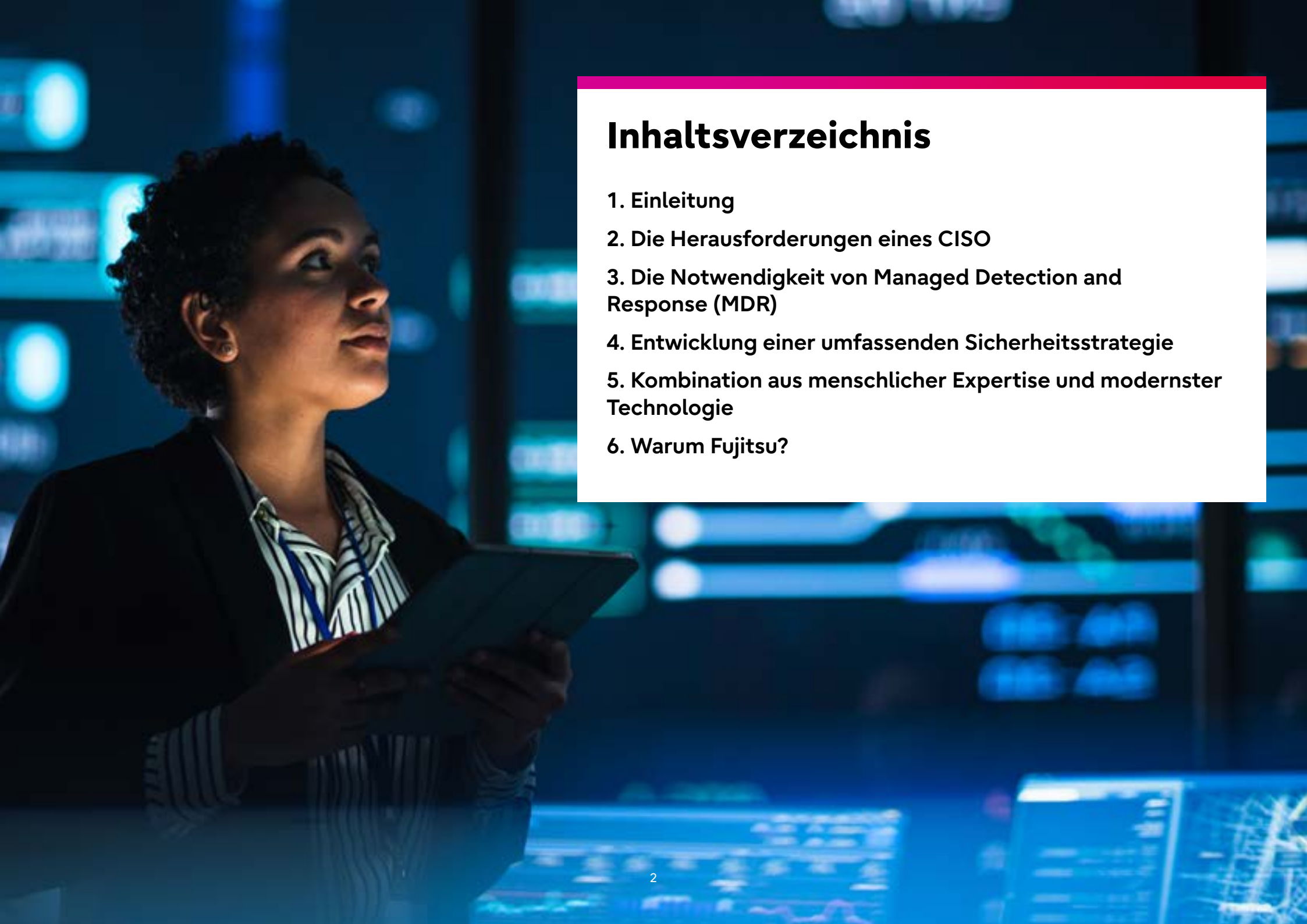
FUJITSU

Managed Detection and Response

Schnellere Sicherheitsreaktionen und geringere Geschäftsrisiken mit Fujitsu

Solution Guide



Inhaltsverzeichnis

1. Einleitung
2. Die Herausforderungen eines CISO
3. Die Notwendigkeit von Managed Detection and Response (MDR)
4. Entwicklung einer umfassenden Sicherheitsstrategie
5. Kombination aus menschlicher Expertise und modernster Technologie
6. Warum Fujitsu?

“Eine schnellere Bedrohungserkennung ohne gleichzeitige Beschleunigung der Reaktion ist sinnlos, da der sichere Ausgangszustand erst durch eine schnelle Reaktion wiederhergestellt werden kann. Das erkennen Sicherheitsverantwortliche zunehmend.”

