SERVICE & DISTRIBUTION GmbH
INDUSTRIEAUTOMATISIERUNG

UNSER MEHRWERT FÜR SIE

INDUSTRIAL CYBER SECURITY

IHNALTSVERZEICHNIS

UNSER MEHRWERT FÜR SIE

In den vergangenen Jahren sind die Anforderungen an die IT- und OT-Abteilungen exponentiell gewachsen und im gleichen Maße überschneiden sich die Aufgaben immer mehr abteilungsübergreifend.

Erst mit einem genaueren Blick auf die Priorisierung innerhalb dieser Aufgaben wird klar, dass hier zum Teil entgegengesetzte Ansprüche aufeinandertreffen:

- Vertraulichkeit vs. Integrität vs. Verfügbarkeit vs. Safety?
- Welche Hardware erfüllt die speziellen Anforderungen einer Produktionsumgebung?
- Welche Aktionen müssen durchgeführt werden und welche dürfen keinesfalls automatisiert umgesetzt werden?
- Macht es tatsächlich Sinn, das Enterprise- und das Produktionsnetzwerk zentral zu verwalten und zu verantworten?
- Diese und viele weitere Fragen beantworten wir Ihnen mit jahrelanger Praxis-Erfahrung und erarbeiten mit Ihnen gemeinsam ein sicheres und verfügbares OT-Netzwerk, welches Ihre persönlichen, sowie die Anforderungen der IEC 62443 erfüllt und zur Steigerung Ihrer KPIs beiträgt.

NETZWERK INFRASTRUKTUR

- Netzwerk designen
- Netzwerk segmentieren
- Zonen und Verbindungen festlegen
- Geräte und Zugänge sichern
- Netzwerk dokumentieren

DATEN SAMMELN & VERWALTEN

- Daten sammeln (Syslog & Sensoren)
- Log-Daten filtern & verwalten
- Untersuchung, Analyse & Reporting

ASSESSMENTS NACH INTERNATIONALEN STANDARS

- Risiko Analysen
- Sicherheitsschwachstellen bewerten
- Best Practice- & Policy-Tests
- Unabhängige Bewertung

INTEGRITÄT SICHERSTELLEN

- In Echtzeit Änderungen feststellen
- Sicherheitslücken beheben
- softwarebasiertes Monitoring & Reporting
- Schulung und Sensibilisierung der Mitarbeiter

KRITISCHE INFRASTRUKTUREN (KRITIS)

Was ist KRITIS?

Kritische Infrastrukturen (KRITIS) sind die wichtigsten Versorgungs- und Sicherheitssysteme unserer Gesellschaft, die für das Funktionieren von Staat und Wirtschaft unerlässlich sind.

Hierzu gehören:

- Energieversorgung
- Wasserversorgung
- Gesundheitswesen
- Transport und Verkehr
- Finanzen und Versicherungen
- Ernährung
- Entsorgung
- Informations- und Kommunikationstechnologie (IKT)

Warum ist es wichtig?

Die KRITIS-Verordnung verpflichtet Unternehmen in diesen Sektoren, robuste Cybersicherheitsmaßnahmen zu implementieren, um ihre Systeme vor Bedrohungen zu schützen. Die Sicherheit von OT-Netzwerken (Operational Technology) spielt hierbei eine zentrale Rolle, da sie die physischen Prozesse steuern, die für den Betrieb dieser kritischen Infrastrukturen verantwortlich sind. Angesichts der zunehmenden Komplexität und der Vernetzung dieser Systeme wird die Notwendigkeit, sie vor Cyber-Angriffen zu schützen, immer dringlicher.

Warum wir der richtige Partner sind:

Wir verstehen die Kritikalität Ihrer Systeme und die gravierenden Folgen von Ausfällen. Als erfahrener Partner bieten wir individuelle Lösungen, die auf Ihre spezifischen Anforderungen zugeschnitten sind. Mit einem schrittweisen Ansatz sichern wir Ihre OT-Umgebung, minimieren Risiken und garantieren maximale Sicherheit – ohne den laufenden Betrieb zu stören.

Warum KRITIS-Compliance für Ihr Unternehmen entscheidend ist:

- **Erhöhte Sicherheitsanforderungen:** Unternehmen, die unter die KRITIS-Verordnung fallen, stehen vor der Herausforderung, ihre IT- und OT-Netzwerke gegen eine Vielzahl von Bedrohungen zu schützen. Dies erfordert eine umfassende Sicherheitsstrategie, die sowohl präventive als auch reaktive Maßnahmen umfasst.
- **Rechtliche und regulatorische Verpflichtungen:** Die Nichteinhaltung der KRITIS-Anforderungen kann zu erheblichen rechtlichen Konsequenzen führen, einschließlich hoher Bußgelder und Schadenersatzforderungen. Darüber hinaus könnte das Vertrauen der Öffentlichkeit in Ihr Unternehmen geschädigt werden, was langfristige Auswirkungen auf Ihr Geschäft haben könnte.
- **Schutz der Gesellschaft:** Als Unternehmen, das eine kritische Infrastruktur betreibt, tragen Sie eine besondere Verantwortung. Der Schutz Ihrer Systeme trägt nicht nur zur Sicherheit Ihres Unternehmens bei, sondern auch zur Stabilität und Sicherheit der gesamten Gesellschaft. Ein erfolgreicher Angriff auf Ihre Systeme könnte schwerwiegende Folgen für die öffentliche Sicherheit und die wirtschaftliche Stabilität haben.

Hierzu gehören all unsere Leistungen auf den Folgeseiten

NIS-2 RICHTLINIE (NETWORK & INFORMATION SECURITY)

Was ist die NIS-2 Richtlinie?

