Erfüllen des IT-Sicherheitsgesetz 2.0

DARKTRACE

/ Introduction

Das IT Sicherheitsgesetz hat sich im Jahr 2022 aktualisiert mit dem Ziel die nationale Kritische Infrastruktur (KRITIS) vollumfassend zu schützen. Die Betreiber Kritischer Infrastruktur müssen in der Zukunft Systeme zur Angriffserkennung einsetzten.

Ab dem 1. Mai 2023 sind alle Betreiber kritischer Infrastruktur dazu verpflichtet bestimme Kriterien anhand eines Umsetzungsgradmodells zu erfüllen.

Dieses Whitepaper dient als Unterstützung um aufzuzeigen wie Darktrace die MUSS, SOLL und KANN Anforderungen der BSI Orientierungshilfe eigenhändig oder in Kombination mit Integrationen und Partnern erfüllt.

Die Technologie von Darktrace basiert auf maschinellem Lernen (ML) und künstlicher Intelligenz (KI) und somit können die Produkte von Darktrace komplexe Netzwerke analysieren und Indikationen von Bedrohungen frühzeitig entdecken. Dies wird durch einen Abgleich vom Verhalten des Geräts oder Benutzers mit einem fundamentalen Verhaltensmuster („Pattern of life") erzielt. Durch kontinuierliches Lernen eines Grundverhaltens gleicht die KI in Echtzeit jede erneute Verbindung des Gerätes oder Benutzers ab. Die Erkennung von Anomalien in diesem Verhalten erlaubt Darktrace Bedrohungen aller Art, von fortgeschrittener Malware zu internen Bedrohungen oder Zero-Days, im initialen Stadion zu identifizieren.

Die Darktrace Software nutzt ML-Algorithmen um ein Verständnis davon aufzubauen was normal ist im Netzwerk und was vom normalen Verhaltensmuster abweicht. Dieser Ansatz entwickelt sich ständig weiter, lernt jede Sekunde dazu und passt die Resultate und Reaktionen auf komplexe und dynamische Netzwerk-, Cloud-Infrastrukturen und Nutzerverhalten an.

Anbieter kritischer Infrastruktur benötigen sowohl IT als auch OT Netzwerke um ihre Dienste zu liefern. Der traditionelle ‚Air-gap' verschwindet. Die IT und OT Netzwerke werden heutzutage immer enger zusammengelegt, was die OT immer mehr den Bedrohungen aus dem Internet aussetzt.

Darktrace kann in der ganzen digitalen Infrastruktur eingesetzt werden und sowohl IT- als auch OT-Ereignisse in einer Benutzeroberfläche anzeigen. Damit können die Sicherheitsbeauftragten eine einheitliche Lösung mit geteilter Intelligenz, der gleichen Funktionalität und der gleichen Sprache sehr leicht einsetzten. Der Informationsaustauch zwischen den zwei Bereichen macht sehr schnell und leicht ersichtlich, falls sich ein Angriff aus dem einen Bereich in den anderen ausbreitet (meistens von der IT in die OT). Dies ist gravierend in einer modernen Zeit, wo die Informationen aus der OT in die IT einfließen müssen.

IT-Risiken haben sich in den meisten Organisationen in die OT übertragen, wobei die OT nicht gemacht ist für IT-artige Richtlinien wie zum Beispiel regelmäßige Updates. Darktrace/OT unterstützt sowohl bei der Erkennung dieser Risiken als auch bei der Triage. Der Cyber AI Analyst kommt mit der Erfahrung mehrerer hundert menschlichen Analysten und untersucht das Netzwerk nach zusammenhängenden anormalen Verbindungen und das Ganze in Maschinengeschwindigkeit.

In einer einheitlichen Lösung, die leicht zu implementieren und verstehen ist, hilft Darktrace den Anbietern kritischer Infrastruktur der wechselhaften Sicherheitslandschaft gerecht zu werden.