Gartner Research Market Guide für Managed Detection and Response Services

1. Einleitung

Die Bedrohungslandschaft wächst rasant an Komplexität und Geschwindigkeit. Unternehmen stehen ständig vor neuen Sicherheitsrisiken: Phishing, Ransomware und die Ausnutzung von Schwachstellen in Anwendungen und Netzwerken sind nur einige Beispiele. Diese Bedrohungen gefährden den Geschäftsbetrieb und erfordern eine umfassende Lösung, die sowohl Erkennung als auch Reaktion umfasst. Ein effektives Sicherheitsmanagement ist daher unerlässlich. Ohne einen zentralen und dynamischen Ansatz zur Abwehr dieser Bedrohungen ist das Unternehmen deutlich anfälliger für Angriffe und Sicherheitsverletzungen.

2. Die Herausforderungen eines CISO

Stellen Sie sich einen Chief Information Security Officer (CISO) vor, dessen Aufgabe der Schutz des Unternehmens vor den ständigen Gefahren von Cyberangriffen ist.

Die Arbeit eines CISO ist ein Spagat zwischen Risikomanagement, Ressourcenmanagement und oft auch Budgetbeschränkungen. Der CISO und das Security Operations Team werden mit einer Flut von Warnmeldungen konfrontiert und müssen die tatsächlichen Bedrohungen (True Positives) identifizieren und darauf reagieren. Es gibt eine Vielzahl manueller Aufgaben, täglicher Kontrollen und die Notwendigkeit, mehrere und unterschiedliche Sicherheitswerkzeuge zu verwalten. Der Druck ist enorm – jedes Übersehen kann zu Sicherheitsverletzungen, erheblichen regulatorischen Strafen, unerwünschter Medienaufmerksamkeit und Reputationsschäden führen.

Die Situation des CISO

- Vergangene Sicherheitsvorfälle mahnen eindrücklich an die möglichen Folgen von Sicherheitsverletzungen.
- Alarmüberlastung ist alltäglich – die Menge an Sicherheitsereignissen ist überwältigend.
- Die Sicherstellung der ordnungsgemäßen Konfiguration, Wartung und Patching der Technologien ist eine kontinuierliche und für die Sicherheitsintegrität unerlässliche Aufgabe.
- Das Feinabstimmen und Konfigurieren von Regeln zur Abwehr hochentwickelter Bedrohungen erfordert Expertenwissen, das nur schwer zu finden ist.
- Die Überwachung von Sicherheitswarnungen ist ein ständiger Aufwand. Eine weitere große Herausforderung besteht darin, effektiv und zeitnah zu reagieren.

Ein neuer Anfang

Die Ressourcenverschwendung durch ineffektive Incident Triage und False Positives gehört der Vergangenheit an. Ein CISO benötigt einen Echtzeit-Überblick über die Sicherheitslage seines Unternehmens mit erhöhter Transparenz, dynamisch und proaktiv. Angereicherte Bedrohungsinformationen ermöglichen es, sich auf reale Bedrohungen zu konzentrieren, zu reagieren und diese zu mindern.

Ein CISO benötigt die Gewissheit, dass sein Ansatz mit der sich entwickelnden Bedrohungslandschaft Schritt hält. Dies stellt sicher, dass das Unternehmen sicher und geschützt arbeiten kann, mit einer Bedrohungsreaktionstrategie, die sich ebenso schnell anpasst und reagiert wie die Bedrohungen, denen sie entgegenwirkt.

3. Die Notwendigkeit von Managed Detection and Response (MDR)

Managed Detection and Response (MDR) geht über traditionelle und voneinander getrennte Sicherheitsdienste wie Security Information and Event Management (SIEM) hinaus. Es handelt sich um einen zentralen, dynamischen Dienst, der durch Anreicherung und Korrelation von Daten echte Bedrohungen (True Positives) identifizieren und eine proaktive und optimale Reaktion ermöglichen kann.

Das Senden von Logs an eine SIEM-Plattform und das Warten auf ausgelöste Alarme ist einfach nicht mehr zeitgemäß. Regeln müssen dynamisch und mit hoher Genauigkeit erstellt werden, um die neuesten Bedrohungen zu erkennen. Daten müssen mit aktuellen Bedrohungsinformationen angereichert und markiert werden, und Reaktionen sollten nach Möglichkeit effizient und automatisiert erfolgen.

Frameworks wie MITRE ATT&CK gewinnen zunehmend an Bedeutung, um die Art des Angriffs und die verwendete Technik zu identifizieren. Die Korrelation dieser Informationen mit anderen Sicherheitsereignissen ermöglicht eine ganzheitliche und angereicherte analytische Sicht.