Die NIS-2 Richtlinie (Network and Information Security) der Europäischen Union stellt eine bedeutende Verschärfung der bestehenden NIS-Verordnung dar und zielt darauf ab, die Cybersicherheit in essenziellen Sektoren zu stärken. Diese Richtlinie ist relevant für Unternehmen, die in folgenden Bereichen tätig sind:

- Energie
- Wasser und Abwasser
- Gesundheit
- Transport und Verkehr
- Staat
- Finanzen und Versicherungen
- Weltraum
- Ernährung
- Entsorgung
- Post/Kurier
- Verarbeitendes Gewerbe
- Digitale Dienste
- Forschung
- Informations- und Kommunikationstechnologie (IKT)

Sie legt strengere Anforderungen an die Cybersicherheitsmaßnahmen fest, die Unternehmen ergreifen müssen, um ihre Netzwerke vor Angriffen zu schützen.

Was bedeutet sie für Ihr Unternehmen?

Unternehmen, die OT-Netzwerke betreiben, stehen vor der Herausforderung, die neuen Anforderungen der NIS-2 Richtlinie zu erfüllen. Diese Netzwerke, die für die Steuerung und Überwachung physischer Prozesse in kritischen Infrastrukturen verantwortlich sind, sind zunehmend Ziel von Cyber-Angriffen. Die NIS-2 Richtlinie fordert nicht nur die Einführung technischer Maßnahmen, sondern auch die Implementierung von organisatorischen und prozessualen Sicherheitsmaßnahmen.

Warum wir der richtige Partner sind:

Wir kennen die hohen Anforderungen der NIS-2 Richtlinie und die Bedeutung von Ausfallsicherheit. Unsere maßgeschneiderten Lösungen sorgen dafür, dass Ihre OT-Systeme sicher und gesetzeskonform bleiben. Schritt für Schritt entwickeln wir eine stabile Sicherheitsstrategie, die Risiken minimiert und Ausfallzeiten vermeidet.

Warum NIS-2 Compliance für Ihr Unternehmen entscheidend ist:

- **Verpflichtende Sicherheitsmaßnahmen:** Die NIS-2 Richtlinie verpflichtet Unternehmen, ihre Cybersicherheitsstrategien umfassend zu überdenken und anzupassen. Dies umfasst die Implementierung von Sicherheitsmaßnahmen wie Intrusion Detection Systems, Firewalls und Network Access Control, um Bedrohungen frühzeitig zu erkennen und abzuwehren.
- **Erhöhte Haftung und Sanktionen:** Die Nichtbeachtung der NIS-2 Anforderungen kann zu erheblichen rechtlichen Konsequenzen führen, einschließlich finanzieller Sanktionen und Reputationsverlust. Unternehmen müssen daher sicherstellen, dass ihre Sicherheitsmaßnahmen den neuesten Standards entsprechen.
- **Schutz kritischer Systeme und Daten:** Die Sicherstellung der Kontinuität Ihrer betrieblichen Prozesse und der Schutz sensibler Daten sind zentrale Elemente der NIS-2 Richtlinie. Ein erfolgreicher Angriff könnte nicht nur finanzielle Schäden verursachen, sondern auch die öffentliche Sicherheit gefährden.

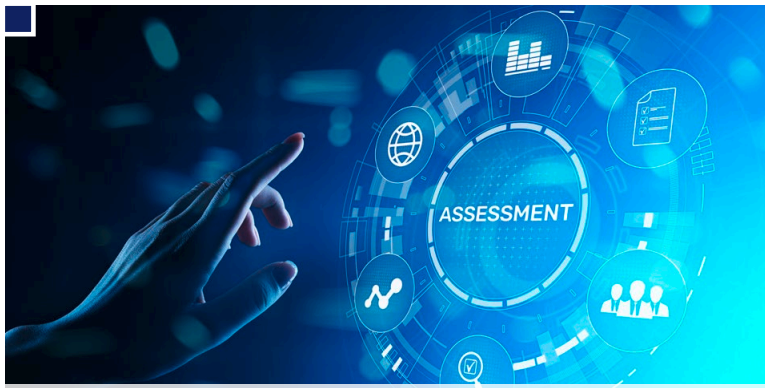
Hierzu gehören all unsere Leistungen auf den Folgeseiten

NETZWERKSTANDARDISIERUNG & SEGMENTIERUNG

Behalten Sie den Überblick über Ihre eingesetzte Hardware, ermöglichen Sie über die Bevorratung wichtiger Spare-Parts möglichst kurzfristige Reaktionszeiten und teilen Sie Ihr Produktionsnetzwerk in hochgradig sichere und autarke Zonen auf.

Unsere Lösungen zur Netzwerkstandardisierung und Segmentierung bieten Ihnen die Werkzeuge und Techniken, um Ihre Netzwerkinfrastruktur effizient zu verwalten und zu schützen. Entdecken Sie unsere spezialisierten Produkte und Dienstleistungen, die Ihnen helfen, Ihre Netzwerke optimal zu gestalten, Risiken zu minimieren und den Betrieb zu sichern. Erfahren Sie mehr über unsere innovativen Ansätze und lassen Sie sich von uns bei der Implementierung Ihrer individuellen Netzwerkstrategie unterstützen.