	Anforderung	Darktrace
Protokollierung		
Planung	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. Die Schritte MÜSSEN dabei so gewählt werden, dass eine angemessene Sichtbarkeit innerhalb angemessener Zeit erzielt wird.	Darktrace ist vollkommen skalierbar. Eine einzige Master-Appliance reicht aus, um in einem ersten Schritt mehrere tausend Geräte in einem Netzwerksegment zu überwachen. Sollten weitere Netzwerksegmente und/oder Standorte dazukommen können weitere Probe Appliances mit der bestehenden Master-Appliance verbunden werden. Dabei werden alle Netzwerksegmente als eine Einheit betrachtet und analysiert. Falls eine einzige Master Appliance nicht mehr ausreichen sollte, können mehrere Master Appliances über den sog. "Unified View" zu einem System zusammengefasst werden. Die Installation zusätzlicher Probe-Appliances kann in sehr kurzer Zeit bewerkstelligt werden.
	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.	Darktrace analysiert vollständig den gesamten IP-Netzwerkdatenverkehr und extrahiert mittels DPI alle relevanten Metadaten daraus. Diese werden zur Modellierung und Erkennung von ungewöhnlichen Ereignissen herangezogen. Alle Ereignisse im IP-Netzwerk werden vom System protokolliert und gespeichert. Eine spätere Auswertung beliebiger Ereignisse ist dabei möglich. Sicherheitsrelevante Ereignisse (SRE) werden dabei automatisch erkannt und bewertet (sog. "Model Breaches").
	Hierzu KÖNNEN zusätzliche Systeme eingesetzt werden, sodass zur wirksamen Angriffserkennung nicht jedes einzelne Gerät Protokollierungsdaten aufzeichnen muss und damit die Verfügbarkeit der Produktivsysteme und damit der kritischen Dienstleistung gewährleistet werden kann. Die zur Speicherung notwendigen Systeme und deren IT-Sicherheitsvorkehrungen MÜSSEN schon in der Planung bedacht werden. Da die Protokollierung teilweise auch datenschutzrechtlich relevante Datensätze beinhalten kann, MUSS der legale Umgang mit diesen bei der Planung einbezogen werden. Ggf. ist dazu eine Anonymisierung bzw. Pseudonymisierung der Protokoll- und Protokollierungsdaten erforderlich.	Darktrace hat Sichtbarkeit über den gesamten IP-Netzwerkdatenverkehr und wertet ihn zur Angriffserkennung aus. Eine Kopie des gesamten IP-Netzwerkdatenverkehrs wird dabei von zentralen Netzwerkkomponenten (z.B. Switchen, Firewalls) dem Darktrace System zugeführt. Des Weiteren benötigt Darktrace keinen Zugriff oder Agenten auf den Produktivsystemen, sodass diese nicht belastet werden. Da in dem Datenverkehr auch datenschutzrechtlich relevante Datensätze vorhanden sein können stellt das Darktrace System eine Pseudonymisierungskomponente zur Verfügung die bei Bedarf aktiviert werden kann.
	Im Rahmen der Planung MÜSSEN alle Systeme identifiziert werden, die zur Aufrechterhaltung der kritischen Dienstleistung maßgeblich sind, damit deren Protokoll- und Protokollierungsdaten später erfasst werden können.	Darktrace kann aufgrund des Datenverkehrs im Netzwerk automatisch ein Inventar aller vorhandenen Systeme dieses Netzwerks erstellen und sie klassifizieren. Weiter werden Systeme ihrer Ähnlichkeit gruppiert (Clusterbildung). Diese erleichtert die Identifikation aller kritischen Systeme. Darüber hinaus ist es optional noch möglich die Systeme aktiv zu kontaktieren und zu identifizieren.
	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.	Sollten aus welchen Gründen auch immer in dem IP-Netzwerkdatenverkehr nicht alle für den Betrieb notwendigen Daten vorhanden sein, können diese z.B. über Log-Dateien dem Darktrace-System zugeführt werden. In manchen Fällen wie z.B. VDI können auch Darktrace Host-Agenten benutzt werden. Allerdings ist letzteres im OT-Umfeld eher selten der Fall.

	Anforderung	Darktrace
Planung	Das anfallende Protokoll- und Protokollierungs-datenaufkommen KANN (und wird dringend empfohlen) anhand eines repräsentativen Systems pro Systemgruppe bestimmt werden.	Abhängig von den Anforderungen an die Verkehrsverarbeitung sind verschiedene Größen von Darktrace-Hardware und virtuellen Sensoren verfügbar. Bei der Größenbestimmung der Sensoren werden Metriken wie die Anzahl der modellierten Geräte, die aufgenommene Bandbreite und die verarbeiteten Verbindungen pro Minute berücksichtigt. Daten von repräsentativen Systemen können verwendet werden, um das gesamte Datenvolumen für Systemgruppen und folglich die Bearbeitungsanforderungen für den Darktrace-Einsatz zu berechnen. Die technischen Spezialisten von Darktrace unterstützen Sie bei diesen Berechnungen anhand der vom Kunden zur Verfügung gestellten Daten.
	Die Ergebnisse der Planungsphase MÜSSEN in einer geeigneten Form dokumentiert werden. Die Dokumentation MUSS alle Netzbereiche, die Protokoll- und Protokollierungsdatenquellen, deren Beziehungen untereinander und den Datenfluss der Protokoll- und Protokollierungsdaten im Anwendungsbereich umfassen.	Nach Abschluss der Ermittlung des Darktrace-Einsatzes in der Kundenumgebung können die technischen Spezialisten von Darktrace bei der Erstellung der Einsatzdokumentation behilflich sein, in der Datenerfassungspunkte, Datentypen, Sensorenplatzierung, erforderliche Kommunikationskanäle und Integrationen für die Datenanreicherung und den Workflow angegeben sind.
	Hierbei ist ein angemessener Abstraktions- und Detailgrad zu wählen, sodass der effektive Einsatz von SzA bewertet werden kann. 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. Darüber hinaus MUSS für jedes System bzw. für jede Systemgruppe dokumentiert werden, welche Ereignisse dieses bzw. diese protokolliert.	In der Einsatzdokumentation werden die Platzierung der Sensoren und die von den einzelnen Sensoren erfassten Daten bzw. Systeme sowie der Darktrace-Einsatz als Ganzes angegeben. Ähnliche Netzwerke werden wahrscheinlich ähnliche Darktrace-Einsatzarchitekturen und Datenerfassungsmethoden verwenden.
	Es MUSS ein Prozess eingerichtet werden, der sicherstellt, dass die Protokollierung bei Veränderungen im Anwendungsbereich (Changes) entsprechend angepasst wird.	Darktrace DETECT erlangt ein spezifisches Verständnis Ihrer digitalen Umgebung und analysiert kontinuierlich Ihre Benutzer, Assets, Geräte und die komplexen Zusammenhänge zwischen ihnen. DETECT lernt "im laufenden Betrieb" und passt sich an Ihr Unternehmen an, während dieses wächst und sich verändert - für einen langfristigen Schutz vor neuartigen Bedrohungen in einer sich ständig entwickelnden Bedrohungslandschaft. Dadurch erfordern viele Änderungen des Leistungsumfangs keine Rekonfiguration in Darktrace. Die modulare Architektur von Darktrace ermöglicht es jedoch zusätzliche Punkte zur Datenerfassung bei Bedarf einfach hinzuzufügen.

