

Network Intrusion Detection Sensor

Intrusion Detection abgestimmt auf kritische Infrastrukturen



Network Intrusion Detecton Sensor

Konzernübergreifend stehen Anlagenbetreiber durch alle Branchen hindurch zunehmend vor der Herausforderung, ihre technische IT- und Automatisierungsumgebung nachhaltig gegen interne wie externe Bedrohungen abzusichern.

Industrial Defender als führender Hersteller von IT-Security für kritische Infrastrukturen, bietet auf Basis einer konsequenten Defense-in-Depth™ Security-Strategie ein skalierbares Lösungskonzept an.

Der Industrial Defender Network Intrusion Detection Sensor (NIDS) ist ein Intrusion Detection System für technische IT- und Automatisierungsumgebungen in kritischen Infrastrukturen, das jeglichen Netzwerkverkehr innerhalb der Sicherheitsperimeter passiv überwacht, sowie die Erkennung von verdächtigen Aktivitäten und damit einhergehender, eingeschränkter Verfügbarkeit, ermöglicht. Dazu gehören sowohl die internen als auch alle externen Angriffe, die möglicherweise den Perimeterschutz durchbrechen würden. Im Gegensatz zu NIDS der Business-IT, kann die NIDS von Industrial Defender die De-facto-Protokolle überwachen, die von Prozessleitsystemen verwendet werden, wie beispielsweise Modbus TCP, DNP3, ODVA Ethernet/IP, ICCP, IEC 60870-5-104 und andere. Im Zusammenspiel mit der Industrial Defender Security Event Manager Konsole werden auftretende Security- und Verfügbarkeitsereignisse analysiert und protokolliert.

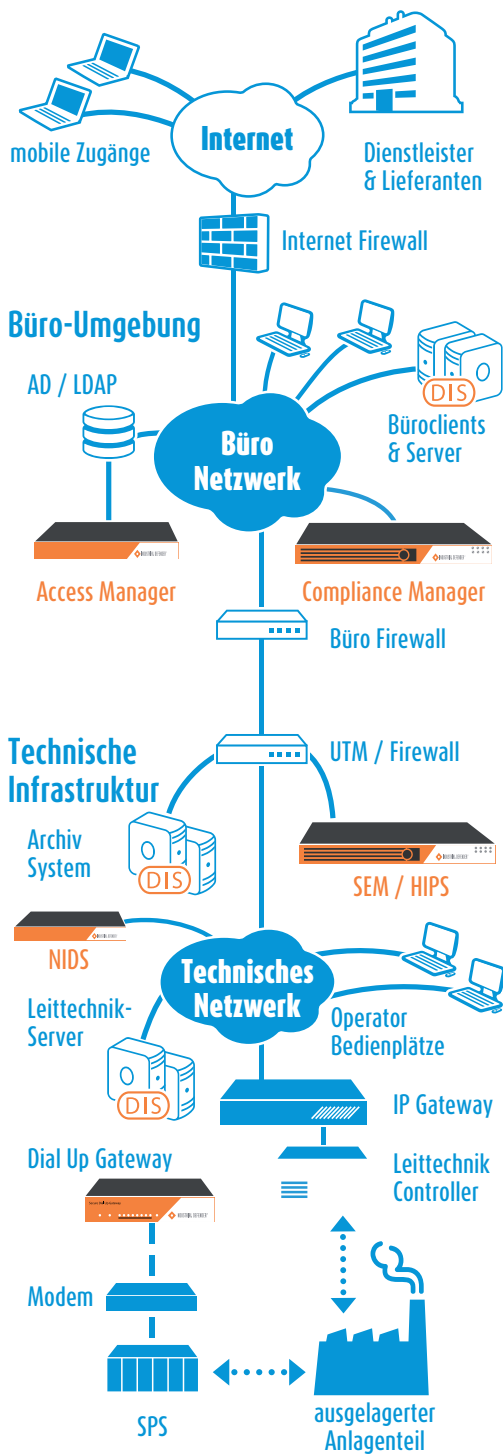
Notwendigkeit eines Intrusion Detection Systems

Obwohl ein starker Perimeterschutz entscheidend für die Absicherung der technischen Infrastruktur ist, zeigen Studien, dass bis zu 70% der Sicherheitsereignisse interne Vorfälle sind und unbeabsichtigt ausgelöst werden. Eine häufige, oft unterschätzte Bedrohung entsteht beispielsweise durch infizierte USB-Laufwerke oder Laptops von Servicetechnikern, die im direkten Kontakt mit leittechnischen Systemkomponenten stehen. Üblicherweise werden solche Sicherheit und Verfügbarkeit relevanten Ereignisse wenn überhaupt, nur als Performance-Einschränkung erkannt. Aufgrund fehlender Möglichkeiten innerhalb der leittechnischen Systeme, können Ursachen und Auswirkungen nur sehr schwer festgestellt werden. An diesem Punkt setzt die Industrial Defender NIDS Technologie an und hilft beim Schutz von leittechnischen Systemen gegen interne und externe Manipulation, indem sie unerlaubten Datenverkehr jeglicher Quellen (innerhalb der Netzwerkperimeter) registriert und meldetechnisch überwacht.