Dies sollte mit proaktiver Bedrohungsjagd kombiniert werden, anstatt auf ausgelöste Alarme zu warten. Dies muss nicht umfassend sein, aber die tägliche Analyse von Telemetriedaten sollte ein Schlüsselelement jedes MDR-Dienstes sein.

Kunden erwarten einen konsistenten und standardisierten Service. Monatliche Berichte mit detaillierten SLAs und Angaben zur Geräteverfügbarkeit sind weiterhin notwendig. Es ist wichtig, dass alle Vorfälle möglichst in Echtzeit gemeldet und analysiert werden, um eine effiziente Reaktion zu demonstrieren und das Vertrauen zu gewährleisten, dass keine Netzwerkverletzungen oder Datenexfiltrationen stattfinden.

Lernen Sie Jane kennen!

Erfahren Sie im Video, wie der Fujitsu Managed Detection and Response Service die Arbeit von Jane, einer erfahrenen CISO, und ihrem Team durch automatisierte Spitzentechnologie optimiert.

Hier geht es zum Video.

4. Entwicklung einer umfassenden Sicherheitsstrategie

Unser MDR-Service, der auf Microsoft Sentinel basiert, wird von unserem erfahrenen Team von Sicherheitsexperten weltweit unterstützt. Unsere Teams verfügen über umfassendes Wissen in kritischen Bereichen wie Bedrohungsinformationen (Threat Intelligence), Detektions-Engineering, Security Orchestration, Automation & Response (SOAR), Threat Hunting und Incident Response.

Wir engagieren uns für die kontinuierliche Verbesserung Ihrer Sicherheitslage, mit einem klaren Fokus auf die zeitnahe Reaktion auf tatsächliche Sicherheitsvorfälle und die Reduzierung von Fehlalarmen. Angesichts neuer Bedrohungen und strenger Compliance-Anforderungen bietet unser Service eine schnelle und zuverlässige Reaktion.

Unser MDR-Service wird die Sicherheit Ihres Unternehmens stärken und verbessern. Mit einem Schwerpunkt auf dem Microsoft-Stack über Microsoft Sentinel konfigurieren und implementieren wir Analyse-Regeln und reichern IP-Daten an, um ein umfassendes Verständnis des Kontextes von Vorfällen zu erhalten.

Unser Bereitstellungsmodell ist auf spezifische Bedürfnisse zugeschnitten. Die MDR-Services werden von unseren Global Delivery Centers (GDCs) aus erbracht, während regionale Sicherheitsteams vor Ort Unterstützung und Expertise bieten. Dieser kombinierte Ansatz stellt sicher, dass jeder Aspekt des Services effektiv und an die individuellen Anforderungen Ihres Unternehmens angepasst bereitgestellt wird.

Automatisierte Bereitstellung

Bedrohungsüberwachung

Standardregeln

Identifiziert gängige Bedrohungen

Vorfall-Triage

Unterscheidet zwischen echten und falschen Bedrohungen

Managed Detection and Response (MDR)

Detektions-Engineering

Dynamische Regeln und Such-Abfragen zur Erkennung und zum Schutz vor den neuesten Bedrohungen

Bedrohungs-Feeds

Anreicherung und Management von Bedrohungsinformationen

Threat Hunting

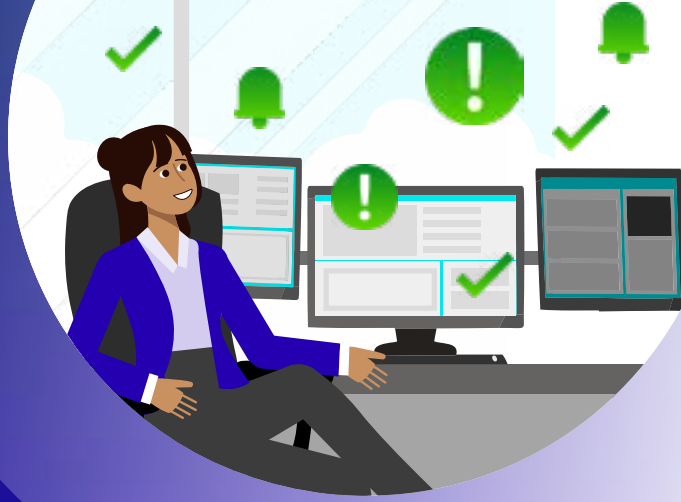
Aufdeckung bisher unerkannter Bedrohungen und angemessene Reaktion

Abhilfemaßnahmen

Definierte Maßnahmen zur Unterbindung von Bedrohungen

Plattform- und Service-Management

5. Kombination aus menschlicher Expertise und modernster Technologie



Unser MDR-Service wurde entwickelt, um die Sicherheit von Unternehmen zu verbessern, indem Ermittlungs- und Analysefunktionen geboten werden, die nicht nur Bedrohungen identifizieren, sondern diese auch effektiv unterbrechen und eindämmen.