	Anforderung	Darktrace
Umsetzung Aufbau zentralisierter Protokollierungsinfrastrukturen:	Alle gesammelten sicherheitsrelevanten Protokoll- und Protokollierungsdaten MÜSSEN an für den jeweiligen Netzbereich zentralen Stellen gespeichert werden. Die Zahl an zentralen Stellen zur Speicherung SOLLTE möglichst gering gehalten werden und sich mindestens an funktionalen Einheiten orientieren, sodass der Zugriff auf die gespeicherten Daten einfach erfolgen kann. Die Protokollierungsinfrastruktur MUSS dazu ausreichend dimensioniert sein. Dafür MÜSSEN genügend technische, finanzielle und personelle Ressourcen verfügbar sein.	Darktrace nutzt eine primäre Appliance & sekundäre Probe(s) Appliance(s) Architektur, in der eine oder mehrere Appliances/Sensoren, die als Probes konfiguriert sind, wichtige Metadaten an eine einzige primäre Appliance weiterleiten. Eine Darktrace-Probe-Appliance kann am gleichen Ort wie die primäre Appliance platziert werden, um die Fähigkeit der Rohpaketerfassung vertikal zu erweitern, oder an einem separaten Ort für geographisch verteilte Topologien. Die primäre Appliance hostet die Benutzeroberfläche, die eine einheitliche Ansicht für den Datenzugriff bietet. Für einen gewöhnlichen Betreiber des Systems ist die Existenz der primären/sekundären Konfiguration nicht sichtbar.
Bereitstellung von Protokoll- und Protokollierungsdaten für die Auswertung:	Die gesammelten Protokoll- und Protokollierungsdaten MÜSSEN gefiltert, normalisiert, aggregiert und korreliert werden. Die so bearbeiteten Protokoll- und Protokollierungsdaten MÜSSEN geeignet verfügbar gemacht werden, damit sie ausgewertet werden können. Eine zeitlich befristete Speicherung der unbearbeiteten Protokolldaten KANN den Detektionsprozess zusätzlich unterstützen.	Darktrace wurde entwickelt, um Protokoll- und Protokollierungsdaten aus einer Vielzahl von Quellen zu sammeln und zu verarbeiten, darunter Netzwerkverkehr in IT- und OT-Umgebungen, Endpunkte außerhalb des Netzwerks, Cloud-Umgebungen und andere externe Quellen über Syslog-Ingestion oder API-Integrationen. Das System filtert, normalisiert, aggregiert und korreliert diese Daten und erleichtert es Sicherheitsanalysten, potenzielle Bedrohungen schnell zu identifizieren und zu untersuchen. Alle erfassten Daten werden über benutzerfreundliche Dashboards zur Verfügung gestellt, die einen umfassenden Überblick über alle Netzwerkaktivitäten bieten und die Auswertung von Anomalien, unerwünschten Aktivitäten und verdächtigem Verhalten ermöglichen. Darüber hinaus unterstützt Darktrace die temporäre Speicherung von unverarbeiteten Protokolldaten in Form von PCAPs, um eine effiziente Untersuchung von Bedrohungen zu ermöglichen.
	Für die Erzielung einer angemessenen Sichtbarkeit von Angriffen SOLLTEN die Protokollierungsdatenquellen auf Netzebene von außen (Netzgrenzen) nach innen (Netzbereiche) erschlossen werden.	Darktrace ist in der Lage, Angriffe dank Konfigurationen von Port/VLAN-Spiegelung oder TAPs zu erkennen. Darktrace zielt darauf ab, den gesamten Datenverkehr, der die betreffende Switch-Infrastruktur durchläuft, sichtbar zu machen, und kann überall im Netzwerk von dem äußersten Rand bis zum internen Netzwerk eingesetzt werden. Dadurch kann das System den gesamten Geräteverkehr (IT, OT, VoIP, IoT) innerhalb eines bestimmten Netzwerks überwachen, ohne dass es direkt an jedem Endpunkt eingesetzt werden muss. Darktrace erfasst und modelliert alle Arten von Datenverkehr, einschließlich verschlüsselter und unbekannter Protokolle, und führt eine Bedrohungserkennung durch.
	Die Systemebene (kritische Anwendungen und Applikationen) SOLLTE ausgehend von den zentralen, kritischen Systemen, wie z. B. Prozessleit- und Automatisierungstechnik und Leitsystemen, erschlossen werden. Die Priorisierung zur Auswahl der Protokollierungsdatenquellen SOLLTE ausgehend von der Kritikalität der Systeme abgeleitet werden.	Darktrace wird an einem zentralen Punkt eingesetzt, um möglichst viele Daten einsehen zu können, kann aber auch in anderen Bereichen eingesetzt werden, um sicherzustellen, dass alle kritischen Systeme, wie z. B. Prozesssteuerungs- und Automatisierungstechnik und Leitsysteme, abgedeckt sind. Darktrace ist in der Lage, die kritischsten Systeme zu priorisieren, da die Lösung stets auf die spezifischen Sicherheitsanforderungen abgestimmt ist.

