OT Security Sensor Guardian™ by Nozomi Networks

OT Security Sensor für die Echtzeit-Überwachung industrieller Netzwerke

Der OT Security Sensor Guardian™ von Nozomi Networks ist eine umfassende, passive Sicherheitslösung für industrielle Netzwerke, die Echtzeit-Überwachung, Inventarisierung und Erkennung von Cyber-Bedrohungen, Schwachstellen und Anomalien ermöglicht.

Integration und Basis-Features

- ✓ Schnelle und störungsfreie Installation
- ✓ Nahtlose Integration in bestehende Sicherheitssysteme
- ✓ Selbstlernendes System zur Anpassung an Veränderungen in der Infrastruktur
- ✓ Bedrohungserkennung inklusive Ransomware, Malware und DDoS-Attacken
- ✓ Skalierbar für jede Unternehmensgröße und Anforderung
- ✓ Unterstützt Rugged Guardians für extreme Bedingungen und den Nozomi Arc Endpoint Sensor für erweiterte Asset-Überwachung

Protokollunterstützung

Guardian unterstützt eine umfassende Liste von OT/IoT- und IT-Protokollen und verbessert so die Sichtbarkeit und Sicherheitsüberwachung in verschiedenen industriellen Umgebungen. Dadurch wird die Integrität und Verfügbarkeit kritischer Prozesse gewährleistet und eine umfassende Netzwerktransparenz gefördert.

Erfüllung von Regulierungsstandards

Durch die Implementierung des Guardian-Sensors können Unternehmen die wesentlichen Anforderungen der NIS2-Richtlinie erfüllen, was zu einer verbesserten Sicherheit und Compliance führt.

IKARUS OT Security Professional Services

Die Kombination der IKARUS OT Security Professional Services mit Nozomi Networks Technologien bildet eine hervorragende Basis für den Auf- und Ausbau eines effektiven OT/IoT-Sicherheitsprogramms. Sie ermöglicht es, Cyber-Risiken zu minimieren, regulatorische Anforderungen zu erfüllen und die operative Resilienz zu erhöhen.

Typische Use Cases für den Einsatz von Guardians

» **Asset Management und Risikobewertung**: Vollständige Sichtbarkeit und Klassifizierung von Assets im Netzwerk, Bewertung von Schwachstellen und Bedrohungen.

» **Echtzeit-Erkennung von Schwachstellen**, Fehlkonfigurationen, Bedrohungen und Angriffen für eine schnelle Reaktion auf sicherheitsrelevante Vorfälle.

» **Netzwerksegmentierung und Zugriffskontrolle**: Unterstützung bei der Implementierung einer sicheren Netzwerkarchitektur durch die Identifizierung und Kontrolle von Netzwerkflüssen.

» **Compliance und Reporting**: Unterstützung bei der Einhaltung relevanter Sicherheitsstandards und -vorschriften, einschließlich Erstellung von Berichten und Audits.

IKARUS Security Software GmbH | Blechturmgasse 11 | 1050 Wien | Österreich | Tel.: +43 1 589 95-0
office@ikarus.at | Firmenbuchnummer: FN 64708i | Gerichtsstand Wien | UID-Nr.: ATU15191405

Ihr nächster Schritt zu mehr industrieller Sicherheit und Widerstandsfähigkeit:

Proof of Value (PoV)

Der Proof of Value (PoV) ermöglicht es Unternehmen, die Effektivität und den direkten Nutzen des OT Security Sensors in ihrer eigenen Netzwerkumgebung zu erleben. Er ist ein entscheidender Bestandteil im Prozess der Implementierung von Sicherheitslösungen, insbesondere im Bereich der Operational Technology (OT).

Während der PoV-Phase werden die Guardian-Sensoren und die zugehörigen Dienste in einer realen Umgebung eingesetzt, um realistische Einblicke in die aktuelle OT-Cyber-Security-Position, bestehende Risiken und die operative Resilienz des Unternehmens zu gewinnen. Ziel dieser Phase ist es, konkrete und messbare Ergebnisse zu liefern, die Entscheidungsträgern helfen, die Notwendigkeit und den Wert von Investitionen in fortschrittliche OT-Sicherheitsmaßnahmen zu verstehen.

Der PoV bietet eine solide Grundlage für fundierte Entscheidungen und erleichtert die strategische Planung von Sicherheitsinitiativen. Er schafft Transparenz über die Leistungsfähigkeit und den Einfluss der vorgeschlagenen Lösungen auf die Verbesserung der Cybersicherheitsposition.