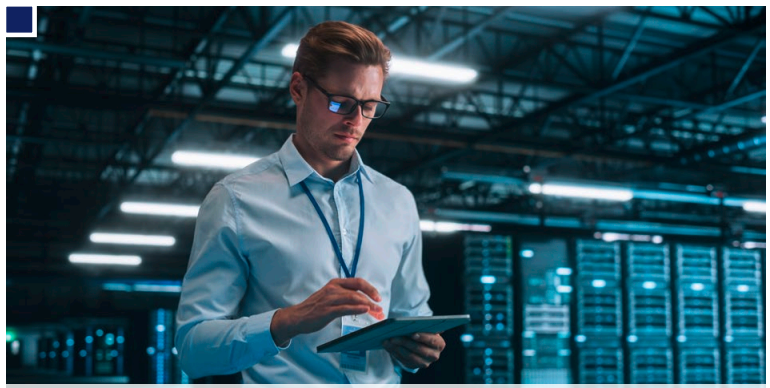
UNSERE LEISTUNGEN



OT Netzwerk Analyse

Risiko Analyse nach IEC 62443

OT Firewall Analyse



Switch Konfigurations Analyse

OT NETZWERK ANALYSE

Unsere OT Netzwerk Analyse bewertet Ihre bestehende Netzwerkinfrastruktur gemäß den aktuellen Sicherheitsstandards. Dies hilft Ihnen, Schwachstellen zu identifizieren und gezielte Verbesserungen vorzunehmen, um Ihre Netzwerksicherheit zu erhöhen.

WARUM EINE OT NETZWERK ANALYSE?

BESTANDSAUFNAHME DES OT NETZWERKS

Wir analysieren Ihr bestehendes OT Netzwerk, um eine umfassende Übersicht über Ihre Infrastruktur zu erstellen.

ÜBERPRÜFUNG NACH IEC 62443 STANDARDS

Unser Assessment folgt den internationalen Sicherheitsstandards der IEC 62443, um sicherzustellen, dass Ihr OT Netzwerk den höchsten Sicherheitsanforderungen entspricht.

ERSTELLUNG VON DOKUMENTATION UND NETZWERKPLAN

Basierend auf unseren Erkenntnissen erstellen wir eine detaillierte Dokumentation und Netzwerktopologie, die als Grundlage für weitere Sicherheitsmaßnahmen dient.

KUNDENBINDUNG

Eine proaktive Sicherheitsstrategie ermöglicht Ihnen, Störungen und Ausfälle zu vermeiden, was nicht nur die Produktivität steigert, sondern auch das Vertrauen Ihrer Kunden in Ihre Dienstleistungen stärkt.

UNSERE SERVICE

GRÜNDLICHE ANALYSE

Unsere Experten führen eine gründliche Analyse Ihres Netzwerks durch, um potenzielle Sicherheitsrisiken zu identifizieren.

DOKUMENTATION UND NETZWERKPLANUNG

Wir erstellen umfassende Dokumentationen und Netzwerkpläne, die Ihnen helfen, Ihre Infrastruktur besser zu verstehen und zu verwalten.

EMPFEHLUNGEN FÜR DIE OPTIMIERUNG IHRER OT-SECURITY

Basierend auf unseren Erkenntnissen geben wir Empfehlungen für die Optimierung Ihrer OT-Security, um die Sicherheit und Zuverlässigkeit Ihres Netzwerks zu erhöhen.

UNABHÄNGIGE BERATUNG

Bei uns erhalten Sie eine unabhängige Beratung, die sich ausschließlich auf Ihre Bedürfnisse konzentriert. Wir helfen Ihnen dabei, die Sicherheit Ihres Netzwerks zu verbessern, unabhängig von spezifischen Anbietern oder Lösungen.

IHR NUTZEN

SICHERHEITSKONFORMITÄT

Unser Assessment hilft Ihnen dabei, die Sicherheitsanforderungen nach internationalen Standards wie IEC 62443 zu erfüllen.

RISIKOMINDERUNG

Durch die Identifizierung und Behebung von Sicherheitsrisiken minimieren wir potenzielle Bedrohungen für Ihr Netzwerk.

VERBESSERTE NETZWERKPERFORMANCE

Eine gründliche Analyse und Dokumentation ermöglicht es Ihnen, Ihr Netzwerk effizienter zu verwalten und zu optimieren.

VERRINGERUNG VON AUSFÄLLEN UND DOWN TIME

Indem wir potenzielle Sicherheitslücken identifizieren und beheben, können wir Ausfallzeiten minimieren und die Verfügbarkeit Ihres OT-Netzwerks maximieren.

RISIKO ANALYSE NACH IEC 62443

Die Risiko Analyse nach IEC 62443 unterstützt Sie bei der Erkennung und Bewertung potenzieller Sicherheitsrisiken in Ihrem Netzwerk. Auf Basis dieser Analyse können Sie effektive Maßnahmen zur Risikominimierung und zur Erhöhung der Betriebssicherheit implementieren.

WARUM EINE RISIKO ANALYSE?

IDENTIFIZIERUNG VON SCHWACHSTELLEN

Unsere Analyse deckt potenzielle Schwachstellen in Ihrem OT-Netzwerk auf, die es Angreifern ermöglichen könnten, einzudringen und / oder Schaden anzurichten.

ERKENNUNG VON BEDROHUNGEN

Wir identifizieren und bewerten aktuelle und potenzielle Bedrohungen, die Ihr Netzwerk gefährden könnten, einschließlich Malware, Phishing-Angriffen und Insider-Bedrohungen.

BEWERTUNG DES RISIKOS

Basierend auf unseren Erkenntnissen bewerten wir das Risiko für Ihr OT-Netzwerk und helfen Ihnen dabei, Prioritäten zu setzen und geeignete Sicherheitsmaßnahmen zu ergreifen.

UNSERE DIENSTLEISTUNGEN

SCHWACHSTELLENANALYSE

Wir führen eine umfassende Analyse Ihres Netzwerks durch, um Schwachstellen in Ihrer Infrastruktur zu identifizieren und zu bewerten.

