Kategorie	MUSS KANN SOLL	Anforderung Orientierungshilfe (wörtlich)	Unterstützung durch Trend Micro möglich?	Lösung aus der Trend Micro Referenzarchitektur	Erläuterung der Funktion	Anmerkung
Allgemein	MUSS	die notwendigen technischen, organisatorischen und personellen Rahmenbedingungen geschaffen werden MÜSSEN	✔	Alle technischen und organisatorischen Lösungen		
	MUSS	Informationen zu aktuellen Angriffsmustern für technische Vulnerabilitäten fortlaufend für die im Anwendungsbereich eingesetzten Systeme eingeholt werden MÜSSEN	✔	Vision One	Für angebundene Systeme werden regelmäßig Schwachstellenprüfungen durchgeführt.	
	MUSS	durchgängig alle zur effektiven Angriffserkennung erforderliche Hard- und Software auf einem aktuellen Stand gehalten werden MUSS	✔	Service One	Die Unterstützung bei der Durchführung von Produkt Updates und Upgrades ist Bestandteil dieses Service	
	MUSS	die Signaturen von Detektionssystemen immer aktuell sein MÜSSEN	✔	Alle technischen Lösungen	Signaturupdates erfolgen per Standard automatisch	
	MUSS	alle relevanten Systeme so konfiguriert sein MÜSSEN, dass Versuche, bekannte Schwachstellen auszunutzen, erkannt werden können, sofern keine schwerwiegenden Gründe dagegensprechen	✔	Cloud One: Endpoint & Workload Security	Mit hostbasiertem IPS werden Angriffe auf Schwachstellen identifiziert und blockiert.	
				TippingPoint	Angriffe auf Schwachstellen werden auf Netzwerkebene identifiziert und blockiert.	
Protokollierung	SOLL	In der Planungsphase SOLLTE, basierend auf den Ergebnissen der Risikoanalyse und in Anbetracht der kritischen Prozesse des Betreibers, eine schrittweise Vorgehensweise für die Umsetzung der Protokollierung geplant werden.	✔	Professional Services	Die Projektumsetzung gemäß Projektablaufplan ist Bestandteil dieses Services	Die Risikoanalyse und Definition / Beschreibung kritischer Prozesse ist Voraussetzung für die Implementierung und muss im Vorfeld durch die Organisation oder externe Dienstleister durchgeführt werden.
	MUSS	Die Schritte MÜSSEN dabei so gewählt werden, dass eine angemessene Sichtbarkeit innerhalb angemessener Zeit erzielt wird.	✔	Professional Services	Die Projektumsetzung gemäß Projektablaufplan ist Bestandteil dieses Services	Die Definition des Umfanges sowie der Zeitspanne liegt in der Verantwortung der Organisation.
	MUSS	Der Betreiber MUSS alle zur wirksamen Angriffserkennung auf System- bzw. Netzebene notwendigen Protokoll- und Protokollierungsdaten (siehe Glossar gemäß § 2 Absatz 8 und 8a BSIG) erheben, speichern und für die Auswertung bereitstellen, um sicherheitsrelevante Ereignisse (SRE) erkennen und bewerten zu können.	✔	Alle technischen Lösungen	Telemetrie- und Metadaten werden erhoben und zentral gespeichert, sodass eine Auswertung erfolgen und die Qualifizierung sicherheitsrelevanter Ereignisse und Vorfälle durchgeführt werden kann.	
	KANN	Hierzu KÖNNEN zusätzliche Systeme eingesetzt werden	✔	Vision One	Vision One stellt einen zentralen Datenspeicher zur Verfügung.	
	MUSS	Die zur Speicherung notwendigen Systeme und deren IT-Sicherheitsvorkehrungen MÜSSEN schon in der Planung bedacht werden	✔	Presales	Im Vorfeld der Einführung des Systems zur Angriffserkennung erfolgt die Bedarfsanalyse und das erforderliche Sizing durch technisches Presales.	
	MUSS	Da die Protokollierung teilweise auch datenschutzrechtlich relevante Datensätze beinhalten kann, MUSS der legale Umgang mit diesen bei der Planung einbezogen werden	✔	Alle technischen und organisatorischen Lösungen	Trend Micro ist 100% DSGVO commited (https://www.trendmicro.com/de_de/about/trust-center.html)	
	MUSS	Im Rahmen der Planung MÜSSEN alle Systeme identifiziert werden, die zur Aufrechterhaltung der kritischen Dienstleistung maßgeblich sind	✔	Deep Discovery Inspector	Nicht geschützte Systeme werden auf Netzwerkebene identifiziert.	Die Einstufung von Systemen im Kontext der Kritikalität liegt in der Verantwortung der Organisation.
