WIRELESS LOGIC **IOT SICHEREHEIT**

wireless logic mdex GmbH

Anomalie-Erkennung

Bedrohungsmanagement für IoT-Geräte

Anomalie-Erkennung ist eine Lösung von Wireless Logic, die den Nutzen und die Auslastung von IoT-Geräten maximieren und gleichzeitig die IT-Infrastruktur des Unternehmens vor externen Bedrohungen schützt.

IoT-Geräte werden typischerweise in Umgebungen außerhalb der klassischen Unternehmens-IT eingesetzt – und das in großer Zahl. Es macht sie anfälliger für Cyberkriminalität und schwieriger zu überwachen und zu verwalten.

Die Anomalie-Erkennung von Wireless Logic nutzt künstliche Intelligenz, um Kommunikationsmuster von IoT-Geräten kontinuierlich zu überwachen. So können Unternehmen frühzeitig Hinweise auf betriebliche oder sicherheitsrelevante Probleme in umfangreichen IoT-Installationen erkennen. Werden solche Probleme nicht erkannt, kann das zu anhaltenden betrieblichen Störungen, Sicherheitsverletzungen, Reputationsschäden, Umsatzeinbußen oder finanziellen Sanktionen in Form von Geldstrafen durch Aufsichtsbehörden führen.

Die Vorteile der Anomalie-Erkennung ...

Intelligenz und Bedrohungsmanagement für IoT-Geräte

Unsere Anomalie-Erkennung identifiziert die ersten Anzeichen unerwarteter Kommunikationsprobleme von IoT-Geräten, die durch Fehlfunktionen oder Cyber-bedrohungen verursacht werden. Solche Probleme können sich auf unterschiedliche Weise äußern, darunter:

- Veränderung der Kommunikationsfrequenz
- Kein Datenverbrauch
- Ungewöhnliche Downloads
- Übermäßig hohes Datenvolumen
- Kommunikation mit unbekannten oder ungewöhnlichen Server-Endpunkten

Auswirkung der Nichterkennung

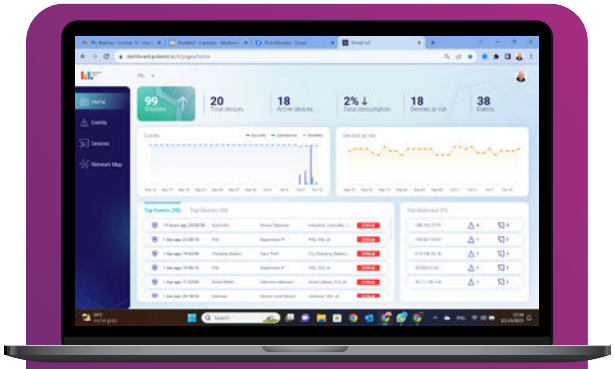
Finanzielle Verluste
Sicherheitsverletzungen kosten Geld. Es kann notwendig sein, die Ursache zu untersuchen, Systeme wiederherzustellen, neue Sicherheits-maßnahmen zu implementieren, Bußgelder oder Lösegeld zu zahlen und externe Experten hinzuzuziehen.

Reputationsschäden
Sicherheitsvorfälle untergraben das Vertrauen. Kunden, Partner und andere Stakeholder verlieren Vertrauen in die Fähigkeit des Unternehmens, Informationen zu schützen – was zu Geschäfts-einbußen und Reputationsverlust führt.

Datendiebstahl
Die Offenlegung sensibler Daten bei einem Vorfall kann Identitätsdiebstahl, Betrug und Cyberkrimi-nalität zur Folge haben – mit weiteren finanziellen Schäden und rechtlichen Konsequenzen.

Betriebsunterbrechungen
Sicherheitsverletzungen können zu Ausfallzeiten führen, während Systeme überprüft, bereinigt und wiederhergestellt werden. Dies stört den regulären Geschäftsbetrieb und beeinträchtigt Produktivität sowie Umsatz.

Regulatorische Folgen
Unternehmen unterliegen strengen Datenschutzvorschriften. Ein Verstoß kann zu Nichteinhaltung führen – mit Geldbußen, Strafen und juristischen Konsequenzen.