BEDROHUNGSIDENTIFIKATION

Unsere Experten erkennen Bedrohungen und Angriffsmuster, um potenzielle Angriffsvektoren zu verstehen und zu bekämpfen.

RISIKOBEWERTUNG

Wir bewerten das Risiko für Ihr Unternehmen und helfen Ihnen dabei, fundierte Entscheidungen über Sicherheitsinvestitionen und Maßnahmen zu treffen.

UNABHÄNGIGE BERATUNG

Wir bieten unabhängige Beratung, die sich ausschließlich auf Ihre Bedürfnisse konzentriert. Unser Ziel ist es, Ihnen dabei zu helfen, das Risiko für Ihr OT-Netzwerk zu minimieren und Ihre Sicherheitsstrategie zu optimieren.

IHR NUTZEN

RISIKOMINIMIERUNG

Durch die Identifizierung und Bewertung von Schwachstellen und Bedrohungen minimieren Sie das Risiko von Sicherheitsvorfällen und Datenverlust.

SCHUTZ VOR VERLUSTEN

Eine fundierte Risikoanalyse ermöglicht es Ihnen, potenzielle finanzielle Verluste durch Sicherheitsvorfälle zu vermeiden und Ihre Geschäftskontinuität zu sichern.

VERBESSERTE COMPLIANCE

Eine umfassende Risk & Threat Analyse hilft Ihnen dabei, die Einhaltung von Sicherheitsstandards und regulatorischen Anforderungen zu gewährleisten.

OT FIREWALL ANALYSE

Unsere OT Firewall Analyse prüft die Konfiguration und Effektivität Ihrer Firewall-Systeme. Dadurch stellen wir sicher, dass Ihre Netzwerksicherheit den höchsten Standards entspricht und unautorisierte Zugriffe verhindert werden.

WARUM EINE OT FIREWALL ANALYSE?

OPTIMIERUNG DER EFFEKTIVITÄT

Unsere Überprüfung stellt sicher, dass Ihre Firewall-Regeln effektiv sind und potenzielle Sicherheitslücken geschlossen werden.

ÜBERPRÜFUNG DES UMFANGS

Wir bewerten den Umfang Ihrer Firewall-Regeln, um sicherzustellen, dass sie angemessen konfiguriert sind und Ihren Sicherheitsanforderungen entsprechen.

UNSERE DIENSTLEISTUNGEN

BEWERTUNG DER FIREWALL-REGELN

Wir überprüfen und analysieren Ihre Firewall-Regeln, um sicherzustellen, dass sie den besten Schutz für Ihr Netzwerk bieten.

ÜBERPRÜFUNG DER COMPLIANCE

Wir stellen sicher, dass Ihre Firewall-Regeln den geltenden Sicherheitsstandards und Compliance-Anforderungen entsprechen.

OPTIMIERUNGSEMPFEHLUNGEN

Basierend auf unseren Erkenntnissen geben wir Empfehlungen zur Optimierung Ihrer Firewall-Regeln, um Sicherheitslücken zu schließen und die Effizienz zu steigern.

UNABHÄNGIGE BERATUNG

Unsere unabhängige Beratung konzentriert sich darauf, die Sicherheit und Effektivität Ihrer Firewall-Regeln zu verbessern, unabhängig von spezifischen Anbietern oder Lösungen.

IHR NUTZEN

ERHÖHTE NETZWERKSICHERHEIT

Durch die Optimierung Ihrer Firewall-Regeln minimieren Sie Sicherheitsrisiken und schützen Ihr Netzwerk vor potenziellen Angriffen.

COMPLIANCE-EINHALTUNG

Wir stellen sicher, dass Ihre Firewall-Regeln den geltenden Sicherheitsstandards und Compliance-Anforderungen entsprechen, um rechtliche Risiken zu minimieren.

VERBESSERTE LEISTUNG

Eine effektive Firewall-Konfiguration sorgt für eine optimale Netzwerkperformance, ohne die Sicherheit zu beeinträchtigen.

SWITCH KONFIGURATIONS ANALYSE

Die Switch Konfigurations Analyse sorgt dafür, dass Ihre Netzwerk-Switches optimal konfiguriert sind. Wir überprüfen und optimieren die Einstellungen, um die Performance und Sicherheit Ihrer Netzwerkinfrastruktur zu maximieren.

WARUM EINE SWITCH KONFIGURATIONS ANALYSE?

SCHWACHSTELLENIDENTIFIKATION

Unsere Analyse deckt potenzielle Schwachstellen in Ihrer Switch Konfiguration auf, die Sicherheitsrisiken für Ihr Netzwerk darstellen können.

OPTIMIERUNG DER KONFIGURATION

Wir helfen Ihnen dabei, Ihre Switch Konfiguration zu optimieren, um die Sicherheit zu verbessern und die Leistung zu maximieren.

UNSERE DIENSTLEISTUNGEN

SCHWACHSTELLENANALYSE

Wir untersuchen Ihre Switch Konfiguration gründlich, um Sicherheitslücken und potenzielle Angriffsvektoren zu identifizieren.

EMPFEHLUNGEN ZUR BEHEBUNG

Basierend auf unseren Erkenntnissen geben wir konkrete Empfehlungen zur Behebung von Schwachstellen und zur Verbesserung der Sicherheit Ihrer Switch Konfiguration.

PERFORMANCE-OPTIMIERUNG

Wir helfen Ihnen dabei, Ihre Switch Konfiguration zu optimieren, um die Leistung Ihres Netzwerks zu verbessern und Engpässe zu vermeiden.

UNABHÄNGIGE BERATUNG

Unsere unabhängige Beratung konzentriert sich darauf, die Sicherheit Ihrer Switch Konfiguration zu verbessern, unabhängig von spezifischen Anbietern oder Lösungen.