Vorteile des PoV

- ✓ Automatisiertes Asset Discovery
- ✓ Sichtbarkeit der Assets und der Netzwerkkommunikation
- ✓ Echtzeiterkennung von Bedrohungen, Schwachstellen und Anomalien
- ✓ Interaktive Netzwerkvisualisierung
- ✓ Monitoring von betriebsrelevanten Prozessvariablen

Kontaktieren Sie uns:

+43 1 58995-500
sales@ikarus.at

OT Security Add-Ons und ergänzende Lösungen

Asset Intelligence

Asset Intellig ence von Nozomi Networks ist eine Schlüsselfunktion innerhalb der OT-Sicherheitslösungen, die es Unternehmen ermöglicht, einen vollständigen und kontinuierlichen Überblick über alle ihre OT- und IoT-Geräte zu erhalten. Das Feature liefert präzise Informationen über Gerätetypen, Hersteller, Verhaltensweisen, Einstellungen und die verwendeten Kommunikationsprotokolle.

Die Integration von Asset Intelligence in Ihr Sicherheitskonzept ermöglicht es, Cyber-Bedrohungen und betriebliche Anomalien schneller und effektiver zu identifizieren. Durch den kontinuierlichen Abgleich der Netzwerkaktivitäten mit einer umfangreichen Datenbank von Geräteprofilen und erlernten Basislinien kann das System falsche Alarme minimieren und den Fokus auf tatsächlich sicherheitsrelevante Ereignisse richten.

Smart Polling

Als innovatives Add-on des OT Security Sensors Guardian ermöglicht **Smart Polling** eine tiefgreifende und differenzierte Überwachung der Netzwerkinfrastruktur. Es erweitert die passive Überwachung d urch aktive Abfragen, um detaillierte Informationen über Betriebssysteme, Software, Firmware-Versionen und Patch-Level der Geräte zu sammeln.

Smart Polling ermöglicht es den Sicherheitsteams, Schwachstellen präzise zu bewerten und effektive Priorisierungsentscheidungen für das Patch-Management und andere Sicherheitsmaßnahmen zu treffen. Diese Funktion ist besonders wertvoll für Umgebungen, in denen vollständige Transparenz und aktuelle Informationen über den Zustand der Assets entscheidend sind, um die Sicherheit und Integrität des Netzwerks zu gewährleisten.

Threat Intelligence

Threat Intelligence von Nozomi Networks liefert umfassende aktuelle Informationen zu den neuesten Sicherheitsbedrohungen und Schwachstellen, die industrielle Netzwerke betreffen können. Der Service umfasst die Bereitstellung von Packet Rules, Yara-Regeln und Stix-Indikatoren, die auf fundierten Analysen und Echtzeit-Daten basieren.

Mit Threat Intelligence können Sicherheitsteams präventive Maßnahmen ergreifen, indem sie Bedrohungen erkennen und verstehen, bevor sie das Netzwerk schädigen. Unternehmen können ihre Verteidigungsstrategien stärken, indem sie auf detaillierte Warnmeldungen und Analysen zurückgreifen, die eine schnelle Identifikation und Reaktion auf potenzielle Angriffe ermöglichen.

Das **TI Expansion Pack, Powered by Mandiant**, integriert Millionen neuer IOCs, um Nozomi Threat Intelligence zu erweitern und tiefere Einblicke in Schwachstellen zu ermöglichen.

Central Management Console (CMC)

Die **Central Management Console** von Nozomi Networks ist eine zentrale Plattform für die Überwachung, Verwaltung und Analyse von Netzwerksicherheitsdaten über verschiedene Standorte und Einheiten hinweg. Diese leistungsstarke Managementlösung ermöglicht Sicherheitsteams einen umfassenden Überblick über alle OT-, IoT- und IT-Assets innerhalb des Unternehmensnetzwerks.

Die CMC bietet fortschrittliche Funktionen für das Ereignis- und Alarmmanagement sowie die Integration von Threat Intelligence. Indem sie Sicherheitsdaten und -ereignisse zentralisiert, erleichtert die CMC die Erkennung von Mustern und Anomalien, die an verschiedenen Standorten oder Geräten auftreten können, und trägt zu einer effizienteren und effektiveren Reaktion auf Sicherheitsvorfälle bei.

IKARUS Vantage

IKARUS Vantage ist eine innovative Lösung, die speziell für die Skalierung, Verwaltung und Optimierung der Sicherheit von Netzwerken und industriellen Systemen über große und komplexe Unternehmenslandschaften hinweg entwickelt wurde.