So funktioniert es ...

Die Lösung erfordert keine Installation von Software auf den IoT-Geräten und beeinträchtigt weder den Datenschutz noch die Systemleistung.

Es werden lediglich die Paket-Header der Gerätekommunikation über Mobilfunk aus unserem Mobile Core gespiegelt und an unsere Engine zur Anomalie- und Bedrohungserkennung weitergeleitet. Dort erfolgt eine nahezu in Echtzeit arbeitende, KI-gestützte Analyse.

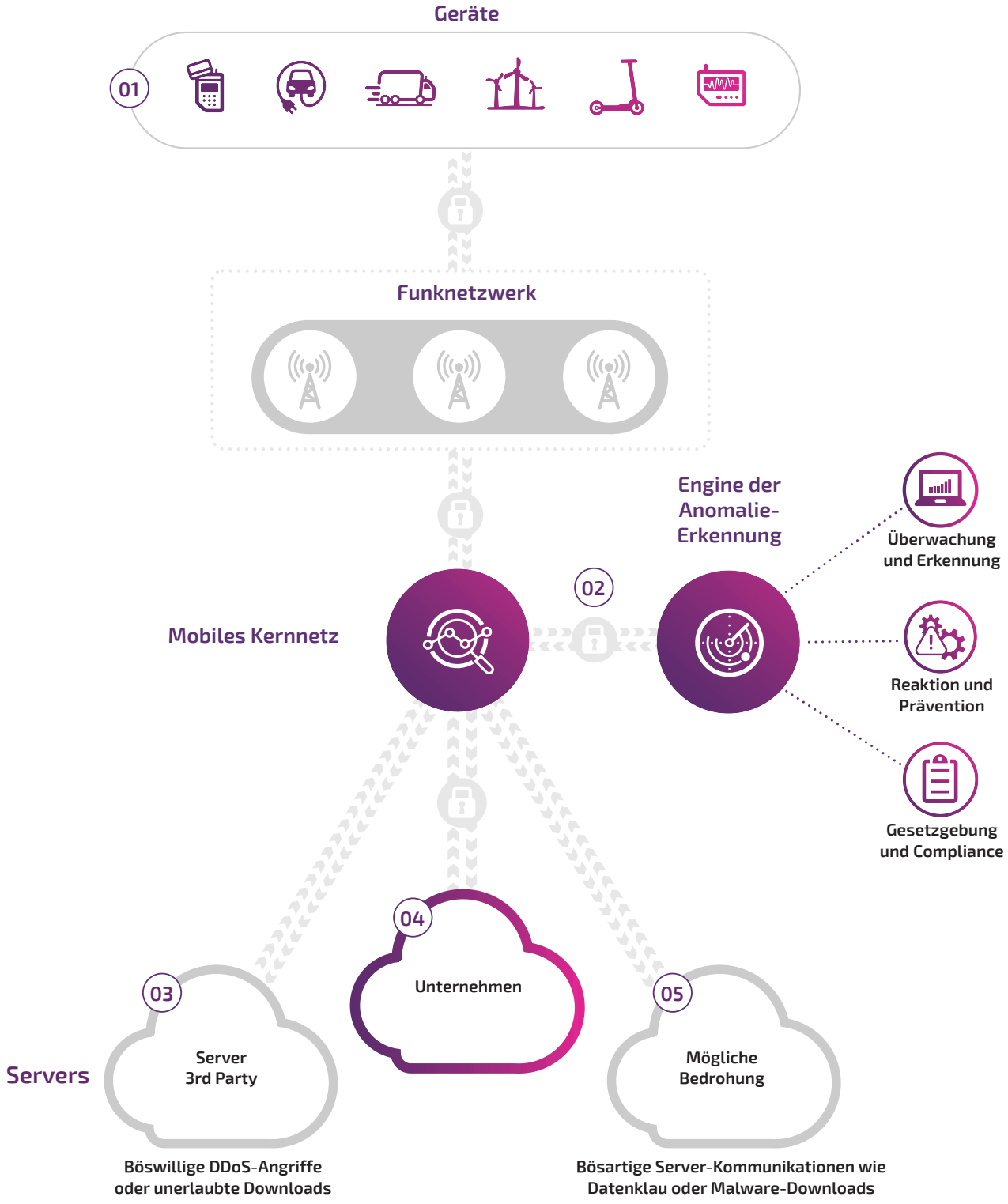
Erkenntnisse und Bedrohungsstufen werden über ein Kundenportal (UI) bereitgestellt, um Untersuchungen und Gegenmaßnahmen zu ermöglichen.