IHR NUTZEN

ERHÖHTE NETZWERKSICHERHEIT

Durch die Identifizierung und Behebung von Schwachstellen minimieren Sie das Risiko von Sicherheitsvorfällen und schützen Ihr Netzwerk vor potenziellen Angriffen.

VERBESSERTE NETZWERKPERFORMANCE

Eine optimierte Switch Konfiguration verbessert die Leistung Ihres Netzwerks und reduziert Engpässe, was zu einer besseren Benutzererfahrung führt.

COMPLIANCE-EINHALTUNG

Wir stellen sicher, dass Ihre Switch Konfiguration den geltenden Sicherheitsstandards und Compliance-Anforderungen entspricht, um rechtliche Risiken zu minimieren.

NETZWERKÜBERWACHUNG

Erstellen Sie einfach und unkompliziert eine aktuelle Asset-Übersicht, speichern einen Blueprint Ihrer gewünschten Netzwerkstruktur und erhalten Sie intelligent priorisierte und zusammengefasste Handlungsempfehlungen von unseren Tools, um Ihr Netzwerk stetig zu verbessern.

Unsere umfassenden Netzwerküberwachungslösungen bieten Ihnen Echtzeit-Einblicke in den Zustand und die Performance Ihrer gesamten IT- und OT-Infrastruktur. Durch kontinuierliche Überwachung und Analyse erkennen Sie potenzielle Probleme frühzeitig und können proaktiv Maßnahmen ergreifen, um Ausfälle zu verhindern und die Betriebssicherheit zu erhöhen. Nutzen Sie unsere fortschrittlichen Überwachungstools und Services, um eine robuste und effiziente Netzwerkumgebung zu gewährleisten, die den höchsten Sicherheits- und Leistungsstandards entspricht.

UNSERE LEISTUNGEN

Intrusion Detection System (IDS)

Management Security Dashboard

IoT Honeypot

Industrial Firewall

Network Access Control (NAC)

Industrial Remote Access

INTRUSION DETECTION SYSTEM (IDS)

Unser Intrusion Detection System (IDS) überwacht Ihr Netzwerk kontinuierlich auf verdächtige Aktivitäten und potenzielle Sicherheitsverletzungen. Es alarmiert Sie in Echtzeit, sodass Sie sofortige Maßnahmen ergreifen können, um Bedrohungen zu neutralisieren.

WARUM EIN INTRUSION DETECTION SYSTEM (IDS)?

FRÜHERKENNUNG VON ANGRIFFEN

Ein IDS ermöglicht es, verdächtiges Verhalten in Echtzeit zu erkennen und darauf zu reagieren, bevor Schaden entsteht.

SCHUTZ VOR DATENVERLUST

Durch die Überwachung des Netzwerkverkehrs können sensible Daten vor unbefugtem Zugriff geschützt werden.

EINHALTUNG VON SICHERHEITSSTANDARDS

Ein IDS hilft Unternehmen dabei, branchenspezifische Sicherheitsstandards einzuhalten und Compliance-Anforderungen zu erfüllen.

UNSER SERVICE

ANALYSE DER KUNDENANFORDERUNGEN

Wir verstehen die einzigartigen Bedürfnisse der OT-Umgebung jedes Kunden und entwickeln maßgeschneiderte Lösungen.

AUSWAHL DER PASSENDEN IDS-LÖSUNG

Basierend auf einer gründlichen Analyse empfehlen wir die geeignete IDS-Software, die Ihren Anforderungen entspricht.

IMPLEMENTIERUNG UND KONFIGURATION

Unsere Experten unterstützen Sie bei der nahtlosen Integration des IDS in Ihre bestehende Infrastruktur und passen es Ihren Bedürfnissen an.

SCHULUNG UND TECHNISCHER SUPPORT

Wir bieten umfassende Schulungen für Ihr Team und kontinuierlichen technischen Support, damit Ihre Fernwartungslösung effizient genutzt wird und Ihre Anforderungen stets erfüllt.

UNABHÄNGIGE BERATUNG

Unsere Beratung konzentriert sich ausschließlich auf Ihre Bedürfnisse, unabhängig von spezifischen Anbietern, um die beste Lösung für Sie zu finden.

IHR NUTZEN

AUSWAHL AUS EINER VIELZAHL VON ANBIETERN

Wir arbeiten mit einer Vielzahl von IDS-Anbietern zusammen, um sicherzustellen, dass Sie die bestmögliche Lösung erhalten.

MASSGESCHNEIDERTE LÖSUNGEN

Wir entwickeln Lösungen, die speziell auf Ihre Anforderungen zugeschnitten sind und bieten keine Einheitslösungen an.

OBJEKTIVE EMPFEHLUNG

Unsere Beratung basiert auf objektiven Kriterien und zielt darauf ab, die langfristige Sicherheit und Effizienz Ihres Netzwerks zu gewährleisten.

MANAGEMENT SECURITY DASHBOARD

Das Management Security Dashboard bietet Ihnen eine zentrale Übersicht über alle sicherheitsrelevanten Ereignisse und Zustände in Ihrem Netzwerk. Es stellt Ihnen klare und verständliche Signale zur Verfügung, damit Sie fundierte Entscheidungen zur Verbesserung Ihrer Netzwerksicherheit treffen können.

WARUM EIN MANAGEMENT SECURITY DASHBOARD?

ÜBERSICHTLICHE DARSTELLUNG

Unsere Dashboard-Lösung bietet eine übersichtliche und intuitive Darstellung aller produktionsrelevanten und Cybersicherheitsrelevanten Kennzahlen.