	Anforderung	Darktrace
Bereitstellung von Protokoll- und Protokollierungsdaten für die Auswertung:	Nach erfolgreicher Umsetzung der Protokollierung MUSS geprüft werden, ob alle geplanten Protokollierungsdatenquellen gemäß der Planung umgesetzt wurden. Sollten branchenspezifisch weitergehende gesetzliche oder regulatorische Anforderungen an die Protokollierung bestehen, so MÜSSEN diese ebenfalls entsprechend umgesetzt werden.	Nach der erfolgreichen Implementierung der Protokollierung wird eine vollständige Datenprüfung mit dem Darktrace-Team durchgeführt. Damit soll sichergestellt werden, dass die während der Planung eingerichteten Datenquellen für die Protokollierung korrekt vom System aufgenommen werden. Während dieses Datenchecks wird überprüft, ob die richtigen Bereiche der Netzwerke überwacht werden, ob der für diese Geräte gesehene Netzwerkverkehr vollständig und von hoher Qualität ist und ob die während der Planung festgelegten Protokollquellen von Dritten ebenfalls gesehen werden und die Daten im System bereichern. Weitere gesetzliche und behördliche Anforderungen an die Protokollierung können ebenfalls während der Planung festgelegt und während des Datenprüfungsprozesses verifiziert werden. Abhängig von diesen Anforderungen gibt es Funktionen zur Anpassung der Implementierung.
Detektion		
Planung	Bei der Auswahl und dem Einsatz von Detektionsmaßnahmen MUSS eine umfassende und effiziente Abdeckung der Bedrohungslandschaft erzielt werden. Dazu MÜSSEN die Ergebnisse der Risikoanalyse sowie die Größe und Struktur des Unternehmens in der Planung einbezogen werden. Zur Bestimmung der Abdeckung KANN (und es wird empfohlen) eine standardisierte Methode angewendet werden (z. B. MITRE ATT&CK bzw. ATT&CK for ICS 6). In Abhängigkeit der Unternehmensgröße und der Bedrohungslandschaft KANN eine separate Betrachtung von Detektionsmaßnahmen für die IT- und OT-Umgebung erforderlich sein.	Darktrace verfügt über eine vollständig modulare Einsatzarchitektur, die vollständig skalierbar ist, um den gewünschten Umfang sowohl in Bezug auf die Größe und Struktur Ihres Unternehmens als auch auf die Sicherheitsanforderungen (wie in Ihrer Risikoanalyse definiert) zu erfüllen. Die Erkennungsmodelle von Darktrace für IT- und OT-Umgebungen sind vorkonfiguriert und den MITRE ATT&CK-Frameworks zugeordnet und können direkt zur Bestimmung der Abdeckung verwendet werden. Getrennte Erkennungsmaßnahmen für IT- und OT-Umgebungen werden bereits von den KI-basierten Erkennungsmodellen berücksichtigt, aber auch zusätzliche benutzerdefinierte Erkennungsmaßnahmen können nach Bedarf konfiguriert werden.

DARKTRACE

Erfüllen des IT-Sicherheitsgesetz 2.0

	Anforderung	Darktrace
Umsetzung	Als Mindestanforderung für die Detektion MÜSSEN alle Basisanforderungen von DER.1 Detektion von sicherheitsrelevanten Ereignissen und die folgenden Anforderungen erfüllt werden:	
Kontinuierliche Überwachung und Auswertung von Protokoll- und Protokollierungsdaten:	Alle Protokoll- und Protokollierungsdaten MÜSSEN kontinuierlich überwacht und ausgewertet werden. Dies KANN automatisiert werden, wenn bei relevanten Ereignissen eine unmittelbare Alarmierung der Verantwortlichen gewährleistet ist. Die Prüfung des Ereignisses und ggf. die Reaktion MUSS innerhalb einer der Risikoanalyse entsprechend geringen Zeitspanne erfolgen. Es MÜSSEN Mitarbeitende bzw. Mitarbeitende von Dienstleistern benannt werden, die dafür zuständig sind.	Darktrace überwacht die eingehenden Daten kontinuierlich 24/7. Darktrace DETECT kann dann anomales Verhalten erkennen und Warnungen generieren, der Darktrace Cyber AI Analyst kann dieses Verhalten untersuchen und Berichte darüber schreiben, und Darktrace RESPOND kann anomales Verhalten in Maschinengeschwindigkeit stoppen. Dies wird von der Darktrace-KI autonom durchgeführt, und die Benutzer können die Berichte einsehen oder die Warnungen in der Darktrace-Benutzeroberfläche weiter untersuchen. Darktrace kann Warnungen über die Darktrace Mobile App, E-Mail-Benachrichtigungen oder die Integration von Drittanbietern versenden. Darüber hinaus kann Darktrace mit Ticketing-Systemen integriert werden.
	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.	Darktrace bietet eine vollständige Protokollierung des Zugriffs und der Aktionen auf Darktrace, einschließlich der Benutzerprotokolle. Dieser Prüfpfad ist nativ in der Darktrace-Benutzeroberfläche verfügbar. Die Prüfprotokolle können auch im Syslog-Format an externe Systeme weitergeleitet werden.
	Für die Detektion von sicherheitsrelevanten Ereignissen MÜSSEN genügend personelle Ressourcen bereitgestellt werden.	Der Cyber AI Analyst verkürzt die Zeit bis zur Bedeutung von Vorfällen erheblich, indem er Schlüsselinformationen und eine Schilderung der Ereignisse liefert. Darktrace ist nicht dafür verantwortlich, auf Vorfälle zu reagieren, kann aber mit Darktrace-spezifischen Informationen helfen. Zugelassene Partner können zur Überwachung von Darktrace im Namen des Kunden eingesetzt werden, und optionale Dienste wie Ask the Expert und Proactive Threat Notification können die nativen Darktrace-Warnungen und das Account-Team ergänzen.
Einsatz zusätzlicher Detektionssysteme:	Es MÜSSEN Schadcodedetektionssysteme eingesetzt und zentral verwaltet werden. Anhand des Netzplans MUSS festgelegt werden, welche Netzsegmente durch zusätzliche Detektionssysteme geschützt werden müssen. Insbesondere MÜSSEN die im Netzplan definierten Übergänge zwischen internen und externen Netzen um netzbasierte Intrusion Detection Systeme (NIDS) ergänzt werden.	In Übereinstimmung mit dem gelieferten Netzwerkplan und den Gesprächen mit dem Kunden wird Darktrace Sonden in zentralen Bereichen einsetzen, in denen der gesamte Datenverkehr sichtbar ist. Dazu gehört ein SPAN auf Core-Switches an physischen Standorten oder die Installation virtueller Sensoren als VMs innerhalb von Hypervisoren oder Cloud-Umgebungen (VNets/VPCs), um virtuellen Verkehr aufzunehmen. Dies ermöglicht eine vollständige Erkennung von internem-internem und internem-externem Datenverkehr, wobei die Umgebung und Topologie des Kunden berücksichtigt wird, um zu bestimmen, wo diese Sonden eingesetzt werden sollten.
Infrastruktur zur Auswertung von Protokoll- und Protokollierungsdaten und Prüfung sicherheitsrelevanter Ereignisse:	Damit die Protokoll- und Protokollierungsdaten korreliert und abgeglichen werden können, SOLLTEN sie alle zeitlich synchronisiert werden. Die gesammelten Ereignismeldungen MÜSSEN regelmäßig auf Auffälligkeiten kontrolliert werden. Damit sicherheitsrelevante Ereignisse auch nachträglich erkannt werden können, MÜSSEN die Signaturen der Detektionssysteme immer auf aktuellstem Stand gehalten werden.	Die Darktrace-Plattform ist mit NTP-Servern integriert, um sicherzustellen, dass die Protokolle zeitlich synchronisiert sind, was es dem Endbenutzer ermöglicht, durch die erfassten Daten im Laufe der Zeit zu navigieren und Ereignisse ganzheitlich zu korrelieren. Beim Einsatz in einem primären/sekundären Appliance-Setup generieren Zeitunterschiede zwischen den Darktrace-Appliances auch Warnungen, sodass der Endbenutzer diese untersuchen und korrigieren kann. Basierend auf den erfassten Daten und Protokollen führt die Darktrace-Plattform eine Echtzeitanalyse des Datenverkehrs durch und warnt vor Anomalien und abnormalem Verhalten auf der Grundlage von KI-Lernen. Da diese Erkennungen nicht auf Regeln oder Signaturen basieren, sondern auf Abweichungen vom normalen Verhalten, werden die Daten, die der Alarmierung zugrunde liegen, durch die kontinuierlich lernende künstliche Intelligenz immer auf dem neuesten Stand gehalten.

