Proof of Value

OT-Security-Sensor
Guardian™ by Nozomi Networks

As the leading Austrian Managed Security Service Provider (MSSP) of Nozomi Networks, IKARUS Security Software enables you to test the OT-Security Sensor „Guardian“ in a Proof of Value (PoV).

What is a Guardian sensor?

Guardian™ by Nozomi Networks is a passive security solution for industrial networks, that provides complete visibility and control over your OT and IoT assets, processes, and network communications. The Guardian sensor detects and alerts in real time to cyber threats, vulnerabilities and anomalies, enabling you to respond before damage occurs.

For PoV, our Industrial Cyber Security experts install the Guardian and monitor all relevant data from the network. This allows for real-time identification of potential threats and individual recommendations.

Benefits of the PoV

- ✓ Automated asset discovery
- ✓ Visibility of assets and network communication
- ✓ Real-time detection of threats, vulnerabilities, and anomalies
- ✓ Interactive network visualization
- ✓ Monitoring of relevant process variables

The Guardian sensor is easy to install and use, making it an effective way to protect your OT networks and safeguard your business from cyberattacks. After completion of the PoV, we will provide you with a detailed report on the results, including recommendations for improving your OT security. In addition, our team of experts is available to answer further questions and support you in implementing measures to improve your OT security.

Who is the PoV suitable for?

Our PoV is aimed at customers who use Operational Technology (OT) and Internet of Things devices in critical infrastructures and/or production facilities and want to improve their OT security. You will gain valuable insights into your OT networks in a short time and learn about the possibilities with the Guardian.

Contact us at sales@ikarus.at or +43 1 58995-500 to learn more about the Guardian sensor and our PoV service. We look forward to helping you improve your OT security and protect your business from cyberattacks and business interruption.

What is the usual procedure for a PoV?

The scope and duration of the PoV may vary depending on individual requirements. The following procedure is to be understood as exemplary, deviations are possible.

Pre PoV

- Mutual NDA was signed
- Coordination meeting on PoV targets, sizing and scoping
- Provision of network settings for the Guardian including hypervisor
- Preparation of PoV hardware by IKARUS

Week 1

- On-site installation of the Guardian sensor
- Passive data collection from deployment of the mirror traffic of your network infrastructure
- Guardian analyses network data and learns what can be considered „normal“ on your network
- Initial screening of assets, vulnerabilities and alarms
- Basic training for the Guardian user interface

Week 2

- Review meeting with an IKARUS Industrial Cyber Security Expert
- Joint consideration of what is happening in your network
- Preparation for the final presentation

At the latest within 30 days

- Summary review and analysis of the results by our Industrial Cyber Security Experts
- Summary report with recommendations to improve your OT security
- Final meeting with our experts to discuss next steps

Questions and Answers

What resources are needed for the PoV?

- Provision of relevant information about network topology, assets, and operational processes
- Provision of a network mirror and network settings for the Guardian sensor
- Time for review meetings and final presentation with our Industrial Cyber Security Experts
- Time and willingness to be available for questions and discussions also during the PoV process

What happens to the collected data after the PoV?

After the PoV, the collected data is deleted to ensure that no confidential information is stored. However, the detailed report and recommendations for improving OT security are provided to the customer and can be used for planning future security measures.

How does passive monitoring with the Guardian work?

The Guardian sensor captures data from the OT network through a process called port spanning, also known as port mirroring. In this process, the network traffic from selected network ports is mirrored to one or more monitoring ports. The Guardian then passively analyses the mirrored data without affecting the data flow in the network or generating additional traffic. This allows the Guardian sensor to capture all network components, including OT assets, and provide comprehensive visibility and analysis of the OT network.

Is the Guardian also suitable for IT network traffic?

Yes, the Nozomi Networks Guardian sensor is also suitable for IT network traffic. Although the Guardian sensor was primarily developed for monitoring OT networks, it can also monitor and analyse the network traffic of IT networks.

What does a PoV cost?

The cost of a POV can vary depending on the scope and individual requirements. It is best to contact our sales team directly to receive an offer.

What are the strengths of IKARUS?

IKARUS Security Software GmbH has over 30 years of experience in developing and implementing security technologies. The company specializes in IT and OT security and offers a wide portfolio of products and solutions to protect customers in various industries and sectors. IKARUS is known for its excellent customer service and quick response time to customer inquiries and issues.

IKARUS
security software

CERTIFIED NOZOMI
MSSP PARTNER