Funktionsweise

Die Industrial Defender NIDS Technologie arbeitet mit einer Bibliothek, die mehr als 2300 Signaturen enthält und ständig vom Industrial Defender Security Event Manager auf den neuesten Stand gebracht wird. Die Industrial Defender NIDS unterstützt die Sicherheits- und Verfügbarkeitsüberwachung in technischen IT-Infrastrukturen und ist unverzichtbar bei der Einhaltung von Normenanforderungen. Sicherheitsbedenken in kritischen Infrastrukturen haben sich lange nur auf den Schutz vor physischen Zugriffen beschränkt. Mit der zunehmenden Vernetzung im Bereich leittechnischer Systeme müssen Netzwerke auf Schadsoftware hin überwacht und geschützt werden. Industrial Defender implementiert speziell entwickelte Regeln auf den NIDS Sensoren zur Überwachung schädlicher Aktivitäten wie:

- Fehlerhafte Pakete während eines Buffer-Overflow-Angriffs
- Denial-of-Service-Angriffe, zum Schutz der leittechnischen Komponenten vor einer Endlosschleife
- Ständige Wiederholung von Paketen, was typisch für einen Replay-Angriff ist
- Erkennung unzulässiger Geräte im leittechnischen Netzwerk



Leittechnische Umgebungen können entweder durch schädliche Aktivitäten oder durch vernachlässigte Wartungsintervalle bzw. Konfigurationen beeinträchtigt werden. Die Industrial Defender NIDS hilft bei der Identifizierung möglicher Probleme mit Regeln zur Überwachung von Leistungskennwerten, wie beispielsweise:

- Auswertung über Logdaten zur Lokalisierung und Nachverfolgung von Protokollfehlern
- Identifikation unzulässiger Manipulationen an Automatisierungskomponenten (z.B. Resetbefehle)
- Fehlerhafte Konfiguration von Schnittstellen und Protokollen, falls diese nicht standardkonform genutzt werden

Normencompliance

Die Industrial Defender NIDS Technologie beinhaltet Regelwerke, die Unternehmen helfen, geforderte Branchenstandards einzuhalten. Die NIDS hilft bei der Erfüllung solcher Standards, indem sie gängige leittechnische Protokolle kontrolliert und bei unerlaubten Lese- und Schreibzugriffen, bei fehlgeschlagenen Logins und bei Nutzung von herstellerspezifischen Standardkennwörtern, Warnmeldungen auslöst.

Hardwareübersicht

Merkmale	NIDS 120	NIDS 1100
Maximale Durchsatzgeschwindigkeit	285 Mb/s	1 Gb/s
Arbeitsspeicher	2 GB	2 GB
Speicherkapazität	80 GB	250 GB
LAN Ports	4 x 10/100/1000 Mb	8 x 10/100/1000 Mb
Energieversorgung	230 V, 250 Watt	120 V, 450 Watt
Form Factor	Rack mount 1 HE	Rack mount 1 HE
Maße (BxHxT)	427 x 44 x 480 mm	427 x 44 x 480 mm
Gewicht	11,5 KG	13 KG

Umgebungsbedingungen

Betriebstemperatur 10°C bis 35°C; die maximale Änderungsrate darf 10°C pro Stunde nicht überschreiten.
Luftfeuchtigkeit von 90%, nicht kondensierend

Produktzertifizierungen
CE, FCC Class A, UL

KORAMIS GmbH

Kompetenzzentrum

Automatisierungstechnik & IT-Sicherheit

Neumühler Weg 32.1

D - 66130 Saarbrücken-Güdingen

Tel. +49 (0)681 - 968 191 - 30

Fax +49 (0)681 - 968 191 - 930

KORAMIS – Ihr Partner für IT-Security

Als innovatives Unternehmen adressiert KORAMIS seit 1985 die Prozess- und Versorgungsindustrie und bietet Lösungen und Tools im technischen Umfeld von kritischen Infrastrukturen an. Im Bereich IT-Security ist KORAMIS Partner von Industrial Defender und bietet von der Risiko-Analyse über Lösungsimplementierung bis zum Support komplette Sicherheitslösungen aus einer Hand.