	Anforderung	Darktrace
Auswertung von Informationen aus externen Quellen:	Um neue Erkenntnisse über sicherheitsrelevante Ereignisse für den eigenen Informationsverbund zu gewinnen, MÜSSEN externe Quellen herangezogen werden. 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. Informationen aus zuverlässigen Quellen MÜSSEN grundsätzlich ausgewertet werden. Alle gelieferten Informationen MÜSSEN danach bewertet werden, ob sie relevant für den eigenen Informationsverbund sind. Ist dies der Fall, MÜSSEN die Informationen entsprechend der Sicherheitsvorfallbehandlung eskaliert werden.	Darktrace kann externe Bedrohungen in Form von STIX- oder TAXII-Benachrichtigungen aufnehmen, um bekannte bösartige externe IP/Domänen zu verstehen. Diese Daten fließen in das Darktrace-Lernsystem ein und ermöglichen es Darktrace, eine Warnung auszusprechen und diese Verbindungen möglicherweise zu blockieren, um zu verhindern, dass Benutzer oder bösartige Programme auf die bekannt schlechte externe Domain zugreifen. Darktrace kann diese Daten auch über Darktrace-API-Aufrufe empfangen - wenn die Daten also in einem inkompatiblen Format vorliegen, können sie zunächst manipuliert und an Darktrace weitergeleitet werden, damit sie in die Modellierung und Alarmierung passen. Wenn andere Programme von Drittanbietern verwendet werden, die Daten in Syslog exportieren können, können diese in Form von benutzerdefinierten Datenalarmen an Darktrace gesendet werden. Diese Alarme können dann aus der Perspektive einer Anomalie verstanden werden, wobei Darktrace diese Alarme analysiert und versteht, um die relevante Anomalie ihres Auftretens für das Gerät oder das Netzwerk als Ganzes zu bestimmen. Darktrace-Kunden können Darktrace Inoculation aktivieren, die zum Schutz der Kunden dient, indem sie Bedrohungen identifiziert, die in der gesamten Darktrace-Basis auftreten, sie anonymisiert und Verbindungen im spezifischen Client-Netzwerk analysiert, um zu sehen, ob sie auch in der lokalen Client-Umgebung auftreten.
Auswertung der Protokoll- und Protokollierungsdaten durch spezialisiertes Personal:	Es MÜSSEN Mitarbeitende bzw. Mitarbeitende von Dienstleistern speziell damit beauftragt werden, alle Protokoll- und Protokollierungsdaten auszuwerten. 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. Dieses Personal SOLLTE spezialisierte weiterführende Schulungen und Qualifikationen erhalten. Ein Personenkreis MUSS benannt werden, der für das Thema Auswertung von Protokoll- und Protokollierungsdaten verantwortlich ist.	Alle von Darktrace empfangenen Daten werden in der Benutzeroberfläche für die Protokollierung zur Verfügung gestellt. Unverarbeiteter Netzwerkverkehr sowie Telemetriedaten, die an Darktrace gesendet und analysiert werden, werden protokolliert und können in der erweiterten Suche überprüft werden. Die Daten werden auch verarbeitet und analysiert, um das typische Verhalten von Nutzer und Geräten zu verstehen, wobei anormale Aktivitäten in Form von Modellverletzungen und AI-Analysten-Vorfällen zur Kenntnis genommen werden. Auf diese Daten kann über den Threat Visualiser zugegriffen werden. Die Protokolle können über die erweiterte Suche abgefragt werden, damit die Benutzer bei Bedarf nach bestimmten Aktivitäten oder Mustern suchen können. Jede Appliance in der Bereitstellung zeigt auch Details zu den Daten an, die in die Appliance eingespeist werden. Es werden Warnungen zum Zustand der Appliances ausgegeben, um eine kontinuierliche Protokollierung und Leistungsüberwachung zu ermöglichen. Benutzer, die für die Analyse von Log- und Protokolldaten verantwortlich sind, können eine spezielle Schulung für die Administration der Darktrace-Plattform erhalten. Das Darktrace Threat Visualizer Administrationstraining ist für alle relevanten Benutzer auf dem Darktrace Kundenportal verfügbar.