				Cloud One: Endpoint & Workload Security	Durch die Anbindung von Active Directory und Cloud Service Provider Accounts können nicht geschützte Systeme identifiziert werden.	

Kategorie	MUSS KANN SOLL	Anforderung Orientierungshilfe (wörtlich)	Unterstützung durch Trend Micro möglich?	Lösung aus der Trend Micro Referenzarchitektur	Erläuterung der Funktion	Anmerkung
Protokollierung	SOLL	Sind die bestehenden Systeme nicht in der Lage, auskömmliche Protokoll- und Protokollierungsdaten bereitzustellen, SOLLTE die Protokollierungsinfrastruktur so angepasst und/oder durch zusätzliche Maßnahmen, Software oder Systeme ergänzt werden, dass Detektion und Reaktion im entsprechend der Risikoanalyse notwendigen Rahmen möglich sind.	✔	Vision One	Mit einem standalone Agent können auch zusätzliche Systeme (auf denen keine Anti-Malware Lösungen installiert werden dürfen) Telemetrie- und Metadaten übermitteln.	
				TxOne Edge IPS / Edge IPS Pro	Intrusion Prevention auf Netzebene, speziell für OT-Netze und -Systeme	
				TippingPoint	Intrusion Prevention auf Netzebene	
				Cloud App Security	Schutzfunktionalitäten und Sensorik für SaaS Anwendungen wie Office 365 und Google Suite	
				Cloud One: Container Security	Schutzfunktionalitäten und Sensorik für Kubernetes Cluster	
				Deep Discovery Inspector	Netzbasiertes Intrusion und Anomaly Detection	
	KANN	Das anfallende Protokoll- und Protokollierungsdatenaufkommen KANN (und wird dringend empfohlen) anhand eines repräsentativen Systems pro Systemgruppe bestimmt werden.	✔	Professional Services	Beratende Funktion zur Planung innerhalb von Trend Micro Lösungen	Die Bestimmung repräsentativer Systeme liegt in der Verantwortung der Organisation.
	MUSS	Die Ergebnisse der Planungsphase MÜSSEN in einer geeigneten Form dokumentiert werden	✔	Professional Services	Bereitstellung erforderlicher Informationen im Kontext eingesetzter Trend Micro Lösungen	Die Dokumentation in geeigneter Form liegt in der Verantwortung der Organisation.
	MUSS	Die Dokumentation MUSS alle Netzbereiche, die Protokoll- und Protokollierungsdatenquellen, deren Beziehungen untereinander und den Datenfluss der Protokoll- und Protokollierungsdaten im Anwendungsbereich umfassen. Hierbei ist ein angemessener Abstraktions- und Detailgrad zu wählen, sodass der effektive Einsatz von SzA bewertet werden kann.	✔	Professional Services	Bereitstellung erforderlicher Informationen im Kontext eingesetzter Trend Micro Lösungen	Die Dokumentation liegt in der Verantwortung der Organisation.
	SOLL	Um dies zu unterstützen, SOLLTE insbesondere eine Gruppierung gleicher Systemgruppen innerhalb der Dokumentation erfolgen. Gleiche bzw. sehr ähnliche Netze (beispielsweise verschiedene Standorte mit gleichem Netzaufbau) können zusammengefasst werden.				Die Erstellung und Art der Dokumentation liegt in der Verantwortung der Organisation.
	MUSS	Darüber hinaus MUSS für jedes System bzw. für jede Systemgruppe dokumentiert werden, welche Ereignisse dieses bzw. diese protokolliert.	✔	Professional Services	Bereitstellung erforderlicher Informationen im Kontext eingesetzter Trend Micro Lösungen	
	MUSS	Es MUSS ein Prozess eingerichtet werden, der sicherstellt, dass die Protokollierung bei Veränderungen im Anwendungsbereich (Changes) entsprechend angepasst wird.	✔	ServiceOne	Der Whiteglove Onboarding Service unterstützt bei der Inbetriebnahme neuer Lösungen. Der Service Manager unterstützt bei der Durchführung von Anpassungen	Die Etablierung des Prozesses liegt in der Verantwortung der Organisation. Trend Micro orientiert sich entsprechend der Vorgaben.
	MUSS	Als Mindestanforderung für die Protokollierung MÜSSEN alle Basisanforderungen von OPS.1.1.5 Protokollierung und die folgenden Anforderungen erfüllt werden	✔	Alle technischen und organisatorischen Lösungen		Die Umsetzung der Protokollierung über Trend Micro Lösungen hinaus reichende Anforderungen liegt in der Verantwortung des Kunden.
	MUSS	Alle gesammelten sicherheitsrelevanten Protokoll- und Protokollierungsdaten MÜSSEN an für den jeweiligen Netzbereich zentralen Stellen gespeichert werden	✔	Vision One	Vision One stellt einen zentralen Datenspeicher zur Verfügung.	

