IKARUS security software

Certified PLATINUM Partner

Certified MSSP Elite Partner

Issued by Nozomi Networks, Leader in OT & IoT Security

NOZOMI NETWORKS
MSSP of the Year 2024
IKARUS security software

Spezifikation

# Implementierung von OT-Security Sensoren zur Überwachung und Sicherung kritischer Infrastrukturen nach NIS2

# Inhalt

# Spezifikation für die Implementierung von OT-Security Sensoren gemäß NIS2-Richtlinie

Ein OT-Security Sensor ist ein Gerät zur **passiven Netzwerkanalyse**, das über Spiegelverkehr (Mirror Traffic) arbeitet, um Bedrohungen und Anomalien zu erkennen.

OT-Security Sensoren integrieren Funktionen wie Intrusion Detection Systeme (IDS), Bedrohungserkennung, Anomalie-Erkennung, Schwachstellenerkennung und Asset-Erkennung. Sie bieten eine detaillierte Überwachung des Netzwerkverkehrs, **ohne in die Datenübertragung einzugreifen**, und ermöglichen eine umfassende Sicherheitsanalyse in industriellen Kontrollsystemen.

OT-Security Sensoren werden meist mit folgenden Spezifikationen ausgeschrieben**:**

| | **Max. zu überwachende private Assets** | **Max. Durchsatz (Mbps)** |
|---|---|---|
| **Low (L)** | 250 | 500 |
| **Medium (M)** | 1000 | 1000 |
| **High (H)** | 5000 | 3000 |
| **Very High (HS)** | 10000 | 6000 |

Die Sensoren sind als rugged, baremetal oder virtuell verfügbar und bieten bis zu 8 Monitoranschlüsse (SFP/SFP+).

## Erläuterungen

Die folgenden Inhalte orientieren sich an den Anforderungen gemäß NIS2-Richtlinie zur Überwachung und Sicherung kritischer Infrastrukturen. Das Dokument ermöglicht einen Abgleich der Funktionen von OT-Security Sensoren mit den regulatorischen Anforderungen bzw. die Erstellung eines NIS2-konformen Anforderungskatalogs, um die Cybersicherheit Ihres Betriebes nachhaltig und zukunftssicher zu gestalten.

Anhand der Bewertungstabelle am Ende des Dokuments können unterschiedliche Technologien miteinander verglichen und ihre Eignung für den Einsatz in kritischen Strukturen bewertet werden. Der Entscheidungsprozess bei der Auswahl und Implementierung geeigneter OT-Security Sensoren wird effizient und nachvollziehbar gestaltet und die Interoperabilität mit bestehenden oder ergänzenden Systemen sichergestellt.

# 1. Basisanforderungen

**§ 1.1** Die OT-Security Sensoren müssen eine kontinuierliche Überwachung und Analyse des Netzwerkverkehrs bieten, um potenzielle Bedrohungen und Anomalien in Echtzeit zu erkennen. Dies umfasst die signaturbasierte Erkennung (SIDS) zur Abgleichung von Mustern aus Netzwerkpaketen mit bekannten Angriffssignaturen sowie die **A**nomalie-basierte Erkennung (AIDS) zur Erstellung eines Profils des normalen Verhaltens und zur Erkennung von Abweichungen. Es müssen Anomalien wie ungewöhnlich hoher Traffic, unbekannte Protokolle und verdächtige Verbindungen erkannt werden. Die Sensoren müssen aktuelle Threat Intelligence Datenbanken des Herstellers nutzen, die Indikatoren für Kompromittierungen (IOCs) enthalten und signaturbasierte Erkennung wie Snort/Suricata unterstützen.

# 2. Leistung und Verfügbarkeit

**§ 2.1** Hohe Verfügbarkeit von 99,99 % muss gewährleistet sein, um den kontinuierlichen Betrieb der OT-Infrastrukturen zu gewährleisten.

**§ 2.2** Minimale Ausfallzeiten (RMA 48h) müssen garantiert sein.

**§ 2.3** Es muss die Möglichkeit bestehen, den eingehenden Traffic mittels BPF-Filter und Whitelists zu filtern, wenn Bedarf besteht.

# 3. Asset Management samt Vulnerabilities

**§ 3.1** Es muss die Fähigkeit vorhanden sein, alle IT-, IoT- und OT-Geräte im Netzwerk zu erkennen und zu inventarisieren, ohne den Betrieb zu beeinträchtigen. Die OT-Security Sensoren müssen ein interaktives, automatisch erstelltes Asset-Inventar bereitstellen, das neue Geräte identifizieren und detaillierte Informationen wie Gerätetyp und Firmware-Versionen umfassen kann.