Erweiterte Servicefunktionen stehen ebenfalls zur Verfügung, unter anderem zur Unterstützung von:

- **Automatisierter Reaktion**
- **Bedrohungsprävention**
- **Einhaltung regulatorischer Vorgaben (Compliance)**

So funktioniert es ➤

Wie Anomalie-Erkennung funktioniert...



01 *Geräte können aufgrund von Fehlfunktionen oder Ransomware offline sein. Sie können von Cyberkriminellen übernommen und für DDoS-Angriffe missbraucht werden.*

02 *Die kontinuierliche Überwachung in unserem Mobilfunk-Kernnetz erkennt Datenstromanomalien und anderes ungewöhnliches Geräteverhalten.*

03 *Unbefugte Gerätenutzung oder kompromittierte Geräte können mit Drittanbieter-Servern kommunizieren oder diese angreifen.*

04 *Die IT-Abteilung des Unternehmens erkennt DDoS-Angriffe, die direkt auf sie abzielen – jedoch nicht den malwarebezogenen Datenverkehr oder Angriffe auf externe Server.*

05 *Infizierte Geräte kommunizieren in der Regel mit bösartigen Servern, um Malware herunterzuladen oder Daten zu stehlen.*

Überwachung und Erkennung

Erhalten Sie in Echtzeit Informationen zu Geräten und Bedrohungserkennung über das Kundenportal (UI).

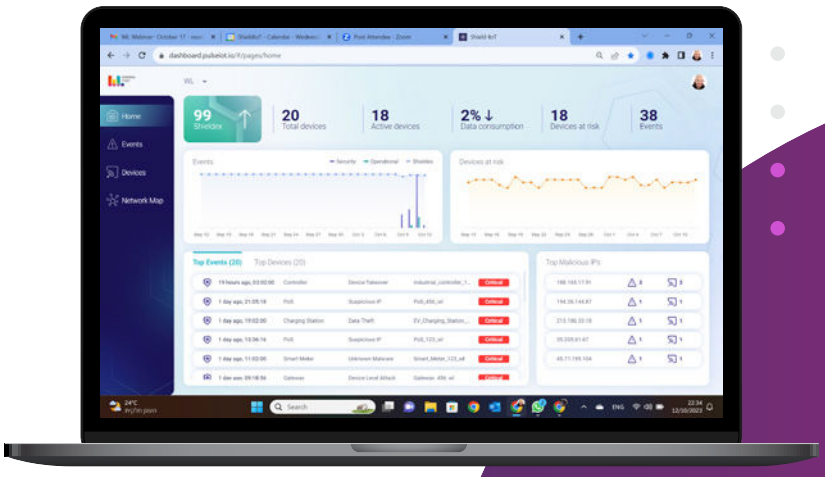
Reaktion und Prävention

Erweitern Sie Ihre Lösung um Funktionen für Bedrohungsmanagement und -prävention. Zusätzlich zum UI-Zugang umfasst dies Exportfunktionen zu Managementsystemen wie:

- Security Information and Event Management (SIEM)
- Connectivity Management Plattform (CMP)
- Servicedesks (Support-Ticketsysteme)
- E-Mail-Systeme

Regulatorik und Compliance

Erweitern Sie den Service um Funktionen, die Sie bei der Einhaltung von Cybersecurity- und Datenschutzvorgaben unterstützen. Dazu gehört der Zugang zur automatisierten Engine zur Erstellung von Compliance-Berichten. Diese stellt Nachweise für die kontinuierliche Überwachung des IoT-Netzwerks, die Reaktion auf Bedrohungen sowie die Weiterentwicklung der Sicherheitsmaßnahmen im Zeitverlauf bereit.