Kategorie	MUSS KANN SOLL	Anforderung Orientierungshilfe (wörtlich)	Unterstützung durch Trend Micro möglich?	Lösung aus der Trend Micro Referenzarchitektur	Erläuterung der Funktion	Anmerkung
Protokollierung	SOLL	Die Zahl an zentralen Stellen zur Speicherung SOLLTE möglichst geringgehalten werden und sich mindestens an funktionalen Einheiten orientieren, sodass der Zugriff auf die gespeicherten Daten einfach erfolgen kann.	✔	Vision One	Vision One stellt einen zentralen Datenspeicher zur Verfügung.	
	MUSS	Die Protokollierungsinfrastruktur MUSS dazu ausreichend dimensioniert sein	✔	Vision One	Die Anzahl / das Volumen eingelieferter Daten spielt keine Rolle, lediglich die Vorhaltezeit kann individuell erweitert werden (Standard: 30 Tage, Erweiterung auf 90/180/365 Tage möglich)	
	MUSS	Dafür MÜSSEN genügend technische, finanzielle und personelle Ressourcen verfügbar sein				Die Bereitstellung von finanziellen und personellen Ressourcen liegt in der Verantwortung der Organisation
	MUSS	Die gesammelten Protokoll- und Protokollierungsdaten MÜSSEN gefiltert, normalisiert, aggregiert und korreliert werden	✔	Vision One	Die Filterung, Normalisierung, Aggregation und Korrelation erfolgt automatisch durch KI, Heuristik, Algorithmen etc.	
	MUSS	Die so bearbeiteten Protokoll- und Protokollierungsdaten MÜSSEN geeignet verfügbar gemacht werden, damit sie ausgewertet werden können	✔	Vision One	Innerhalb von Vision One werden die aufbereiteten Daten zur Verfügung gestellt.	
	KANN	Eine zeitlich befristete Speicherung der unbearbeiteten Protokolldaten KANN den Detektionsprozess zusätzlich unterstützen	✔	Alle technischen Lösungen	Der Zeitraum zur Aufbewahrung von Protokollierungsdaten ist beschränkt	
	SOLL	Für die Erzielung einer angemessenen Sichtbarkeit von Angriffen SOLLTEN die Protokollierungsdatenquellen auf Netzebene von außen (Netzgrenzen) nach innen (Netzbereiche) erschlossen werden	✔	Service One	Die Aus- und Bewertung von Protokollierungsdaten ist Bestandteil des Services	
				Professional Services	Die Inbetriebnahme der Protokollierungsinfrastruktur kann gemäß Projektablaufplan durchgeführt werden.	
	SOLL	Die Systemebene (kritische Anwendungen und Applikationen) SOLLTE ausgehend von den zentralen, kritischen Systemen, wie z. B. Prozessleit- und Automatisierungstechnik und Leitsystemen, erschlossen wer-den	✔	Service One	Die Aus- und Bewertung von Protokollierungsdaten ist Bestandteil des Services	
				Professional Services	Die Inbetriebnahme der Protokollierungsinfrastruktur kann gemäß Projektablaufplan durchgeführt werden.	
	SOLL	Die Priorisierung zur Auswahl der Protokollierungsdatenquellen SOLLTE ausgehend von der Kritikalität der Systeme abgeleitet werden				Die Bewertung der Kritikalität von Assets liegt in der Verantwortung der Organisation
	MUSS	Nach erfolgreicher Umsetzung der Protokollierung MUSS geprüft werden, ob alle geplanten Protokollierungsdatenquellen gemäß der Planung umgesetzt wurden	✔	Professional Services	Der Abgleich zwischen SOLL/IST Anforderungen kann im Zuge der Leistungserbringung erfolgen.	
	MUSS	Sollten branchenspezifisch weitergehende gesetzliche oder regulatorische Anforderungen an die Protokollierung bestehen, so MÜSSEN diese ebenfalls entsprechend umgesetzt werden				Anforderungsabgleiche müssen durch die Organisation erfolgen bzw. die spezifischen Anforderungen müssen bereitgestellt werden, um Lösungsansätze bewerten zu können.

Kategorie	MUSS KANN SOLL	Anforderung Orientierungshilfe (wörtlich)	Unterstützung durch Trend Micro möglich?	Lösung aus der Trend Micro Referenzarchitektur	Erläuterung der Funktion	Anmerkung
Detektion	MUSS	Bei der Auswahl und dem Einsatz von Detektionsmaßnahmen MUSS eine umfassende und effiziente Abdeckung der Bedrohungslandschaft erzielt werden	✔	Alle technischen und organisatorischen Lösungen	Trend Micro ist ein global führender Anbieter von Produkten und Services in der Cybersecurity Branche und erfüllt diese Anforderung.	
