EXYS
WHERE PASSION
MEETS TECHNOLOGY




# KONDRA

SIEM, MDR, CTI FOR SMALL AND MEDIUM ENTERPRISES

KONDRA:

## ROUND-THE-CLOCK MONITORING WITHOUT BUILDING YOUR OWN SOC.

Your firewalls, Windows machines and Microsoft 365 tenant already record what happens on the network. Almost nobody reads it. Watching those records around the clock takes a security operations centre (SOC) with analysts on shifts, which few small and medium companies can staff.

So the logs pile up, and the first sign of an intrusion is usually the damage.

Kondra collects those logs, indexes them as they arrive and reads the network traffic itself through a mirror port on your switch. Detection rules and threat intelligence turn the volume into alerts, and EXYS analysts work through them 24 hours a day.

Everything runs on an appliance in your own network. The analysts look at your data where it is; it does not leave the building.

**ENTERPRISE DETECTION.**
**SMALL BUSINESS INVOICE.**

www.exys.swiss

The appliance reads the traffic passively from a switch mirror port, across more than 20 network protocols. Unusual connections, misconfigured hosts and data leaving the network show up even on machines with nothing installed.

Ombra, the Kondra endpoint agent, adds what the network cannot see: the applications installed on each machine and how it is configured. Changes to Active Directory users, groups and group policies are recorded too, so a new admin account is an event Kondra can alert on.

Auditors and regulators ask the same questions after every incident: what happened, when, and what was done about it. With Kondra the answers are already on record. Every event is searchable, the EXYS SOC opens a case with the logs and indicators of compromise (IoC) attached, and the forensic report is written from the same data. Retention is set per customer, so logs are kept as long as your auditors, regulators or internal policies require. EXYS itself is ISO 27001 certified.



## WHAT YOU GET:

- On-premises appliance sized to your number of endpoints, logs stay on your site
- Monitoring and response 24/7 by EXYS SOC analysts
- Passive network monitoring from a switch mirror port, more than 20 protocols
- Log collection from firewalls of several vendors, Microsoft 365, Windows events, network and IDS, plus custom sources on request
- Correlation with open-source and proprietary threat intelligence
- Pre-built dashboards, a network map of problem hosts and multi-channel alerting
- Ombra endpoint agent for software inventory and endpoint configuration
- Active Directory change tracking: users, groups, group policies and organizational units
- Incident case management inside the EXYS SOC, with linked logs, IoCs and forensic reports
- MITRE ATT&CK and RE&CT matrices showing detection and response coverage
- Malware analysis, with isolated files and PCAP captures kept for investigation
- Extensions for OT event management
- Log retention, integrity checks and backup for compliance audits

## CONTACT US


ADDRESS

**EXYS SA**
Strada Regina 16
CH-6934 Bioggio
Ticino, Switzerland

CONTACT

**Phone +41 (0)91 220 52 00**

www.exys.swiss
office@exys.swiss

EXYS SA is ISO/IEC 27001 certified


EXYS
WHERE PASSION MEETS TECHNOLOGY

EXYS7950-KONDRA

KONDRA 2v1 20261001