

# Proof of Value

## OT-Security-Sensor Guardian™ by Nozomi Networks

Als der führende österreichische Managed Security Service Provider (MSSP) von Nozomi Networks ermöglicht Ihnen IKARUS Security Software, den OT-Security Sensor „Guardian“ in einem Proof of Value (PoV) zu testen.

## Was ist ein Guardian-Sensor?

Guardian by Nozomi Networks ist eine passive Sicherheitslösung für industrielle Netzwerke, die vollständige Sichtbarkeit und Kontrolle über Ihre OT- und IoT-Assets, Prozesse und Netzwerkkommunikation bietet. Der Guardian-Sensor erkennt und alarmiert in Echtzeit bei Cyber-Bedrohungen, Schwachstellen und Anomalien und ermöglicht es Ihnen, vor Schäden zu reagieren.

Für den PoV wird der Guardian durch unsere Industrial Cyber Security Expert\*innen installiert und alle relevanten Daten aus dem Netzwerk werden überwacht. Damit können potenzielle Bedrohungen in Echtzeit identifiziert und individuelle Empfehlungen ausgesprochen werden.

## Vorteile des PoV

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

Der Guardian-Sensor ist einfach und ohne Netzwerkunterbrechungen zu installieren und bietet eine effektive Möglichkeit, industrielle Netzwerke zu schützen und Ihr Unternehmen vor Cyberangriffen zu bewahren.

Nach Abschluss des PoV erhalten Sie von uns einen detaillierten Bericht über die Ergebnisse, einschließlich Empfehlungen zur Verbesserung Ihrer OT-Sicherheit. Darüber hinaus steht Ihnen unser Expert\*innenteam zur Verfügung, um weitere Fragen zu beantworten und Sie bei der Umsetzung von Cyber-Security-Maßnahmen zu unterstützen.

## Für wen eignet sich der PoV?

Unser PoV richtet sich an Kunden, die Operational Technology (OT) und Internet of Things Devices in kritischen Infrastrukturen und/oder Produktionsbetrieben einsetzen und ihre OT-Sicherheit verbessern möchten. Sie gewinnen in kürzester Zeit wertvolle Erkenntnisse über Ihre OT-Netzwerke und lernen die Möglichkeiten mit dem passiven Netzwerksensor Guardian in der Praxis kennen.

Kontaktieren Sie uns unter [sales@ikarus.at](mailto:sales@ikarus.at) oder +43 1 58995-500, um mehr über den Guardian-Sensor und unseren PoV-Service zu erfahren. Wir helfen Ihnen gerne, Ihre OT-Sicherheit zu verbessern und Ihr Unternehmen vor Cyberangriffen und Betriebsunterbrechungen zu schützen!

## Wie läuft ein PoV üblicherweise ab?

Umfang und Dauer des PoV können je nach individuellen Anforderungen variieren. Der folgende Ablauf ist als beispielhaft zu verstehen, Abweichungen sind möglich.

### Pre PoV

- Mutual NDA wurde unterzeichnet
- Abstimmungsmeeting zu PoV-Zielen, Sizing and Scoping
- Bereitstellung von Netzwerkeinstellungen für den Guardian samt Hypervisor
- Vorbereitung PoV-Hardware durch IKARUS

### Tag 1

- Installation des Guardian-Sensors vor Ort
- Passive Datenerfassung ab Bereitstellung des Mirror Traffics Ihrer Netzwerk infrastruktur
- Guardian analysiert Netzwerkdaten und lernt, was auf Ihrem Netzwerk als „normal“ betrachtet werden kann
- Erste Überprüfung von Assets, Schwachstellen und Alarmen

### Woche 1

- Basistraining für die Benutzeroberfläche des Guardian

### Woche 2

- Erstes Review-Meeting mit einem/r IKARUS Industrial Cyber Security Expert\*en/in
- Gemeinsame Betrachtung, was in Ihrem Netzwerk passiert

### Woche 3

- Zweites Review-Meeting mit einem/r IKARUS Industrial Cyber Security Experten/in
- Vorbereitung auf die abschließende Präsentation

### Woche 4 / 30 Tage

- Zusammenfassende Überprüfung und Analyse der Ergebnisse durch unsere Expert\*innen
- Zusammenfassender Bericht mit Empfehlungen zur Verbesserung Ihrer OT-Sicherheit
- Abschlussbesprechung mit unseren Expert\*innen, um die nächsten Schritte zu besprechen

# Fragen und Antworten

## Welche Ressourcen werden für den PoV benötigt?

- Bereitstellung von relevanten Informationen über die Netzwerktopologie, Assets und Betriebsprozesse
- Bereitstellung eines Netzwerk-Spiegels und der Netzwerk-Einstellungen für den Guardian-Sensor
- Zeit für Review-Meetings und Abschlusspräsentation mit unseren Industrial Cyber Security Expert\*innen
- Zeit und Bereitschaft, auch während des PoV-Prozesses für Fragen und Diskussionen zur Verfügung zu stehen

## Was passiert mit den erfassten Daten nach dem PoV?

Nach dem Proof of Value (PoV) werden die gesammelten Daten von IKARUS gelöscht, um sicherzustellen, dass keine vertraulichen Informationen aufbewahrt werden. Der detaillierte Bericht und die Empfehlungen zur Verbesserung der OT-Sicherheit werden dem Kunden zur Verfügung gestellt und können zur Planung zukünftiger Sicherheitsmaßnahmen genutzt werden.

## Wie funktioniert die passive Erfassung mit dem Guardian?

Der Guardian-Sensor erfasst Daten aus dem OT-Netzwerk durch sogenanntes Port Spanning, auch bekannt als Port Mirroring. Dabei wird der Datenverkehr von ausgewählten Netzwerkports an einen oder mehrere Überwachungs-Ports gespiegelt. Der Guardian analysiert dann passiv die gespiegelten Daten, ohne den Datenfluss im Netzwerk zu beeinträchtigen oder zusätzlichen Verkehr zu erzeugen. Auf diese Weise erfasst der Guardian-Sensor alle Netzwerkkomponenten, inklusive der OT-Assets, und ermöglicht eine umfassende Sichtbarkeit und Analyse des OT-Netzwerks.

## Ist der Guardian auch für IT-Netzwerkverkehr geeignet?

Ja, der Guardian-Sensor von Nozomi Networks ist auch für IT-Netzwerkverkehr geeignet. Obwohl der Guardian-Sensor hauptsächlich für den Einsatz in OT-Netzwerken entwickelt wurde, kann er auch den Netzwerkverkehr von IT-Netzwerken überwachen und analysieren.

## Was kostet ein PoV?

Die Kosten für einen PoV können je nach Umfang und individuellen Anforderungen variieren. Kontaktieren Sie das IKARUS Sales-Team, um ein Angebot zu erhalten!

## Was sind die Stärken von IKARUS?

IKARUS Security Software GmbH hat mehr als 30 Jahre Erfahrung in der Entwicklung und Implementierung von Sicherheitstechnologien. Das Unternehmen ist spezialisiert auf IT- und OT-Sicherheit und bietet ein breites Portfolio an Produkten und Lösungen, um Kunden in verschiedenen Branchen und Sektoren zu schützen. IKARUS ist bekannt für seinen exzellenten Kundenservice und seine schnelle Reaktionszeit auf Kundenanfragen und -probleme.