Die Plattform ermöglicht es Unternehmen, ihre Sicherheits- und Überwachungsfunktionen zentral zu steuern und gleichzeitig Einblicke in Tausende von Geräten und Systemen weltweit zu erhalten. Durch den Einsatz fortschrittlicher Analyse- und maschineller Lernfunktionen bietet Vantage eine proaktive Überwachung und Bedrohungserkennung, die über herkömmliche Sicherheitsansätze hinausgeht. Dies erleichtert die Früherkennung und Abwehr komplexer Cyber-Bedrohungen und sorgt für eine kontinuierliche Verbesserung der Sicherheit in dynamischen und sich ständig verändernden industriellen Umgebungen.

Nozomi Arc

Arc ist eine spezialisierte Softwarekomponente für die erweiterte Datenerfassung und -analyse von Endpunkten und Netzwerkgeräten außerhalb des direkten Überwachungsbereichs der Standard Guardian Sensoren. Arc ermöglicht die detaillierte Überwachung und Auswertung von Geräten wie Workstations, Servern und anderen kritischen Endpunkten im industriellen Netzwerk.

Durch die Implementierung von Arc erhalten Sicherheitsteams Einblicke in die Aktivitäten und den Sicherheitsstatus von Geräten, die zuvor als blinde Flecken galten. Dazu gehören die Analyse von Protokolldateien, die Erkennung von Insider-Bedrohungen und die Überwachung angeschlossener USB-Geräte. Diese tiefere und breitere Sichtbarkeit stärkt die Sicherheitsarchitektur und hilft bei der Erkennung und Abwehr von Bedrohungen, die sonst unentdeckt geblieben wären.

Arc Embedded

Arc Embedded, entwickelt in enger Zusammenarbeit mit Mitsubishi Electric, ist der weltweit erste eingebettete Sicherheitssensor in industriellen Steuerungssystemen (PLCs), der tiefe Einblicke bis zu den Steuerungsebenen 1 und 0 ermöglicht. Sicherheits- und Betriebsteams erhalten damit erstmals wichtige erweiterte Daten von Industriesteuerungssystemen wie z. B. speicherprogrammierbare Steuerungen (SPS) und die von diesen SPS gesteuerten Feldgeräte.

Durch die Überwachung von Steuerungsgeräten (PLCs) auf Programmänderungen, physische Zugriffe und Anomalien und die Echtzeitanalyse von Netzwerkverkehr, Speicherstrukturen und Kommunikationsmustern stärken Betriebe ihre betriebliche Widerstandsfähigkeit, reduzieren Ausfallzeiten, schützen kritische Infrastrukturen und bewahren die Prozessintegrität.

Vantage

Nozomi Vantage ist eine Cloud-Managementplattform für die Sicherheitsüberwachung und das Risikomanagement von Guardian-Sensoren und Arc-Endpunkten für eine unbegrenzte Anzahl von OT-, IoT-, IT-, Edge- und Cloud-Ressourcen.

Sicherheitsteams können über verschiedene Standorte und Regionen hinweg das Anlagenmanagement, die Schwachstellenbewertung sowie die Erkennung von und Reaktion auf Bedrohungen in einer einzigen Benutzeroberfläche zentralisieren. Intuitive Dashboards vereinfachen die kontinuierliche Überwachung aller OT/IoT-Ressourcen, Protokolle und Schwachstellen. Daten können auf der Makroebene angezeigt oder detaillierte Informationen über das Verhalten von Anlagen, Rollen, Protokollen und Datenflüssen abgerufen werden.

Vantage IQ

Vantage IQ, ein Addon zur Cloud-Managementplattform Vantage, ist die erste KI-basierte Analyse- und Abfrage-Engine der Branche, entwickelt für kritische Infrastrukturen und OT-Umgebungen. Vantage IQ erweitert die Fähigkeiten der Vantage-Plattform um eine AI-/ML-gestützte Engine, ein Query- und Analyse-System und Time Series Analysen.

Vantage IQ automatisiert das Prüfen, Korrigieren und Priorisieren von Netzwerk- und Asset-Daten, um Anomalien vorherzusagen und Bedrohungen schnell und präzise zu begegnen. Dank maschinellem Lernen werden Alarme automatisch priorisiert und Handlungsempfehlungen generiert, was die Effizienz des Teams erhöht und den Arbeitsaufwand verringert.