	MUSS	Dazu MÜSSEN die Ergebnisse der Risikoanalyse sowie die Größe und Struktur des Unternehmens in der Planung einbezogen werden				Die Risikoanalyse und Betrachtung der Verhältnismäßigkeit liegt in der Verantwortung der Organisation
	KANN	Zur Bestimmung der Abdeckung KANN (und es wird empfohlen) eine standardisierte Methode angewendet werden (z. B. MITRE ATT&CK bzw. ATT&CK for ICS	✔	Vision One	Vision One setzt alle Taktiken, Techniken und Prozeduren von Cyberangriffen in Kontext zu MITRE ATT&CK (sofern dort gelistet)	
	KANN	In Abhängigkeit der Unternehmensgröße und der Bedrohungslandschaft KANN eine separate Betrachtung von Detektionsmaßnahmen für die IT- und OT-Umgebung erforderlich sein.	✔	TxOne Stellar	Anti-Malware, speziell für OT-Netze und -Systeme	
				TxOne Edge IPS / Edge IPS Pro	Intrusion Prevention auf Netzebene, speziell für OT-Netze und -Systeme	
	MUSS	Als Mindestanforderung für die Detektion MÜSSEN alle Basisanforderungen von DER.1 Detektion von sicherheitsrelevanten Ereignissen und die folgenden Anforderungen erfüllt werden	✔	Alle technischen und organisatorischen Lösungen		Anforderungsabgleiche müssen durchdie Organisation erfolgen bzw. die spezifischen Anforderungen müssen bereitgestellt werden, um Lösungsansätze bewerten zu können.
	MUSS	Alle Protokoll- und Protokollierungsdaten MÜSSEN kontinuierlich überwacht und ausgewertet werden.	✔	Vision One	Durch Technologie findet eine automatische Überwachung und Vorqualifizierung eingelieferter Daten statt	
				Service One	Die Überwachung durch Trend Micro SOCs ist Bestandteil des Service	
	KANN	Dies KANN automatisiert werden, wenn bei relevanten Ereignissen eine unmittelbare Alarmierung der Verantwortlichen gewährleistet ist	✔	Vision One	Bei Erkennung von relevanten Ereignissen ist eine automatische Alarmierung konfigurierbar	
	MUSS	Die Prüfung des Ereignisses und ggf. die Reaktion MUSS innerhalb einer der Risikoanalyse entsprechend geringen Zeitspanne erfolgen	✔	Service One	Die Prüfung und ggf. Reaktion auf Ereignisse ist Bestandteil des Service	
	MUSS	Es MÜSSEN Mitarbeitende bzw. Mitarbeitende von Dienstleistern benannt werden, die dafür zuständig sind	✔	Service One	Ansprechpartner, Teams und deren Aufgaben können benannt werden.	Die Definition von kundeninternen Zuständigkeiten liegt in der Verantwortung der Organisation
	MUSS	Müssen die verantwortlichen Mitarbeitenden aktiv nach sicherheitsrelevanten Ereignissen suchen, z. B. wenn sie IT-Systeme kontrollieren oder testen, MÜSSEN solche Aufgaben in entsprechenden Verfahrensanleitungen dokumentiert sein	✔	Service One	Trend Micro stellt entsprechende Dokumente für eigenes Personal zur Verfügung	Die Erstellung kundeninterne Verfahrensanleitungen liegt in der Verantwortung der Organisation
	MUSS	Für die Detektion von sicherheitsrelevanten Ereignissen MÜSSEN genügend personelle Ressourcen bereitgestellt werden.	✔	Service One	Trend Micro stellt ausreichende personelle Ressourcen zur Verfügung.	Die Bereitstellung kundeninterner Ressourcen liegt in der Verantwortung der Organisation
	MUSS	Es MÜSSEN Schadcodedetektionssysteme eingesetzt und zentral verwaltet werden	✔	Cloud One: Endpoint & Workload Security	Diverse state of the Art Technologien zur Erkennung von Schadcode auf Windows/Linux/macOS basierten Clients und Servern	
				Deep Discovery Inspector	Erkennung von Schadcode auf Netzebene	
				TxOne Stellar	Anti-Malware, speziell für OT-Netze und -Systeme	

Kategorie	MUSS KANN SOLL	Anforderung Orientierungshilfe (wörtlich)	Unterstützung durch Trend Micro möglich?	Lösung aus der Trend Micro Referenzarchitektur	Erläuterung der Funktion	Anmerkung
Detektion	MUSS	Anhand des Netzplans MUSS festgelegt werden, welche Netzsegmente durch zusätzliche Detektionssysteme geschützt werden müssen				Die Definition zusätzlich zu schützender Netzbereiche liegt in der Verantwortung der Orgnanisation
