verarbeitet werden.
DER.1.A10	SOLLTE	Es SOLLTE eine organisatorische Regelung erstellt werden, unter welchen datenschutzrechtlichen Voraussetzungen die Logdaten manuell ausgewertet werden dürfen.	Nein	X	
DER.1.A11 Nutzung einer zentralen Protokollierungsinfrastruktur für die Auswertung sicherheitsrelevanter Ereignisse [Fachverantwortliche] (S)					
DER.1.A11	SOLLTE	Die auf einer zentralen Protokollinfrastruktur gespeicherten Ereignismeldungen der IT-Systeme und Anwendungen (siehe OPS.1.1.5 Protokollierung) SOLLTEN mithilfe eines Tools abgerufen werden können.	Ja		Das ist zentraler Bestandteil des Trovent MDR-Systems und der darauf aufbauenden SOC-Dienstleistung.
DER.1.A11	SOLLTE	Mit dem auswählten Tool SOLLTEN die Meldungen ausgewertet werden können.	Ja		
DER.1.A11	SOLLTE	Die gesammelten Ereignismeldungen SOLLTEN regelmäßig auf Auffälligkeiten kontrolliert werden.	Ja		
DER.1.A11	SOLLTE	Die Signaturen der Detektionssysteme SOLLTEN immer aktuell und auf dem gleichen Stand sein, damit sicherheitsrelevante Ereignisse auch nachträglich erkannt werden können.	Ja		
DER.1.A12 Auswertung von Informationen aus externen Quellen [Fachverantwortliche] (S)					
DER.1.A12	SOLLTE	Um neue Erkenntnisse über sicherheitsrelevante Ereignisse für den eigenen Informationsverbund zu gewinnen, SOLLTEN externe Quellen herangezogen werden.	Ja	X	Trovent informiert sich regelmäßig über neue sicherheitsrelevante Ereignisse, Angriffsmethoden und Schwachstellen. Dahingehend werden Detektionsregeln/-methoden von Trovent MDR fortlaufend verbessert. Maßgeblich sind hierbei: - Neuerungen/Erweiterungen des MITRE ATT&CK Frameworks - Sigma Rule Repository - Elastic Detection Rules
DER.1.A12	SOLLTE	Meldungen über unterschiedliche Kanäle SOLLTEN von den Mitarbeitern auch als relevant erkannt und an die richtige Stelle weitergeleitet werden.	Ja	X	
DER.1.A12	SOLLTE	Informationen aus zuverlässigen Quellen SOLLTEN grundsätzlich ausgewertet werden.	Ja	X	
DER.1.A12	SOLLTE	Alle gelieferten Informationen SOLLTEN danach bewertet werden, ob sie relevant für den eigenen Informationsverbund sind.	Ja	X	

Nr.	Art	Anforderung	Erfüllung Trovent MDR	Aufgabe des AG	Anmerkungen
DER.1.A12	SOLLTE	Ist dies der Fall, SOLLTEN die Informationen entsprechend der Sicherheitsvorfallbehandlung eskaliert werden.	Ja	X	- verschiedene Threat Intelligence Quellen Ergebnisse aus bestehenden Schwachstellenscannern des AG können in das automatisch aufgebaute Kontextwissen über die IT-Infrastruktur (Trovent Context Engine) mit einbezogen werden, um so die Risikobewertung einzelner SRE zu präzisieren. Ein bestimmtes Angriffsmuster ist vor allem dann von besonderer Relevanz, wenn die hierfür notwendige Schwachstelle nachweislich im Informationsverbund vorliegt.
DER.1.A13 Regelmäßige Audits der Detektionssysteme (S)					
DER.1.A13	SOLLTE	Die vorhandenen Detektionssysteme und getroffenen Maßnahmen SOLLTEN in regelmäßigen Audits daraufhin überprüft werden, ob sie noch aktuell und wirksam sind.	Ja	X	Die Detektionsregeln/-methoden von Trovent MDR werden fortlaufend in Trovent-Laborumgebungen überprüft. Eine vollständig aussagekräftige Evaluierung setzt jedoch eine Überprüfung in der Produktivumgebung des AG voraus, vorzugsweise im Rahmen eines strukturiert durchgeführten Red-Teamings (Angriffssimulation). Letzteres liegt im Verantwortungsbereich des AG.
DER.1.A13	SOLLTE	Es SOLLTEN die Messgrößen ausgewertet werden, die beispielsweise anfallen, wenn sicherheitsrelevante Ereignisse aufgenommen, gemeldet und eskaliert werden.	Ja	X	
DER.1.A13	SOLLTE	Die Ergebnisse der Audits SOLLTEN nachvollziehbar dokumentiert und mit dem Soll-Zustand abgeglichen werden.	Ja	X	
DER.1.A13	SOLLTE	Abweichungen SOLLTE nachgegangen werden.	Ja	X	
		ANFORDERUNGEN BEI ERHÖHTEM SCHUTZBEDARF			
DER.1.A14 Auswertung der Protokollierungsdaten durch spezialisiertes Personal (H)					
DER.1.A14	SOLLTE	Es SOLLTEN Mitarbeiter speziell damit beauftragt werden, alle Protokollierungsdaten zu überwachen.	Ja		Alle Mitarbeiter des Trovent SOC werden entsprechend gezielt geschult, um die protokollierten Daten und sicherheitsrelevanten Ereignisse der überwachten Systeme auswerten/bewerten zu können.
DER.1.A14	SOLLTE	Die Überwachung der Protokollierungsdaten SOLLTE die überwiegende Aufgabe der beauftragten Mitarbeiter sein.	Ja		
DER.1.A14	SOLLTE	Die beauftragten Mitarbeiter SOLLTEN spezialisierte weiterführende Schulungen und Qualifikationen erhalten.	Ja		
DER.1.A14	SOLLTE	Ein Personenkreis SOLLTE benannt werden, der ausschließlich für das Thema Auswertung von Protokollierungsdaten verantwortlich ist.	Ja		
DER.1.A15 Zentrale Detektion und Echtzeitüberprüfung von Ereignismeldungen (H)					
DER.1.A15	SOLLTE	Zentrale Komponenten SOLLTEN eingesetzt werden, um sicherheitsrelevante Ereignisse zu erkennen und auszuwerten.	Ja		Das ist zentraler Bestandteil des Trovent MDR-Systems und der darauf aufbauenden SOC-Dienstleistung.
DER.1.A15	SOLLTE	Zentrale, automatisierte Analysen mit Softwaremitteln SOLLTEN eingesetzt werden.	Ja		
DER.1.A15	SOLLTE	Mit diesen zentralen, automatisierten Analysen mit Softwaremitteln SOLLTEN alle in der Systemumgebung anfallenden Ereignisse aufgezeichnet und in Bezug zueinander gesetzt werden.	Ja		