ECHTZEITDATEN

Mit Echtzeitdaten haben Sie jederzeit einen aktuellen Überblick über den Status Ihrer Produktion und die Sicherheit Ihres Netzwerks.

INFORMATIONSGRUNDLAGE FÜR ENTSCHEIDUNGEN

Unser Dashboard liefert Ihnen die notwendigen Informationen, um fundierte Entscheidungen zur Optimierung Ihrer Produktion und zur Verbesserung Ihrer Cybersicherheit zu treffen.

UNSER SERVICE

PRODUKTIONSKENNZAHLEN

Visualisierung von Produktionsdaten wie Maschinenauslastung, Ausfallzeiten, Produktionsfortschritt usw.

CYBERSECURITY-KENNZAHLEN

Darstellung von Cybersecurity-Kennzahlen wie Angriffshäufigkeit, Sicherheitsereignisse, Compliance-Status usw.

BENUTZERDEFINIERTE DASHBOARDS

Anpassbare Dashboards, die es Ihnen ermöglichen, die für Sie relevanten Kennzahlen und Metriken zu verfolgen.

ALARMFUNKTIONEN

Unsere Beratung konzentriert sich ausschließlich auf Ihre Bedürfnisse, unabhängig von spezifischen Anbietern, um die beste Lösung für Sie zu finden.

IHR NUTZEN

EFFIZIENZSTEIGERUNG

Durch die übersichtliche Darstellung aller relevanten Kennzahlen können Sie Ihre Produktionsprozesse optimieren und Engpässe identifizieren.

VERBESSERTE SICHERHEIT

Unser Dashboard ermöglicht es Ihnen, Sicherheitsrisiken frühzeitig zu erkennen und geeignete Maßnahmen zu ergreifen, um Ihr Netzwerk zu schützen.

ENTSCHEIDUNGSUNTERSTÜTZUNG

Mit Echtzeitdaten und aussagekräftigen Visualisierungen treffen Sie fundierte Entscheidungen, um Ihr Unternehmen voranzubringen.

IoT HONEYPOT

Unser IoT Honeypot ist eine strategisch platzierte Falle für Cyberkriminelle, die versuchen, unautorisiert in Ihr Netzwerk einzudringen. Es hilft Ihnen, Angreifer zu identifizieren und wertvolle Informationen über deren Methoden zu sammeln, um Ihre Sicherheitsmaßnahmen zu verstärken.

WARUM EIN IoT HONEYPOT?

ANGREIFER TÄUSCHEN

Mit einem Honeypot können Sie Angreifer in die Irre führen, indem Sie eine offensichtliche Schwachstelle simulieren, die keine produktiven Daten enthält.

FRÜHERKENNUNG VON ANGRIFFEN

Durch die Alarmierung bei unerlaubtem Zugriff erhalten Sie frühzeitig Hinweise auf potenzielle Angriffe und können entsprechend reagieren.

SCHUTZ DES HAUPTNETZWERKS

Indem Sie Angreifer von Ihrem Hauptnetzwerk fernhalten, können Sie die Sicherheit Ihrer produktiven Systeme gewährleisten.

UNSER SERVICE

KONFIGURATION EINER OFFENSICHTLICHEN SCHWACHSTELLE

Wir konfigurieren einen Honeypot als eine gezielte Schwachstelle, um potenzielle Angreifer anzulocken.

ECHTZEIT-ALARMIERUNG

Bei unerlaubtem Zugriff auf den Honeypot werden sofort Alarme ausgelöst, um Sie über potenzielle Bedrohungen zu informieren.

NACHVERFOLGUNG VON ANGRIFFSMUSTERN

Wir analysieren die Angriffsdaten, um Angriffsmuster zu erkennen und geeignete Gegenmaßnahmen zu ergreifen.

INTEGRATION IN BESTEHENDE SICHERHEITSINFRASTRUKTUR

Unsere Honeypot-Lösung lässt sich nahtlos in Ihre bestehende Sicherheitsinfrastruktur integrieren und ergänzt Ihre vorhandenen Schutzmechanismen.

IHR NUTZEN

FRÜHERKENNUNG VON BEDROHUNGEN

Durch die frühzeitige Erkennung von Angriffen können Sie schnell reagieren und potenzielle Schäden minimieren.

VERBESSERTE SICHERHEIT

Ein Honeypot ergänzt Ihre bestehenden Sicherheitsmaßnahmen und erhöht die Resilienz Ihres Netzwerks gegenüber Angriffen.

REDUZIERUNG VON RISIKEN

Indem Sie Angreifer von Ihren produktiven Systemen fernhalten, reduzieren Sie das Risiko von Datenverlust und Betriebsunterbrechungen.

INDUSTRIAL FIREWALL

Die Industrial Firewall schützt Ihre Betriebstechnologie vor unautorisierten Zugriffen und Angriffen. Durch die Implementierung spezifischer Regeln und Filter stellt sie sicher, dass nur berechtigte Datenverkehrsströme zugelassen werden, was die Sicherheit und Integrität Ihres Netzwerks erhöht.

WARUM EINE INDUSTRIAL FIREWALL

SCHUTZ VOR CYBERANGRIFFEN

Eine Industrial Firewall bietet umfassenden Schutz vor unbefugtem Zugriff und gezielten Angriffen auf Ihre Betriebstechnologie. Sie filtert den Netzwerkverkehr und blockiert schädliche Datenpakete, bevor sie Ihr System erreichen können.

SICHERUNG DER BETRIEBSPROZESSE

Durch die Trennung und Überwachung von Netzwerkschnittstellen gewährleistet eine Industrial Firewall, dass Ihre kritischen Betriebsprozesse sicher und störungsfrei ablaufen.