	MUSS	Insbesondere MÜSSEN die im Netzplan definierten Übergänge zwischen internen und externen Netzen um netzbasierte Intrusion Detection Systeme (NIDS) ergänzt werden	✔	Deep Discovery Inspector	Erkennung von Schadcode, Ausnutzung von Schwachstellen und zielgerichteten Angriffen auf Netzebene	
	SOLL	Damit die Protokoll- und Protokollierungsdaten korreliert und abgeglichen werden können, SOLLTEN sie alle zeitlich synchronisiert werden	✔	Vision One	Die zeitliche Synchronisierung erfolgt innerhalb von Vision One	
	MUSS	Die gesammelten Ereignismeldungen MÜSSEN regelmäßig auf Auffälligkeiten kontrolliert werden	✔	Service One	Die Kontrolle durch Trend Micro SOCs ist Bestandteil des Service	
	MUSS	Damit sicherheitsrelevante Ereignisse auch nachträglich erkannt werden können, MÜSSEN die Signaturen der Detektionssysteme immer auf aktuellstem Stand gehalten werden.	✔	Alle technischen Lösungen	Signaturupdates erfolgen per Standard automatisch	
	MUSS	Um neue Erkenntnisse über sicherheitsrelevante Ereignisse für den eigenen Informationsverbund zu gewinnen, MÜSSEN externe Quellen herangezogen werden	✔	Vision One	Ergebnisse von Trend Micro Threat Research (Bedrohungsforschung) fließen kontinuierlich in Vision One ein. Drittanbieterquellen können per TAXII angebunden werden. Attack Surface Management stellt Risiken für die Infrastruktur der Organisation übersichtlich dar.	
	MUSS	Da Meldungen über unterschiedliche Kanäle in eine Institution gelangen, MUSS sichergestellt sein, dass diese Meldungen von den Mitarbeitenden auch als relevant erkannt und an die richtige Stelle weitergeleitet werden	✔	Vision One	Informationen werden nach Quelle differenziert und sind somit als solche erkennbar und können innerhalb der Organisation weitergegeben werden.	Organisationsinterne Abläufe müssen durch die Organisation entwickelt und umgesetzt werden.
	MUSS	Informationen aus zuverlässigen Quellen MÜSSEN grundsätzlich ausgewertet werden	✔	Vision One	Eine generalisierte, automatische Auswertung findet im Vorfeld statt.	
				Service One	Bedrohungsinformationen aus externen Quellen werden im Zuge von Analysen durch Trend Micro SOCs berücksichtigt.	
	MUSS	Alle gelieferten Informationen MÜSSEN danach bewertet werden, ob sie relevant für den eigenen Informationsverbund sind	✔	Vision One	Attack Surface Management stellt Risiken für die Infrastruktur der Organisation übersichtlich dar.	
	MUSS	Ist dies der Fall, MÜSSEN die Informationen entsprechend der Sicherheitsvorfallbehandlung eskaliert werden.				Die Meldung und Eskalation von Risiken liegt in der Verantwortung der Organisation
	MUSS	Es MÜSSEN Mitarbeitende bzw. Mitarbeitende von Dienstleistern speziell damit beauftragt werden, alle Protokoll- und Protokollierungsdaten auszuwerten.	✔	Service One	Die Auswertung durch Trend Micro SOCs ist Bestandteil des Service	
	SOLL	Die Auswertung der Protokoll- und Protokollierungsdaten SOLLTE bei diesen höher priorisiert sein, als ihre übrigen Aufgaben. Daher empfiehlt es sich, dass dies ihre überwiegende Aufgabe ist	✔	Service One	Trend Micro stellt personellen Ressourcen in den Bereichen Incident Response und managed XDR ausschließlich zur Erfüllung dieser Aufgaben bereit.	

Kategorie	MUSS / KANN / SOLL	Anforderung Orientierungshilfe (wörtlich)	Unterstützung durch Trend Micro möglich?	Lösung aus der Trend Micro Referenzarchitektur	Erläuterung der Funktion	Anmerkung
Detektion	SOLL	Dieses Personal SOLLTE spezialisierte weiterführende Schulungen und Qualifikationen erhalten.	✔	Service One	Die von Trend Micro bereitgestellten Ressourcen sind für die Bereiche Incident Response und managed XDR geschult, entsprechend qualifiziert und erfahren.	
				Training	Trend Micro bietet Trainings an.	