Zentrale Funktionen

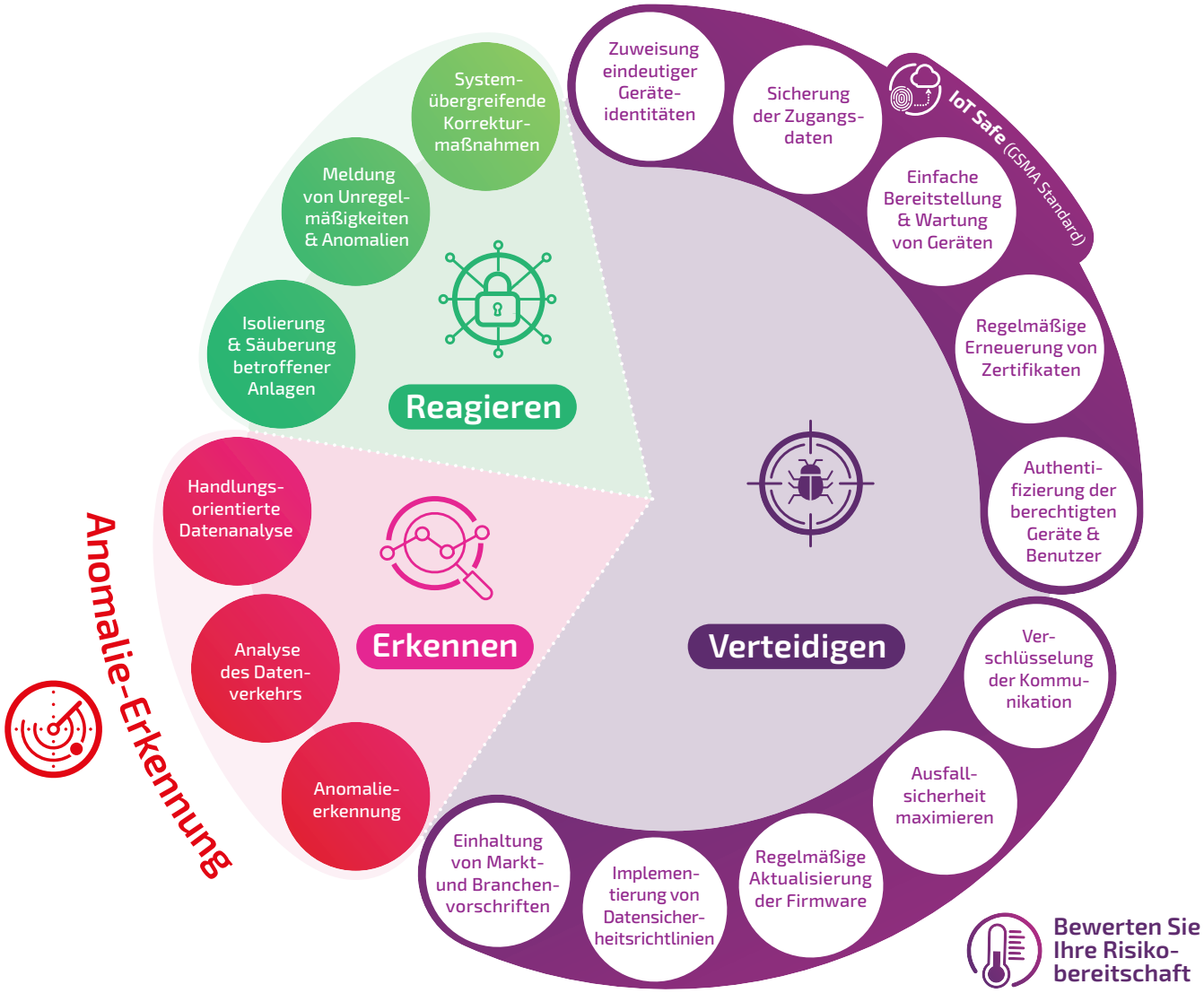
- Geräteübersicht
- Umsetzbare Gerätewarnungen
- Ereignisanalyse
- Netzwerkübersichten
- Mandantenfähigkeit
- Erkenntnisse & Empfehlungen
- API-Integration
- Compliance-Berichte

Mehr über IoT Sicherheit ...