Vorteile des Fujitsu MDR-Service:

Bessere Transparenz

Umfassendes Verständnis Ihrer Sicherheitslandschaft, schnelle Erkennung und Behebung kritischer Bedrohungen.

Optimierte Informationen

Zentrale Übersicht über Bedrohungen, Anreicherung von Vorfällen und Reduzierung von Fehlalarmen.

Automatische Einrichtung

Schnelle und einfache Implementierung, geringer Zeit- und Arbeitsaufwand, wettbewerbsfähiger Preis.

Schnelle Reaktionen

Agiler Service, schnelles und entschlossenes Handeln, Minimierung von Schäden und Gewährleistung der Betriebssicherheit.

Mit dem Fujitsu MDR-Service gehören ständige Sicherheitsbedrohungen der Vergangenheit an. Ihre Teams können sich voll und ganz auf strategische Initiativen und den Erfolg Ihres Unternehmens konzentrieren. Das bedeutet mehr Zeit für Innovation, Wachstum und den Ausbau Ihres Geschäfts – und weniger Zeit für die Abwehr von Cyberangriffen.

6. Warum Fujitsu?

Fujitsu zeichnet sich durch globale Expertise in Sicherheitsdienstleistungen aus. Unsere strategischen Partnerschaften in Wissenschaft, öffentlichem und privatem Sektor gewährleisten, dass wir an der Spitze der Branchenanforderungen bleiben.

Globale Reichweite mit lokaler Präsenz

Unser umfassendes Netzwerk von Global Delivery Centers (GDCs) wird durch lokale Expertise ergänzt. Wir stellen sicher, dass Ihnen jederzeit und an jedem Ort kompetente Unterstützung zur Verfügung steht. Wir liefern standardisierte Dienstleistungen zu kalkulierbaren Kosten. Wir bieten Ihnen die Expertise, die Sie benötigen – genau dann und dort, wo Sie sie benötigen.

Schnelle, sofort einsatzbereite Lösung

Unser MDR-Service wird als Code bereitgestellt und ist nicht nur datenbereit, sondern auch darauf ausgelegt, frühzeitig verwertbare Warnmeldungen zu liefern. Diese schnelle Bereitstellungsfähigkeit ist entscheidend für Unternehmen, die schnell auf sich entwickelnde Sicherheitsbedrohungen reagieren müssen.

Nahtlose technologische Integration

Fujitsu unterhält langjährige Partnerschaften mit weltweit führenden Anbietern von Sicherheitstechnologie, darunter Microsoft und andere.

Nachhaltigkeit im Vordergrund

Unser Engagement für Nachhaltigkeit ist in die Struktur unserer Dienstleistungen eingebunden. Wir legen bei der Bereitstellung unserer Services Wert auf umweltfreundliche Praktiken und zeigen damit unser Engagement, nicht nur digitale Assets zu schützen, sondern auch unseren Planeten zu bewahren.

FUJITSU

Beschleunigen Sie Ihre Sicherheitsreaktion mit Fujitsu

Stehen Sie vor scheinbar unüberwindlichen Herausforderungen im Bereich Cybersicherheit? Egal, ob Sie mit den Komplexitäten der Bedrohungserkennung zu kämpfen haben oder Ihre Reaktion auf Vorfälle optimieren möchten – Fujitsu unterstützt Sie dabei, Ihre Sicherheitsstrategie zu verbessern und Geschäftsrisiken zu mindern.

Von der ersten Bewertung über einen 30-tägigen Proof-of-Value-Test bis hin zur vollständigen Implementierung stehen unsere Experten bereit, um eine maßgeschneiderte Lösung zu entwickeln, die Ihre Abwehrkräfte stärkt und Ihren individuellen Sicherheitsanforderungen entspricht.

Nehmen Sie noch heute Kontakt mit Fujitsu auf und erfahren Sie, wie unsere globale Expertise, unsere innovativen Lösungen und unsere engagierten Teams zu Ihrem Erfolg im Bereich Cybersicherheit beitragen können.

Besuchen Sie uns unter Fujitsu's Managed Detection and Response service – Microsoft : Fujitsu Deutschland

Für weitere Informationen oder Fragen kontaktieren Sie uns bitte unter: cic@fujitsu.com