	MUSS	Ein Personenkreis MUSS benannt werden, der für das Thema Auswertung von Protokoll- und Protokollierungsdaten verantwortlich ist.	✔	Service One	Ansprechpartner, Teams und deren Aufgaben können benannt werden.	Die Definition von kundeninternen Zuständigkeiten obliegt dem Kunden
	MUSS	Es MÜSSEN zentrale Komponenten eingesetzt werden, um sicherheitsrelevante Ereignisse zu erkennen und auszuwerten	✔	Vision One	Vision One ist die zentrale Infrastruktur zur Speicherung und Auswertung relevanter Daten.	
	MUSS	Zentrale automatisierte Analysen mit Softwaremitteln MÜSSEN dazu eingesetzt werden, um alle in der Systemumgebung anfallenden Protokoll- und Protokollierungsdaten aufzuzeichnen, in Bezug zueinander zu setzen und sicherheitsrelevante Vorgänge sichtbar zu machen	✔	Vision One	Die Korrelation von Ereignissen über Trend Micro Sensorik sowie automatische Bewertung und Vorqualifizierung ist Bestandteil der Lösung	
	MUSS	Alle eingelieferten Protokoll- und Protokollierungsdaten MÜSSEN lückenlos in der Protokollverwaltung einsehbar und auswertbar sein.	✔	Alle technischen Lösungen	Die Datenqualität innerhalb von Trend Micro Lösungen entspricht dieser Anforderung.	
	MUSS	Die Daten MÜSSEN kontinuierlich ausgewertet werden.	✔	Vision One	Durch Technologie findet eine grundlegende automatische Auswertung eingelieferter Daten statt.	
				Service One	Die Auswertung der Daten durch Trend Micro Experten ist Bestandteil des Services.	
	MUSS	Werden definierte Schwellenwerte überschritten, MUSS automatisch alarmiert werden	✔	Vision One	Die automatische Alarmierung bei neuen sicherheitsrelevanten Ereignissen und Vorfällen kann aktiviert werden.	
				Service One	Die Benachrichtigung bei relevanten Ereignissen ist Bestandteil des Services.	
	MUSS	Das zuständige Personal MUSS sicherstellen, dass bei einem Alarm nach fachlicher Bewertung und innerhalb einer der Risikoanalyse entsprechend geringen Zeitspanne eine qualifizierte und dem Bedarf entsprechende Reaktion eingeleitet wird	✔	Service One	Die Bewertung und ggf. Reaktion auf Ereignisse ist Bestandteil des Service	
	MUSS	Die Systemverantwortlichen MÜSSEN regelmäßig die Analyseparameter auditieren und anpassen, falls dies erforderlich ist	✔	Service One	Der zugewiesene Service Manager kann Systemverantwortliche bei der Umsetzung unterstützen und beraten.	
	MUSS	Zusätzlich MÜSSEN bereits überprüfte Protokoll- und Protokollierungsdaten regelmäßig hinsichtlich sicherheitsrelevanter Ereignisse automatisch untersucht werden	✔	Vision One	Eine historische Untersuchung kann auf Basis verschiedener Parameter ausgeführt werden.	
				Service One	Trend Micro SOCs prüfen bei der Analyse auch den historischen Kontext	

Kategorie	MUSS KANN SOLL	Anforderung Orientierungshilfe (wörtlich)	Unterstützung durch Trend Micro möglich?	Lösung aus der Trend Micro Referenzarchitektur	Erläuterung der Funktion	Anmerkung
Detektion	MUSS	Als eine zentrale Grundvoraussetzung für die effektive Detektion MÜSSEN zudem Informationen zu aktuellen Angriffsmustern für technische Vulnerabilitäten fortlaufend für die im Anwendungsbereich eingesetzten Systeme eingeholt werden	✔	Vision One	Ergebnisse von Trend Micro Threat Research (Bedrohungsforschung) fließen kontinuierlich in Vision One ein. Drittanbieterquellen können per TAXII an Vision One angebunden werden. Attack Surface Management stellt Risiken für die Infrastruktur der Organisation übersichtlich dar. Ergebnisse der Zero Day Initiative fließen kontinuierlich in Vision One ein.	
	MUSS	Dazu MÜSSEN fortlaufend Meldungen der Hersteller (Hard- und Software), von Behörden, den Medien und weiterer relevanter Stellen geprüft werden und in dokumentierte Prozesse des Schwachstellenmanagements einfließen				Der Abruf und die Bewertung von Meldungen in Bezug auf die spezifische Infrastruktur des Kunden liegt in der Verantwortung der Organisation
	SOLL	Bei der Umsetzung von Detektionsmechanismen SOLLTE initial eine Kalibrierung durchgeführt werden, um festzustellen, welche sicherheitsrelevanten Ereignisse (SRE) im Normalzustand auftreten (Baselining).	✔	Professional Services	Diese Anforderung kann im Zuge des Projektes umgesetzt werden.	