	Anforderung	Darktrace
Zentrale Detektion und Echtzeitüberprüfungen von Ereignismeldungen:	Es MÜSSEN zentrale Komponenten eingesetzt werden, um sicherheitsrelevante Ereignisse zu erkennen und auszuwerten. 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. Alle eingelieferten Protokoll- und Protokollierungsdaten MÜSSEN lückenlos in der Protokollverwaltung einsehbar und auswertbar sein. Die Daten MÜSSEN kontinuierlich ausgewertet werden.	Darktrace stellt sicher, dass zentrale Komponenten verwendet werden, um sicherheitsrelevante Ereignisse zu erkennen und auszuwerten, indem die Aktivitäten innerhalb einer Umgebung in einem einzigen Fenster angezeigt werden. Ein Deployment-Setup umfasst entweder eine Primary-Secondary-Appliance-Konfiguration, bei der sekundäre Sonden verwendet werden, um den Datenverkehr von einer Vielzahl physisch verteilter Punkte zu erfassen, oder ein Unified View, der aus mehreren Appliances besteht und die Skalierung des Deployments ermöglicht. Die zentrale, automatisierte Analyse innerhalb des Systems wird auf der Ebene der primären Appliance durchgeführt, sodass Daten von verschiedenen Sonden korreliert und relevante Sicherheitswarnungen ausgelöst werden können. In Unified View-Umgebungen werden Modellbrüche auf den Mastern selbst ausgelöst, wobei der Darktrace Cyber AI Analyst auf der Unified View läuft und in der Lage ist, Informationen für Cybersicherheitsereignisse und -vorfälle miteinander zu korrelieren. Daten und Protokolle in Darktrace sind vollständig sichtbar und können über den Threat Visualizer abgefragt und ausgewertet werden. Mit der erweiterten Suche von Darktrace können Sie nach bestimmten Aktivitäten oder Verbindungen filtern, um Bedrohungen aufzuspüren oder Protokolle zu verwalten. Die in Darktrace eingehenden Daten werden kontinuierlich überwacht, wobei Modellbrüche bei anomaler Aktivität ausgelöst werden, wenn das Aktivitätsmuster eines Benutzers oder Geräts von der normalen Aktivität abweicht. Die Daten können in der erweiterten Suche überprüft und ausgewertet werden, um weitere Bedrohungen zu finden und zu analysieren.

	Anforderung	Darktrace
Zentrale Detektion und Echtzeitüberprüfungen von Ereignismeldungen:	Werden definierte Schwellenwerte überschritten, MUSS automatisch alarmiert werden. 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. Die Systemverantwortlichen MÜSSEN regelmäßig die Analyseparameter auditieren und anpassen, falls dies erforderlich ist. Zusätzlich MÜSSEN bereits überprüfte Protokoll- und Protokollierungsdaten regelmäßig hinsichtlich sicherheitsrelevanter Ereignisse automatisch untersucht werden.	Die Darktrace-Plattform überwacht kontinuierlich die Aktivitäten innerhalb der Umgebung und versteht das normale Verhalten eines Benutzers und der Geräte. Dadurch kann Darktrace anomale Aktivitäten erkennen und Warnungen in Form von Modellbrüchen auslösen, um Verhaltensänderungen hervorzuheben. Bei einem Modellbruch untersucht der Cyber AI Analyst die Aktivitäten des Benutzers oder Geräts, um festzustellen, ob ein Sicherheitsvorfall ausgelöst werden muss, wobei relevante Details für weitere Untersuchungen bereitgestellt werden, wenn ein AI-Analyst-Vorfall ausgelöst wird. Modellbrüche und AI-Analyst-Vorfälle werden mit einem Schweregrad (0-100) ausgelöst, um die Dringlichkeit des Vorfalls hervorzuheben, und können auch auf der Grundlage der Kritikalität des Verhaltens (kritisch, verdächtig, Compliance oder informativ) klassifiziert werden. Modellbrüche und AI-Analyst-Vorfälle stehen den Benutzern für die Triage zur Verfügung. Es kann eine Mindestpunktzahl oder ein Mindestverhalten festgelegt werden, damit die Benutzer die Aktivitäten je nach Schwerpunkt untersuchen können. Alarme werden direkt in Darktrace ausgelöst oder können an externe Systeme (wie SIEMs oder SOARs) zum Zwecke des Workflows gesendet werden. Es kann eine Mindestpunktzahl und ein Mindestverhalten festgelegt werden, um sicherzustellen, dass die gewünschten Alarme an die Systeme gesendet werden. Innerhalb der Darktrace-Benutzeroberfläche stehen den Benutzern Workflow-Mechanismen zur Verfügung, wie z. B. das Bestätigen von Alarmen und Vorfällen nach Abschluss der Untersuchung sowie das Kommentieren von Alarmen und Vorfällen, um ihre Erkenntnisse und alle relevanten Details hervorzuheben. Die Systemmanager können die Aktivitäten innerhalb der Benutzeroberfläche regelmäßig überprüfen, um die durchgeführten Warnungen und Analysen zu verstehen, und sie können bei Bedarf die Schwellenwerte für Warnungen an andere Systeme anpassen. Während der Untersuchung oder zum Zweck des Audits können die Benutzer die Protokolle regelmäßig überprüfen, um frühere Aktivitäten zu verstehen, die bei einem Benutzer oder einem Gerät ausgelöst wurden, oder innerhalb der Umgebung mithilfe der erweiterten Suche, um einen ganzheitlichen Überblick über ein Gerät über einen längeren Zeitraum zu erhalten. Darüber hinaus können Berichte erstellt werden, die eine Zusammenfassung der Sicherheitswarnungen und -vorfälle in einer Umgebung über einen bestimmten Zeitraum liefern.
	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. 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.	PREVENT von Darktrace gibt Sicherheitsteams die Informationen an die Hand, die sie benötigen, um ihre Systeme kontinuierlich zu härten, indem es Schwachstellen sowohl auf den dem Internet zugewandten Systemen als auch auf den Systemen innerhalb des Netzwerks sichtbar macht. Das Attack Surface Management Tool sucht nach bekannten Schwachstellen und potenziellen Fehlkonfigurationen, die ausgenutzt werden können, um Zugang zum internen Netzwerk zu erhalten. Darüber hinaus extrahiert die Newsroom-Funktion Berichte von Anbietern, Medien und Nachrichtenquellen, um auf aktuelle Schwachstellen aufmerksam zu machen und betroffene Systeme hervorzuheben.