**§ 3.2** Die Erkennung muss auch eine Bewertung und Verwaltung von Schwachstellen einschließen, um die Transparenz und Sicherheit des Netzwerks zu gewährleisten.

**§ 3.3** Diese Daten müssen exportierbar sein bzw. Drittsystemen via API zur Verfügung gestellt werden können.

**§ 3.4** Die OT-Security Sensoren müssen spezifische IT-, IoT- und OT-Schwachstellen identifizieren können.

# 4. Visibilität der Kommunikationsbeziehungen

**§ 4.1** Die OT-Security Sensoren müssen eine umfassende Sichtbarkeit der Kommunikationsbeziehungen zwischen den Geräten im Netzwerk bieten.

**§ 4.2** Diese Sichtbarkeit muss mittels Graphen und Listen dargestellt werden können.

**§ 4.3** Die Sichtbarkeit muss eine detaillierte Analyse der Netzwerkverkehrsmuster umfassen.

**§ 4.4** Die Analyse muss in Echtzeit erfolgen, um Anomalien und potenzielle Bedrohungen zu erkennen.

**§ 4.5** Die Sensoren müssen die Segmentierung des Netzwerks aufzeigen und den Quer-Traffic zwischen Netzwerkzonen klar darstellen.

**§ 4.6** Es muss eine quantitative Aussage über den Netzwerk-Traffic, einschließlich Retransmissions und Handshakes zwischen Zonen und Assets, gegeben werden.

## 5. Advanced Cyber Threat Detection & adaptive Abwehr

**§ 5.1** Die Erkennung von Malware in Dateien muss durch YARA-Regeln, STIX-Indikatoren und Sigma-Regeln erfolgen.

**§ 5.2** Aktuelle Schwachstelleninformationen müssen integriert sein, einschließlich CPE, CWE und CVE. Die OT-Security Sensoren müssen aktualisierte Sicherheitsdatenbanken zur schnellen Erkennung und Minimierung von Cyberangriffen nutzen.

**§ 5.3** Die Sensoren müssen adaptive Abwehrmechanismen bieten, die sich automatisch an neue Bedrohungen anpassen und diese abwehren können.

**§ 5.4** Die Sensoren müssen in der Lage sein, Verhaltensanalysen durchzuführen, um kontinuierlich Lernmodelle zu aktualisieren und präventive Maßnahmen gegen unbekannte Bedrohungen zu ergreifen.

**§ 5.5** Die Sensoren müssen Berichte und Dashboards bereitstellen, die eine klare Darstellung der Sicherheitslage und erkannter Bedrohungen bieten.

**§ 5.6** Indikatoren für Kompromittierungen (IoC) müssen ungewöhnliche Login-Versuche, Datenexfiltration und Malware-Aktivitäten umfassen.

**§ 5.7** Die OT-Security Sensoren müssen die Robustheit gegen Cyberangriffe erhöhen.

**§ 5.8** Die OT-Security Sensoren müssen eine aktive Blockfunktion in Kombination mit einem Firewall-System bieten.

**§ 5.9** Die OT-Security Sensoren müssen Sofortschutz gegen Ransomware bieten.

**§ 5.10** Die OT-Security Sensoren müssen proaktive Schwachstellen- und Risikoerkennung sowie die Identifizierung von MITRE-Angriffsmustern ermöglichen.

**§ 5.11** Die OT-Security Sensoren müssen Echtzeit-Warnungen zu verdächtigen Aktivitäten und Bedrohungen wie z.B. Malware-Erkennung bereitstellen.

## 6. Protokollunterstützung

**§ 6.1** Die OT-Security Sensoren müssen eine breite Palette von Protokollen unterstützen, um eine umfassende Abdeckung und Interoperabilität zu gewährleisten. Dazu gehören Modbus, DNP3, BACnet, IEC 61850, OPC UA, Ethernet/IP, PROFINET, CIP, HTTP, HTTPS, FTP, SFTP, SNMP, SMTP, RDP, SSH, Telnet, LDAP, SMB, DNS, DHCP und NTP.

## 7. Integration von Drittsystemen

**§ 7.1** Die OT-Security Sensoren müssen über Schnittstellen und Protokolle wie REST APIs, SNMP und Syslog verfügen.

**§ 7.2** Die Sensoren müssen in der Lage sein, sich mit bestehenden Sicherheitslösungen wie SIEM, Firewalls und Endpoint Protection zu integrieren. Dazu zählen beispielsweise FortiGate NGFW, PA-Series von Palo Alto Networks, Cisco Firepower, Check Point Firewall, SonicWall, Cortex XSOAR, Splunk, IBM QRadar, ArcSight, LogRhythm, Microsoft Sentinel, ServiceNow.

