CYJAN Intrusion Detection System

SENTRY MODE FOR OT

CYJAN

INTRUSION DETECTION SYSTEM

Passives OT-Netzwerkmonitoring. Echtzeit-Bedrohungserkennung. Self-Learning-Feedback-Loop.

PROTECT · DETECT · RESPOND

DAS PRODUKT

CYJAN Sentry Mode erkennt Einbrüche in industrielle Netzwerke – passiv, ohne Eingriff in laufende Prozesse. Das System kombiniert drei Erkennungsschichten: regelbasierte Signaturen, Machine-Learning-Anomalieerkennung und die Suricata-Engine. Alle Alarme laufen in einem zentralen Echtzeit-Dashboard zusammen, das im Browser läuft und keinen Client benötigt.

Spezieller Fokus auf OT/ICS-Umgebungen: SCADA, Modbus, DNP3, EtherNet/IP, BACnet, S7Comm. Ausschließlich Header-Analyse – kein Payload-Zugriff, kein Eingriff in die Kommunikation.

KERNFÄHIGKEITEN AUF EINEN BLICK

Passives Monitoring

Mirror-Port-Betrieb – keine Auswirkung auf laufende Prozesse oder Netzwerklatenz.

Drei Erkennungsschichten

Signaturen + ML-Anomalieerkennung + Suricata laufen parallel und ergänzen sich.

OT/ICS-Fokus

Native Unterstützung für Modbus, DNP3, EtherNet/IP, BACnet, S7Comm und weitere Industrieprotokolle.

Self-Learning

Feedback-Loop: True/False-Positive-Bewertungen fließen direkt in den ML-Retrain ein.

Echtzeit-Dashboard

WebSocket-Stream, Verbindungsgraph, PCAP-Download und Threat-Level-Gauge im Browser.

IRMA-Integration

Externe IRMA-IDS-Alarme werden nahtlos in den Alert-Feed integriert – eine Oberfläche für alles.

WARUM CYJAN SENTRY MODE?

Für Betreiber & Security-Teams

- Keine Downtime bei der Installation – passives Tap am Mirror-Port
- Ein Dashboard für Signatur-, ML-, Suricata- und IRMA-Alarme
- PCAP-Download pro Alert für sofortige forensische Analyse
- Threat-Level-Gauge auf einen Blick: 0–100, farbkodiert
- Rollen: Admin, Viewer, API-Service-Account (365-Tage-JWT)

Für Entwickler & Integratoren

- Vollständige REST-API + WebSocket mit Swagger UI und ReDoc
- Offene Architektur: Kafka, TimescaleDB, MinIO, Docker Compose
- Debian Live ISO mit First-Boot-Wizard für schnelle Inbetriebnahme
- ML-Parameter live anpassbar: Threshold, Contamination, Retrain
- Eigene Regelquellen per URL ergänzbar, Live-Reload ohne Restart

- CSV-Export, SMTP/SFTP/REST-API-Alarmierung, OPC UA DA
- SAML/SSO-Integration für Enterprise-Umgebungen

SO FUNKTIONIERT CYJAN

1 Capture
Rust-Sniffer liest Header am Mirror-Port (kein Payload)

2 Analyse
Signaturen, ML und Suricata analysieren Flows parallel

3 Alert
Enrichment: DNS, GeoIP, ASN, Trust – dann Alarm + PCAP

4 Lernen
FP/TP-Feedback verbessert das ML-Modell kontinuierlich

EINSATZBEREICHE

Energie & Versorgung | **Produktion & Fertigung** | **Wasser & Abwasser** | **Transport & Logistik**

SCADA & ICS | **Kritische Infrastruktur** | **Gebäudeautomation** | **Network SOC**

TECHNOLOGIE AUF EINEN BLICK

Appliance & Deployment

- Debian Live ISO mit First-Boot-Wizard oder Docker Compose
- Industrie-Appliance: lüfterlos, -20 bis +70 °C, IP20
- Bis zu 1 Gbps Datendurchsatz, 3× Monitor-/SPAN-Ports
- DC 12–48 V / AC 100–240 V, max. 45 W
- Bestellnummern: SM-250 / SM-500 / SM-1000 Assets

Stack & Protokolle

- Rust + Kafka + TimescaleDB + Redis + MinIO
- ML: Isolation Forest (Scikit-learn) + River Online-Scaler
- OT-Protokolle: Modbus TCP, DNP3, EtherNet/IP, BACnet, S7
- Alarmierung: SMTP, SFTP, REST-API, Syslog, OPC UA DA
- Export: PCAP (Wireshark), CSV, XLSX, PDF, XML

CYJAN Sentry Mode ist Open Source – Releases und Dokumentation:

github.com/JxxKal/ids

CYJAN Security Systems · protect@cyjan.dev · www.cyjan.dev