	SOLL	Dazu SOLLTE bewertet werden, ob dieser Normalzustand in Hinblick auf die Zahl der falsch positiven Meldungen hingenommen werden kann oder ob Änderungen vorzunehmen sind.	✔	Professional Services	Diese Anforderung kann im Zuge des Projektes umgesetzt werden.	Die finale Bewertung der Konfiguration liegt in der Verantwortung der Organisation
	SOLL	Die Kalibrierung SOLLTE bei Änderungen innerhalb des Anwendungsbereichs oder der Bedrohungslage erneut durchgeführt werden	✔	Service One	Die Unterstützung bei der Durchführung von Konfigurationsanpassungen ist Bestandteil dieses Service	
				Professional Services	Die Durchführung der Umsetzung kann bei Bedarf übernommen werden.	
	MUSS	Die SRE MÜSSEN überprüft und dahingehend bewertet werden, ob sie auf einen Sicherheitsvorfall (qualifizierter SRE) hindeuten	✔	Vision One	Eine Vorabqualifizierung findet durch die automatische Korrelation von sicherheitsrelevanten Ereignissen statt.	
				Service One	Die Qualifizierung sicherheitsrelevanter Ereignisse und Vorfälle ist Bestandteil des Services.	
	SOLL	Die zur Angriffserkennung eingesetzten Systeme sollten, in eindeutig zuordenbaren Fällen, eine automatisierte Qualifizierung der SRE ermöglichen.	✔	Vision One	Durch die Korrelation von Daten werden sicherheitsrelevante Ereignisse und Vorfälle automatisch qualifiziert und in Kontext zu Cyberangriffen gesetzt	
	SOLL	Nur qualifizierte SRE SOLLTEN den Prozess der Reaktion auslösen	✔	Visione One	Automatische Reaktionen können deaktiviert oder granular konfiguriert werden.	
				Service One	Eine Reaktion erfolgt nur im Rahmen der im Vorfeld des Service Onboarding festgelegten Parameter sowie ausschließlich nach Qualifizierung eines sicherheitsrelevanten Ereignisses oder Vorfalls.	
	SOLL	Die Qualifizierung SOLLTE in automatisiert nicht eindeutig zuordenbaren Fällen manuell durch festgelegte Verantwortliche vorgenommen werden	✔	Service One	Die Qualifizierung sicherheitsrelevanter Ereignisse und Vorfälle ist Bestandteil des Services.	

Kategorie	MUSS KANN SOLL	Anforderung Orientierungshilfe (wörtlich)	Unterstützung durch Trend Micro möglich?	Lösung aus der Trend Micro Referenzarchitektur	Erläuterung der Funktion	Anmerkung
Detektion	MUSS	Basierend auf den gewonnenen Erkenntnissen der Qualifizierung MÜSSEN die Detektionsmechanismen nachjustiert werden	✔	Service One	Die Unterstützung bei der Durchführung von Konfigurationsanpassungen ist Bestandteil dieses Service	
				Professional Services	Die Durchführung der Umsetzung kann bei Bedarf übernommen werden.	
	MUSS	Sollten branchenspezifisch weitergehende gesetzliche oder regulatorische Anforderungen bestehen, so MÜSSEN diese ebenfalls entsprechend umgesetzt werden				Anforderungsabgleiche müssen durch die Organisation erfolgen bzw. die spezifischen Anforderungen müssen bereitgestellt werden, um Lösungsansätze bewerten zu können.
Reaktion	MUSS	Als Mindestanforderung für die Reaktion MÜSSEN alle Basisanforderungen von DER.2.1 Behandlung von Sicherheitsvorfällen erfüllt werden, für alle möglichen Sicherheitsvorfälle, die im Zusammenhang mit Angriffen stehen bzw. stehen könnten	✔	Alle technischen und organisatorischen Lösungen		
	SOLL	Es SOLLTEN zudem die Standardanforderungen aus DER.2.1 Behandlung von Sicherheitsvorfällen umgesetzt werden, für alle möglichen Sicherheitsvorfälle, die im Zusammenhang mit Angriffen stehen bzw. stehen könnten	✔	Alle technischen und organisatorischen Lösungen		
	MUSS	Außerdem MUSS die folgende Anforderung erfüllt werden	✔	Alle technischen und organisatorischen Lösungen		
	MUSS	Bei einem sicherheitsrelevanten Ereignis MÜSSEN die eingesetzten Detektionssysteme das Ereignis automatisch melden und in Netzen, wo durch die automatische Reaktion die kritische Dienstleistung nicht gefährdet wird, mit geeigneten Schutzmaßnahmen reagieren	✔	Alle technischen Lösungen	Die Meldung von sicherheitsrelevanten Ereignissen ist Bestandteil von Vision One. Alle technischen Lösungen können so konfiguriert werden, dass Indikatoren einer Kompromittierung automatisch blockiert (Dateien, Webseiten, IPs, Benutzerkonten, Systeme) werden.	