## 8. Audit, Compliance und Reporting

**§ 8.1** Die OT-Security Sensoren müssen in der Lage sein, interne Systemereignisse und Benutzeraktivitäten aufzuzeichnen. Dies schließt die Aufzeichnung von Änderungen der Systemkonfiguration, der An- und Abmeldung von Benutzern, von Fehlermeldungen sowie von sicherheitsrelevanten Ereignissen ein. Die Daten müssen manipulationssicher gespeichert und für Prüfungs- und Analysezwecke zugänglich gemacht werden.

**§ 8.2** Die OT-Security Sensoren müssen eine vollumfängliche Timemachine-Funktion (Snapshot-Funktion) inkl. Versionsvergleichsprüfung bieten.

# Bewertungstabelle

Die Punkte zeigen an, welche Funktionen für Ihre Sicherheit besonders wichtig sind. Je mehr Punkte ein Element aufweist, desto höher ist dessen Relevanz für Ihre Sicherheit.

| § | Anforderung | Punkte |
|---|---|---|
| **1. Basisanforderungen (20)** | | |
| **1.1** | Kontinuierliche Überwachung und Analyse | 20 |
| **2. Leistung und Verfügbarkeit (15)** | | |
| **2.1** | Hohe Verfügbarkeit | 8 |
| **2.2** | Minimale Ausfallzeiten | 5 |
| **2.3** | Filtermöglichkeiten | 2 |
| **3. Asset Management samt Vulnerabilities (12)** | | |
| **3.1** | Erkennung und Inventarisierung | 5 |
| **3.2** | Bewertung und Verwaltung von Schwachstellen | 4 |
| **3.3** | Datenexport via API | 1 |
| **3.4** | Erkennung spezifischer Schwachstellen | 2 |
| **4. Visibilität der Kommunikationsbeziehungen (10)** | | |
| **4.1** | Sichtbarkeit der Kommunikationsbeziehungen | 5 |
| **4.2** | Darstellung mittels Graphen und Listen | 1 |
| **4.3** | Verkehrsflussanalyse | 1 |
| **4.4** | Echtzeitanalyse | 1 |
| **4.5** | Segmentierung | 1 |
| **4.6** | Quantitative Analyse des Netzwerk-Traffics | 1 |
| **5. Advanced Cyber Threat Detection und adaptive Abwehr (30)** | | |
| **5.1** | Erkennung von Malware | 2 |
| **5.2** | Integration aktueller Schwachstelleninformationen | 1 |
| **5.3** | Adaptive Abwehrmechanismen | 2 |
| **5.4** | Verhaltensanalyse | 2 |
| **5.5** | Berichterstellung | 1 |
| **5.6** | Erkennung von IoCs | 1 |
| **5.7** | Nutzung aktueller Sicherheitsdatenbanken | 1 |
| **5.8** | Erhöhung der Robustheit gegen Cyberangriffe | 1 |

| | | |
|---|---|---|
| **5.9** | Aktive Blockfunktion | 1 |
| **5.10** | Sofortschutz gegen Ransomware | 1 |
| **5.11** | Schwachstellen- und Risikoerkennung | 1 |
| **5.12** | Echtzeit-Warnungen | 1 |
| **6. Protokollunterstützung (6)** | | |
| **6.1** | Breite Protokollunterstützung | 6 |
| **7. Integration von Drittsystemen (5)** | | |
| **7.1** | Schnittstellen und Protokolle | 3 |
| **7.2** | Integration bestehender Sicherheitslösungen | 2 |
| **8. Audit, Compliance und Reporting (2)** | | |
| **8.1** | Aufzeichnung Systemereignisse und Benutzeraktivitäten | 1 |
| **8.2** | Vollumfängliche Timemachine | 1 |

Die Bewertungstabelle hilft Ihnen, verschiedene Lösungen zu vergleichen und diejenige zu finden, die Ihren Anforderungen am besten entspricht ist und den größten Sicherheitsvorteil bietet.

## Informationen und Beratung

IKARUS unterstützt Sie bei der Lösungsauswahl, Kostenbetrachtung und Implementierung Ihrer OT-Security Sensoren. Mit den IKARUS Professional Services stehen wir Ihnen im auch laufenden Betrieb beratend und unterstützend zur Seite.

**Kontaktieren Sie uns:**

Tel.: +43 1 58995-500
E-Mail: sales@ikarus.at

Über IKARUS

IKARUS Security Software GmbH ist ein spezialisierter Anbieter von OT-Sicherheitslösungen und professionellen Dienstleistungen zur Verbesserung der Sicherheit kritischer Infrastrukturen in Europa. Durch Partnerschaften mit Branchenführern wie Nozomi Networks und Axonius bietet IKARUS integrierte Lösungen für umfassendes Asset Management, Bedrohungserkennung und Compliance.

**www.IKARUSsecurity.com/industrial-cyber-security**