EINHALTUNG VON SICHERHEITSRICHTLINIEN

Mit einer Industrial Firewall können Unternehmen branchenspezifische Sicherheitsstandards einhalten und Compliance-Anforderungen erfüllen, um sicherzustellen, dass Ihre OT-Infrastruktur geschützt ist.

UNSER SERVICE

ANALYSE DER KUNDENANFORDERUNGEN

Wir verstehen die spezifischen Bedürfnisse Ihrer OT-Umgebung und entwickeln maßgeschneiderte Firewall-Lösungen, die perfekt zu Ihren Anforderungen passen.

AUSWAHL DER PASSENDEN INDUSTRIAL FIREWALL

Basierend auf einer gründlichen Analyse empfehlen wir die geeignete Firewall-Technologie, die Ihren Sicherheitsanforderungen entspricht und Ihre Netzwerkinfrastruktur optimal schützt.

IMPLEMENTIERUNG UND KONFIGURATION

Unsere Experten unterstützen Sie bei der nahtlosen Integration der Industrial Firewall in Ihre bestehende Infrastruktur und passen die Konfiguration an Ihre individuellen Bedürfnisse an.

SCHULUNG UND SUPPORT

Wir bieten umfassende Schulungen für Ihr Team an und stehen Ihnen mit technischem Support zur Seite, um sicherzustellen, dass Ihre Industrial Firewall optimal genutzt wird und Ihre Sicherheitsanforderungen erfüllt.

UNABHÄNGIGE BERATUNG

Bei uns erhalten Sie eine unabhängige Beratung, die sich ausschließlich auf Ihre Bedürfnisse konzentriert. Wir sind nicht an bestimmte Anbieter gebunden und suchen stattdessen die beste Lösung für Sie aus.

IHR NUTZEN

AUSWAHL AUS EINER VIELZAHL VON ANBIETERN

Wir arbeiten mit einer Vielzahl von Industrial Firewall Anbietern zusammen, um sicherzustellen, dass Sie die bestmögliche Lösung erhalten, die Ihren spezifischen Anforderungen entspricht.

MASSGESCHNEIDERTE LÖSUNGEN

Wir entwickeln Lösungen, die speziell auf Ihre Anforderungen zugeschnitten sind, und bieten keine Einheitslösungen an. Jede Firewall-Lösung wird individuell an Ihre Sicherheitsbedürfnisse angepasst.

OBJEKTIVE EMPFEHLUNGEN

Unsere Beratung basiert auf objektiven Kriterien und zielt darauf ab, die langfristige Sicherheit und Effizienz Ihres Netzwerks zu gewährleisten. Wir empfehlen Ihnen die besten Technologien und Strategien, um Ihre OT-Infrastruktur zu schützen.

NETWORK ACCESS CONTROL (NAC)

Mit Network Access Control (NAC) ermöglichen wir Ihnen die Kontrolle und Überwachung aller Netzwerkzugriffe. Diese Lösung hilft Ihnen, den Zugang zu Ihrem Netzwerk strikt zu regulieren und unautorisierte Geräte auszuschließen.

WARUM EINE NETWORK ACCESS CONTROL (NAC) LÖSUNG?

SCHUTZ VOR UNAUTORISIERTEM ZUGRIFF

Unsere NAC-Lösung verhindert unautorisierten Zugriff auf Endpunkte und schützt Ihr Netzwerk vor potenziellen Bedrohungen.

STRENGERE ZUGANGSKONTROLLE

Durch die Implementierung einer strengen Zugangskontrolle können Sie sicherstellen, dass nur autorisierte Benutzer und Geräte auf Ihr Netzwerk zugreifen können.

SICHERUNG SENSIBLER DATEN

Indem Sie unautorisierte Zugriffe auf Endpunkte verhindern, schützen Sie sensible Unternehmensdaten vor unbefugtem Zugriff und Datenverlust.

FUNKTIONEN

ENDPUNKTIDENTIFIKATION

Unsere NAC-Lösung identifiziert alle Endpunkte, die versuchen, auf Ihr Netzwerk zuzugreifen, und überprüft ihre Autorisierung.

RICHTLINIENBASIERTE ZUGANGSKONTROLLE

Wir implementieren richtlinienbasierte Zugangskontrollen, um sicherzustellen, dass nur autorisierte Benutzer und Geräte auf Ihr Netzwerk zugreifen können.

GASTZUGANGSKONTROLLE

Wir ermöglichen Ihnen die sichere Bereitstellung von Gastzugängen, während gleichzeitig die Sicherheit Ihres Netzwerks gewährleistet wird.

ECHTZEIT-ÜBERWACHUNG

Unsere NAC-Lösung überwacht kontinuierlich den Netzwerkzugriff und reagiert sofort auf unautorisierte Zugriffsversuche.

IHR NUTZEN

ERHÖHTE SICHERHEIT

Unsere NAC-Lösung stärkt die Sicherheit Ihres Netzwerks, indem sie unautorisierte Zugriffe auf Endpunkte verhindert und sensible Daten schützt.

VERBESSERTE COMPLIANCE

Durch die Implementierung strenger Zugangskontrollen können Sie die Einhaltung von Sicherheitsstandards und regulatorischen Anforderungen sicherstellen.

REDUZIERUNG VON SICHERHEITSRISIKEN

Indem Sie den Zugriff auf Ihr Netzwerk kontrollieren, reduzieren Sie das Risiko von Sicherheitsvorfällen und Datenverlust.

INDUSTRIAL REMOTE ACCESS

Unsere OT Fernwartungslösungen bieten sichere und zuverlässige Möglichkeiten zur Fernüberwachung und -wartung Ihrer Betriebstechnologie. Dies gewährleistet eine schnelle Problemlösung und reduziert Ausfallzeiten in Ihrer Produktion.