Nr.	Art	Anforderung	Erfüllung Trovent MDR	Aufgabe des AG	Anmerkungen
DER.1.A15	SOLLTE	Die sicherheitsrelevanten Vorgänge SOLLTEN sichtbar gemacht werden.	Ja		
DER.1.A15	SOLLTE	Alle eingelieferten Daten SOLLTEN lückenlos in der Protokollverwaltung einsehbar und auswertbar sein.	Ja		
DER.1.A15	SOLLTE	Die Daten SOLLTEN möglichst permanent ausgewertet werden.	Ja		
DER.1.A15	SOLLTE	Werden definierte Schwellwerte überschritten, SOLLTE automatisch alarmiert werden.	Ja		
DER.1.A15	SOLLTE	Das Personal SOLLTE sicherstellen, dass bei einem Alarm unverzüglich eine qualifizierte und dem Bedarf entsprechende Reaktion eingeleitet wird.	Ja		
DER.1.A15	SOLLTE	In diesem Zusammenhang SOLLTE auch der betroffene Mitarbeiter sofort informiert werden.	Ja		
DER.1.A15	SOLLTE	Die Systemverantwortlichen SOLLTEN regelmäßig die Analyseparameter auditieren und anpassen, falls dies erforderlich ist.	Ja		
DER.1.A15	SOLLTE	Zusätzlich SOLLTEN bereits überprüfte Daten regelmäßig hinsichtlich sicherheitsrelevanter Ereignisse automatisch untersucht werden.	Ja		
DER.1.A16 Einsatz von Detektionssystemen nach Schutzbedarfsanforderungen (H)					
DER.1.A16	SOLLTE	Anwendungen mit erhöhtem Schutzbedarf SOLLTEN durch zusätzliche Detektionsmaßnahmen geschützt werden.	Ja	X	Der AG kann diese zusätzlichen Systeme gemäß des Schutzbedarfs bestimmen. Trovent kann hier bei Bedarf fachlich unterstützen. Die aus diesen zusätzlichen Detektionssystemen erzeugten Protokollierungsdaten bzw. SRE können nachgelagert im Trovent MDR-System entgegengenommen und verarbeitet werden. Die Bearbeitung der SRE fließt in nachgelagerte Detektionsszenarien und die SOC-Prozesse von Trovent MDR mit ein.
DER.1.A16	SOLLTE	Dafür SOLLTEN z. B. solche Detektionssysteme eingesetzt werden, mit denen sich der erhöhte Schutzbedarf technisch auch sicherstellen lässt.	Ja	X	
DER.1.A17 Automatische Reaktion auf sicherheitsrelevante Ereignisse (H)					
DER.1.A17	SOLLTE	Bei einem sicherheitsrelevanten Ereignis SOLLTEN die eingesetzten Detektionssysteme das Ereignis automatisch melden und mit geeigneten Schutzmaßnahmen reagieren.	Ja		
DER.1.A17	SOLLTE	Hierbei SOLLTEN Verfahren eingesetzt werden, die automatisch mögliche Angriffe, Missbrauchsversuche oder Sicherheitsverletzungen erkennen.	Ja		
DER.1.A17	SOLLTE	Es SOLLTE möglich sein, automatisch in den Datenstrom einzugreifen, um einen möglichen Sicherheitsvorfall zu unterbinden.	Ja		Das MDR System kann bei Bedarf über automatisierte Aktionen mittels Verwendung externer Komponenten Netzwerkverbindungen automatisch blockieren (z.B. durch autom. Umsetzung entsprechender Firewall-Regeln oder NAC-Konfigurationen)
DER.1.A18 Durchführung regelmäßiger Integritätskontrollen (H)					
DER.1.A18	SOLLTE	Alle Detektionssysteme SOLLTEN regelmäßig daraufhin überprüft werden, ob sie noch integer sind.	Ja		
DER.1.A18	SOLLTE	Auch SOLLTEN die Benutzerrechte kontrolliert werden.	Ja		

Nr.	Art	Anforderung	Erfüllung Trovent MDR	Aufgabe des AG	Anmerkungen
DER.1.A18	SOLLTE	Zusätzlich SOLLTEN die Sensoren eine Integritätskontrolle von Dateien durchführen.	Nein		Trovent MDR verwendet keine abgesetzten Sensoren, sondern sammelt nur Logdaten bzw. Ereignisse von Quellsystemen. Das Trovent MDR-System an sich besteht aus mehreren Docker Images, die mit Hashes versehen sind. Eine Veränderung dieser Hash-Werte würde entsprechend detektiert werden.
DER.1.A18	SOLLTE	Bei sich ändernden Werten SOLLTE eine automatische Alarmierung ausgelöst werden.	Ja		