Wireless Logic **IoT Security Framework**

IoT-Sicherheit ist ein fortlaufender Prozess, da ständig neue Bedrohungen auftauchen. Selbst Unternehmen, die bereits bewährte Cybersicherheitsmaßnahmen wie die Anomalie-Erkennung implementiert haben, müssen auf allen Ebenen Maßnahmen ergreifen, um ihre Netzwerke, Geräte, Daten und Anwendungen sicher zu halten.

Unsere IoT-Sicherheitsexperten haben ein Framework entwickelt, mit dem wir Unternehmen dabei unterstützen, ihr Risikopotenzial zu bewerten und eine Strategie zu entwickeln, die Reputation und Umsatz schützt. Das Framework umfasst 16 Maßnahmen, mit denen Unternehmen Schützen (Defend), Erkennen (Detect) und Reagieren (React) können – gegen Bedrohungen im Bereich der IoT-Cybersicherheit.



Für viele der 16 Maßnahmen gibt es technologische Lösungen, doch das Framework berücksichtigt auch Menschen, Prozesse und die Risikotoleranz eines Unternehmens. Das angemessene Sicherheitsniveau kann von verschiedenen Faktoren bestimmt werden – etwa durch die Anforderungen Ihrer Kunden, branchenspezifische Standards oder Ihre eigene Einschätzung akzeptabler Risiken. Dabei gilt es, einen Ausgleich zu finden zwischen Aspekten wie Kosten, Rechenressourcen oder Benutzerfreundlichkeit.

The **Wireless Logic IoT Security Stack**

Weltweiter 24/7-Betrieb

Unser globaler NOC/SOC-Service bietet eine durchgehende 24/7-Überwachung, Berichterstattung und Behebung von Betriebs- und Sicherheitsvorfällen.

Anwendungsentwicklung

Entwickeln und modellieren Sie Ihre Anwendungen mit einem Fokus auf Sicherheit – direkt ab der Planungsphase.

Anomalie-Erkennung

Überwachen Sie die Kommunikation zwischen Gerät und Cloud-Endpunkt und erkennen Sie Abweichungen vom Normalverhalten.

Gerätemanagement

DevicePro ermöglicht Lösungsanbietern, OEMs und Unternehmen die Echtzeitüberwachung und Fernverwaltung von Geräten und Hardware.

Sicheres privates Netzwerk

NetPro stellt ein sicheres und widerstandsfähiges privates Netzwerk bereit, das Unternehmen direkt mit ihren IoT-Geräten und -Diensten verbindet.

Konnektivitätsmanagement

SIMPro vereinfacht und automatisiert das Management von IoT-Konnektivität auf einer einzigen, sicheren Plattform – mit Zugriff über API oder Benutzeroberfläche.

Conexa

Unser speziell für IoT entwickeltes Mobilfunk-Kernnetzwerk ermöglicht die Echtzeitkontrolle und -überwachung des Verhaltens von IoT-Geräten.

Cloud Secure

Enthält IoT SAFE-Technologie zur sicheren Verwaltung von Geräteidentitäten und ermöglicht eine skalierbare, dynamisch abgesicherte IoT-Infrastruktur.

Kontaktieren Sie uns ...

Ihr Kontakt für IoT Projekte:

Tel: +49 (0)4109-555-444
E-Mail: vertrieb@mdex.de

Deutschland

Wireless Logic mdex GmbH
Bäckerbarg 6
22889 Tangstedt / Hamburg
+49 (0)4109-555-444
vertrieb@mdex.de

Unsere Niederlassungen:

China
Dänemark
Deutschland
Frankreich
Italien
Liechtenstein
Niederlande
Norwegen
Österreich
Spanien
USA

mdex.de

wireless logic mdex GmbH