WARUM OT FERNWARTUNG

SCHNELLE PROBLEMLÖSUNG

Industrielle Fernwartung ermöglicht es Technikern, auf Ihre Systeme zuzugreifen und Probleme sofort zu diagnostizieren und zu beheben, ohne vor Ort sein zu müssen. Dies reduziert Ausfallzeiten erheblich.

KOSTENEFFIZIENZ

Durch den Fernzugriff entfallen Reisekosten und der damit verbundene Zeitaufwand. So können Wartungsarbeiten effizienter und kostengünstiger durchgeführt werden.

SICHERER ZUGRIFF

Unsere OT Fernwartungslösungen bieten verschlüsselte Verbindungen und strikte Zugriffskontrollen, um sicherzustellen, dass nur autorisierte Personen auf Ihre Systeme zugreifen können.

UNSER SERVICE

BEDARFSGERECHTE ANALYSE

Wir verstehen die speziellen Anforderungen Ihrer OT-Umgebung und entwickeln maßgeschneiderte Fernwartungslösungen, die exakt zu Ihren Bedürfnissen passen.

INDIVIDUELLE LÖSUNGSAUSWAHL

Basierend auf einer detaillierten Analyse empfehlen wir die passenden Fernwartungstools und -technologien, die optimal zu Ihrer Infrastruktur und Ihren Anforderungen passen.

NAHTLOSE INTEGRATION UND EINRICHTUNG

Unsere Experten helfen Ihnen bei der Implementierung und Konfiguration der Fernwartungslösung in Ihre bestehende Infrastruktur, um einen reibungslosen Betrieb sicherzustellen.

SCHULUNG UND TECHNISCHER SUPPORT

Wir bieten umfassende Schulungen für Ihr Team und kontinuierlichen technischen Support, damit Ihre Fernwartungslösung effizient genutzt wird und Ihre Anforderungen stets erfüllt.

UNABHÄNGIGE BERATUNG

Unsere Beratung konzentriert sich ausschließlich auf Ihre Bedürfnisse, unabhängig von spezifischen Anbietern, um die beste Lösung für Sie zu finden.

IHR NUTZEN

VIELFALT DER ANBIETER

Wir arbeiten mit zahlreichen OT Fernwartungsanbietern zusammen, um sicherzustellen, dass Sie die optimale Lösung für Ihre speziellen Anforderungen erhalten.

INDIVIDUELL ANGEPASSTE LÖSUNGEN

Jede Fernwartungslösung wird speziell auf Ihre Bedürfnisse zugeschnitten und nicht als Einheitslösung angeboten.

OBJEKTIVE EMPFEHLUNGEN

Unsere Empfehlungen basieren auf objektiven Kriterien und zielen darauf ab, die langfristige Effizienz und Sicherheit Ihrer OT-Infrastruktur zu gewährleisten.

SERVICE LEVEL AGREEMENTS

Ihre Techniker können die Funktion und den Support Ihres Produktionsnetzwerks nicht permanent garantieren? Kein Problem, denn wir unterstützen Sie 24/7 telefonisch, per Mail und persönlich vor Ort. Darüber hinaus ermöglichen Mitarbeiterschulungen „on the Job“, kombiniert mit einer ausführlichen Dokumentation, Reaktionszeiten von wenigen Minuten im Service-Fall.

Unsere Service Level Agreements (SLAs) stellen sicher, dass Sie rund um die Uhr auf erstklassigen Support zählen können, insbesondere bei einem Cyber Security Vorfall oder dem unvorhergesehenen Versagen Ihres Produktionsnetzwerks. Wir bieten maßgeschneiderte SLA-Pakete, die genau auf Ihre Bedürfnisse und Anforderungen abgestimmt sind. Ob präventive Wartung, proaktive Überwachung oder schnelle Fehlerbehebung – unser Team steht Ihnen jederzeit zur Verfügung, um einen reibungslosen Betrieb Ihrer Netzwerkinfrastruktur zu gewährleisten.

Im Falle eines Cyber Security Vorfalls oder eines unvorhergesehenen Netzwerkversagens ist es für uns von höchster Priorität, dass Ihre Produktion so schnell wie möglich wieder läuft, damit Sie keinen großen Schaden davontragen. Mit unseren SLAs profitieren Sie von garantierten Reaktions- und Lösungszeiten, sodass technische Probleme schnell und effizient behoben werden. Unsere Experten sorgen dafür, dass Ihre Systeme rasch wiederhergestellt und gesichert werden, sodass Ihre Produktionsprozesse nicht unterbrochen werden. Vertrauen Sie auf unsere umfassenden Serviceleistungen und genießen Sie die Sicherheit, dass Ihr Netzwerk in den besten Händen ist.

KONTAKT

UMER BHATTI

Business Development Manager OT-Security
(TÜV cert. Information Security Officer)

+49 151 27648814
bhatti@sud-gmbh.de

PATRICK POBERITZ

Head of Business Development & Marketing

+49 151 27648842
poberitz@sud-gmbh.de

https://sud-gmbh.de/industrial-cyber-security

SERVICE & DISTRIBUTION GmbH
INDUSTRIEAUTOMATISIERUNG

S&D Service & Distribution GmbH
Bischofstraße 113, 47809 Krefeld
Carl-Zeiss-Str. 8, 72124 Pliezhausen
Fuggerstraße 1b, 04158 Leipzig

+49 2151 4576-600
+49 2151 4576-777
info@sud-gmbh.de
www.sud-gmbh.de

Value-Add Distributor
A ROCKWELL AUTOMATION PARTNER