				Service One	Die Meldung sicherheitsrelevanter Ereignisse und Vorfälle ist Bestandteil dieses Service. Im Rahmen von Parametern, die während des Service Onboarding festgelegt werden, kann auch (sofern technisch umsetzbar) eine Reaktion auf sicherheitsrelevante Ereignisse und Vorfälle erfolgen.	
	MUSS	In Netzen, wo die kritische Dienstleistung durch die Umsetzung nicht gefährdet wird, MUSS es möglich sein, automatisch in den Datenstrom einzugreifen, um einen möglichen Sicherheitsvorfall zu unterbinden	✔	TippingPoint	Schadsoftware und Angriffsversuche werden auf Netzwerkebene blockiert.	
	MUSS	Sollte eine automatische Reaktion nicht möglich sein, MUSS über manuelle Prozesse sichergestellt werden, dass der mögliche Sicherheitsvorfall unterbunden wird	✔	Service One	Im Rahmen von Parametern, die während des Service Onboarding festgelegt werden, kann auch (sofern technisch umsetzbar) eine Reaktion auf sicherheitsrelevante Ereignisse und Vorfälle erfolgen.	
	MUSS	Der Ausschluss von Netzen oder Netzsegmenten von einer automatischen Reaktion, bzw. dem Eingriff in den Datenstrom MUSS schlüssig begründet sein				Die Begründung für einen Ausschluss von Netzen oder Netzsegmenten liegt in der Verantwortung der Organisation

Kategorie	MUSS KANN SOLL	Anforderung Orientierungshilfe (wörtlich)	Unterstützung durch Trend Micro möglich?	Lösung aus der Trend Micro Referenzarchitektur	Erläuterung der Funktion	Anmerkung
Reaktion	MUSS	Festgestellte Sicherheitsvorfälle im vermeintlichen Zusammenhang mit Angriffen MÜSSEN behandelt werden.	✔	Service One	Diese Leistung ist Bestandteil des Service.	
	MUSS	Bei Störungen und Sicherheitsvorfällen insbesondere im vermeintlichen Zusammenhang mit Angriffen MUSS überprüft werden, ob diese den Kriterien der Meldepflicht nach § 8b Absatz 3 BSIG bzw. §11 Absatz 1c EnWG entsprechen und eine Meldung an das BSI notwendig ist				Die Prüfung und ggf. Meldung liegt in der Verantwortung der Organisation
	SOLL	Die zur Angriffserkennung eingesetzten Systeme SOLLTEN automatisiert Maßnahmen zur Vermeidung und Beseitigung von angriffsbedingten Störungen ergreifen können, sofern das zu Grunde liegende SRE eindeutig qualifizierbar ist.	✔	Alle technischen Lösungen	Alle technischen Lösungen können so konfiguriert werden, dass Indikatoren einer Kompromittierung automatisch blockiert (Dateien, Webseiten, IPs, Benutzerkonten, Systeme) werden.	
				Service One	Die Meldung sicherheitsrelevanter Ereignisse und Vorfälle ist Bestandteil dieses Service. Im Rahmen von Parametern, die während des Service Onboarding festgelegt werden, kann auch (sofern technisch umsetzbar) eine Reaktion auf sicherheitsrelevante Ereignisse und Vorfälle erfolgen	
	MUSS	Dabei MUSS gewährleistet sein, dass ausschließlich automatisiert ergriffene Maßnahmen nicht zu einer relevanten Beeinträchtigung der kritischen Dienstleistung des Betreibers führen können.	✔	Service One	Die Unterstützung bei der Durchführung von Konfigurationsanpassungen ist Bestandteil dieses Service	Die Bekanntgabe von Netzen und Systemen für die Erbringung kritischer Dienstleistungen sowie die Mitwirkung bei der Anpassung von Konfigurationsparameter für diese liegt in der Verantwortung der Organisation
				Professional Services	Die Planung zur Umsetzung sowie Durchführung im Rahmen der Projektrealisierung kann erfolgen.	
	SOLL	Die eingesetzten SzA SOLLTEN auch eine nicht-automatisierte Qualifizierung und Behandlung von Ereignissen unterstützen.	✔	Vision One	Manuelle Reaktionen sind im Rahmen technischer Machbarkeit möglich.	
				Service One	Im Rahmen von Parametern, die während des Service Onboarding festgelegt werden, kann auch (sofern technisch umsetzbar) eine Reaktion auf sicherheitsrelevante Ereignisse und Vorfälle erfolgen	