	Anforderung	Darktrace
Zentrale Detektion und Echtzeitüberprüfungen von Ereignismeldungen:	Bei der Umsetzung von Detektionsmechanismen SOLLTE initial eine Kalibrierung durchgeführt werden, um festzustellen, welche sicherheitsrelevanten Ereignisse (SRE) im Normalzustand auftreten (Baselining). Dazu SOLLTE bewertet werden, ob dieser Normalzustand in Hinblick auf die Zahl der falsch positiven Meldungen hingenommen werden kann oder ob Änderungen vorzunehmen sind. Die Kalibrierung SOLLTE bei Änderungen innerhalb des Anwendungsbereichs oder der Bedrohungslage erneut durchgeführt werden.	Die selbstlernende KI von Darktrace benötigt keine feste Basisperiode, um einen Normalzustand zu definieren. Sie nutzt kontinuierliches Lernen, um sich an Veränderungen anzupassen, wenn sich das Netzwerk weiterentwickelt. Das System ermöglicht die Anpassung von Anomalien, die als harmlos angesehen werden. Dies kann durch das Hinzufügen von Anlagen oder Bereichen zu Erlaubnislisten oder durch das gezielte Hinzufügen von Niederlagen zu einzelnen Alarmen erreicht werden. Dieser Abstimmungsprozess kann zu jedem Zeitpunkt nach der Installation beliebig oft durchgeführt werden.
	Die SRE MÜSSEN überprüft und dahingehend bewertet werden, ob sie auf einen Sicherheitsvorfall (qualifizierter SRE) hindeuten. Die zur Angriffserkennung eingesetzten Systeme sollten, in eindeutig zuordenbaren Fällen, eine automatisierte Qualifizierung der SRE ermöglichen. Nur qualifizierte SRE SOLLTEN den Prozess der Reaktion auslösen. Die Qualifizierung SOLLTE in automatisiert nicht eindeutig zuordenbaren Fällen manuell durch festgelegte Verantwortliche vorgenommen werden. Basierend auf den gewonnenen Erkenntnissen der Qualifizierung MÜSSEN die Detektionsmechanismen nachjustiert werden.	Darktrace-Warnungen werden automatisch klassifiziert als: "Kritisch", "Verdächtig", "Informativ" und "Compliance". Dies basiert auf der ungewöhnlichen Stärke der Aktivität und der möglichen Auswirkung, die sie auf das Netzwerk haben könnte, z. B. würde eine sich schnell bewegende Ransomware als kritisch eingestuft werden. Diese Zuordnungen können auch durch Erhöhen oder Verringern der Prioritäten von Assets und des zugrunde liegenden Erkennungsmodells angepasst werden.
	Sollten branchenspezifisch weitergehende gesetzliche oder regulatorische Anforderungen bestehen, so MÜSSEN diese ebenfalls entsprechend umgesetzt werden.	Da Darktrace einen vollständigen Überblick über den digitalen Besitz einschließlich aller Netzwerkverkehrsströme bietet, kann es dabei helfen, festzustellen, wo rechtliche oder regulatorische Anforderungen nicht korrekt erfüllt werden.

	Anforderung	Darktrace
Reaktion		
	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. 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.	Darktrace ist branchenführend bei der Erkennung und Reaktion auf bekannte und unbekannte, neuartige Bedrohungen - unabhängig davon, ob diese von innerhalb oder außerhalb Ihres Unternehmens ausgehen - und in allen von Ihnen verwendeten Datenumgebungen. Auf diese Weise sollte der Einsatz der Darktrace-Software das Risiko eines Sicherheitsvorfalls erheblich verringern. Sollte es dennoch zu einem solchen Vorfall kommen, bietet die Darktrace-Software eine umfassende forensische Analyse, die dem Analystenteam eines Unternehmens Zeit spart und dazu beiträgt, dass das Unternehmen so schnell wie möglich wieder voll funktionsfähig ist. Neben dieser menschlichen Analyse bietet Darktrace auch eine KI-gesteuerte Analystenfunktion, die jeden potenziellen Sicherheitsvorfall selbstständig untersucht, wodurch ein menschliches Analystenteam erheblich entlastet und die Zeit bis zum Verständnis eines Ereignisses verkürzt wird. Falls erforderlich, würde dies auch die Zeit eines solchen Teams für die Meldung eines solchen Vorfalls an die zuständige interne oder externe Behörde erheblich reduzieren
Automatische Reaktion auf sicherheitsrelevante Ereignisse:	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. 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. Sollte eine automatische Reaktion nicht möglich sein, MUSS über manuelle Prozesse sichergestellt werden, dass der mögliche Sicherheitsvorfall unterbunden wird.	Darktrace schlägt nicht nur Alarm, wenn es eine sicherheitsrelevante Verhaltensanomalie feststellt, sondern der Reaktionsmechanismus schlägt auch eine mögliche Blockiermaßnahme vor, um das Verhalten zu stoppen, die angemessen und proportional zum festgestellten Vorfall ist. Der Reaktionsmechanismus kann im Bestätigungsmodus konfiguriert werden, sodass Administratoren die vorgeschlagenen Sperren kontrollieren können, bevor sie das System sperren lassen, oder im autonomen Modus, d. h. das System sperrt automatisch entsprechend den vorgeschlagenen Abhilfemaßnahmen, gibt Administratoren aber immer noch die Möglichkeit, diese zu übersteuern. Eine automatische Reaktion ist in allen Fällen möglich, zusätzlich erlaubt Darktrace jedoch auch manuelle Sperren. Darktraces einzigartiges KI-basiertes Lernen stellt außerdem sicher, dass die von Darktrace vorgeschlagenen oder angewendeten Sperren sehr präzise sind und nicht die Geschäftssysteme blockieren, sondern nur den spezifischen Datenverkehr, den Darktrace als verhaltensauffällig einstuft, um sicherzustellen, dass kritische Dienste nicht beeinträchtigt werden.
	Der Ausschluss von Netzen oder Netzsegmenten von einer automatischen Reaktion, bzw. dem Eingriff in den Datenstrom MUSS schlüssig begründet sein.	Darktrace ermöglicht es den Administratoren des Systems, die Subnetze und Gerätetypen auszuwählen, auf die das autonome Reaktionssystem angewendet werden darf. Mit Hilfe des Tagging-Systems können Kunden bestimmte hochsensible Bereiche des Netzwerks von einer möglichen Unterbrechung durch die Darktrace Response-Funktion ausschließen.
	Festgestellte Sicherheitsvorfälle im vermeintlichen Zusammenhang mit Angriffen MÜSSEN behandelt werden.	Darktrace lernt das Verhalten von Geräten im Netzwerk. Sollten diese Geräte anfangen, sich seltsam zu verhalten, wird Darktrace zunächst eine Warnung ausgeben, wenn ein möglicher Sicherheitsvorfall zu diesem Verhalten besteht. Sollte sich das Verhalten fortsetzen, wird die Darktrace Response-Funktion ebenfalls eingreifen, mit dem Ziel, das seltsame Verhalten zu blockieren. Darktrace kann auch in SIEM-Lösungen integriert werden, um Kunden dabei zu helfen, kritische Alarme in Dashboards anzuzeigen, die das SOC-Team möglicherweise erstellt hat. Die mobile App ermöglicht Administratoren einen schnellen mobilen Zugriff auf Darktrace-Warnungen und Response-Aktionen.

	Anforderung	Darktrace
Automatische Reaktion auf sicherheitsrelevante Ereignisse:	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.	Im Falle eines Sicherheitsvorfalls bieten Darktrace DETECT und RESPOND Sichtbarkeit und automatische Reaktion, um einen solchen Vorfall zu verhindern. Sollte es notwendig sein, einen Vorfall zu analysieren, um festzustellen, ob der Vorfall eine Meldepflicht erfüllt, kann Darktrace den Vorfall auf verschiedene Weise vollständig kontextualisieren. Das Sicherheitsteam kann eine AI-Analysten-Untersuchung des Vorfalls/Geräts auslösen, um eine Zusammenfassung der ungewöhnlichen Aktivitäten im Berichtsformat zu erhalten. Vollständige Verbindungsdetails und Metadaten können für den jeweiligen Vorfall/das jeweilige Gerät exportiert werden, um die Besonderheiten jeder Verbindung zu ermitteln. Teilweise Paketerfassungen können in Bezug auf die beteiligten Verbindungen heruntergeladen werden. Mithilfe von Darktrace DETECT kann das Sicherheitsteam eine fundierte Entscheidung darüber treffen, ob der Vorfall in Bezug auf die relevanten BSIG- und EnWG-Gesetze gemeldet werden muss.
	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. Dabei MUSS gewährleistet sein, dass ausschließlich automatisiert ergriffene Maßnahmen nicht zu einer relevanten Beeinträchtigung der kritischen Dienstleistung des Betreibers führen können.	Darktrace analysiert kontinuierlich alle Geräte und IPs im Netzwerk und erstellt ein Lebensmuster für diese einzelnen Geräte sowie für das Netzwerk als Ganzes. Ungewöhnliche und/oder bösartige Aktivitäten werden erkannt, wenn Geräte von der normalen Aktivität abweichen. Darktrace warnt vor diesen Ereignissen und Angriffen und ist in der Lage, selbstständig und angemessen zu reagieren, um den Angriff zu neutralisieren. Wichtig ist, dass Darktrace ein Verständnis von "normal" hat und somit in der Lage ist, auf Angriffe zu reagieren, ohne den normalen Geschäftsbetrieb zu beeinträchtigen oder kritische Dienste zu beeinträchtigen.
	Die eingesetzten SzA SOLLTEN auch eine nicht-automatisierte Qualifizierung und Behandlung von Ereignissen unterstützen.	Der Reaktionsmechanismus von Darktrace kann von Administratoren vollständig kontrolliert werden, um festzulegen, welche Verhaltensweisen automatisch blockiert werden sollen. Dies kann auf der Basis von Verhaltensabweichungen und auf Zeitbasis gesteuert werden. Darüber hinaus können manuelle RESPOND-Aktionen und Blockierungen durch das Sicherheitsteam ausgelöst werden.

Über Darktrace

Darktrace (DARK.L), ein weltweit führendes Unternehmen im Bereich der künstlichen Intelligenz für Cybersicherheit, bietet umfassende KI-gestützte Lösungen an, um die Welt von Störungen durch das Internet zu befreien. Die Technologie von Darktrace lernt und aktualisiert kontinuierlich ihr Wissen über "Sie" in einem Unternehmen und wendet dieses Verständnis an, um einen optimalen Zustand der Cybersicherheit zu erreichen. Darktrace liefert den ersten Cyber-KI-Loop, der eine kontinuierliche End-to-End-Sicherheitsfunktion bereitstellt, die neuartige, laufende Bedrohungen in Echtzeit selbstständig verhindern, erkennen und darauf reagieren kann. Darktrace beschäftigt weltweit mehr als 2.200 Mitarbeiter und schützt mehr als 8.400 Organisationen weltweit vor fortschrittlichen Cyber-Bedrohungen.

Scannen, um mehr zu erfahren

DARKTRACE

Evolving threats call for evolved thinking™

Nordamerika: +1 (415) 229 9100
Europa: +44 (0) 1223 394 100
Asien-Pazifik: +65 6804 5010
Lateinamerika: +55 11 4949 7696
info@darktrace.com
darktrace.com