EXYS7950-KONDRA

SIEM, MDR, CTI FOR SMALL AND MEDIUM ENTERPRISES

EXYS7950-KONDRA: ENTERPRISE-GRADE MANAGED DETECTION AND RESPONSE AT AFFORDABLE PRICES

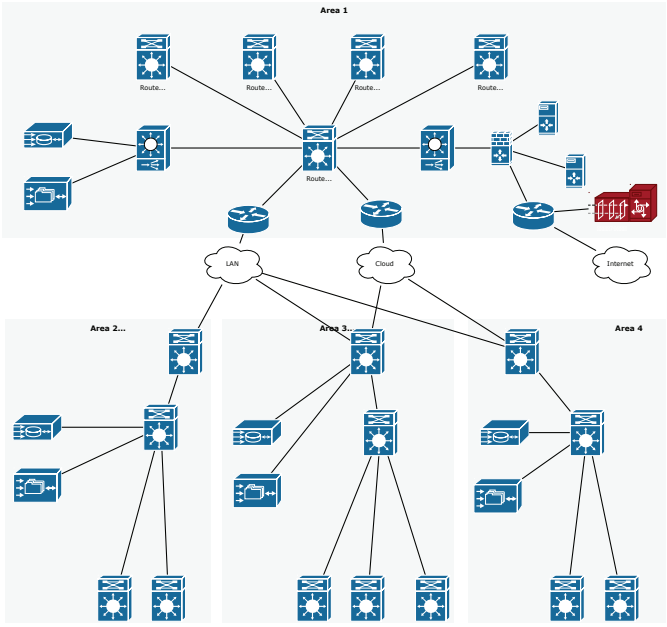
ECLEXYS

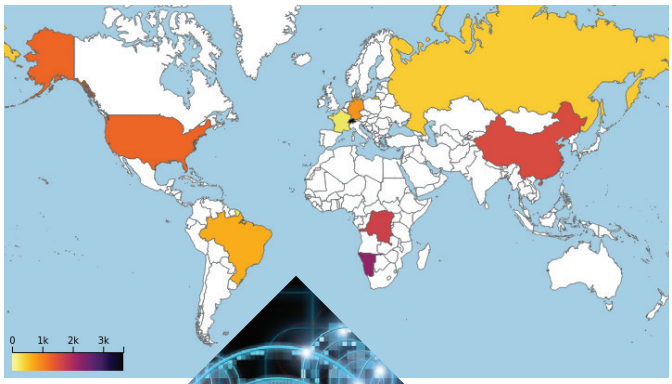
Where Passion Meets Technology

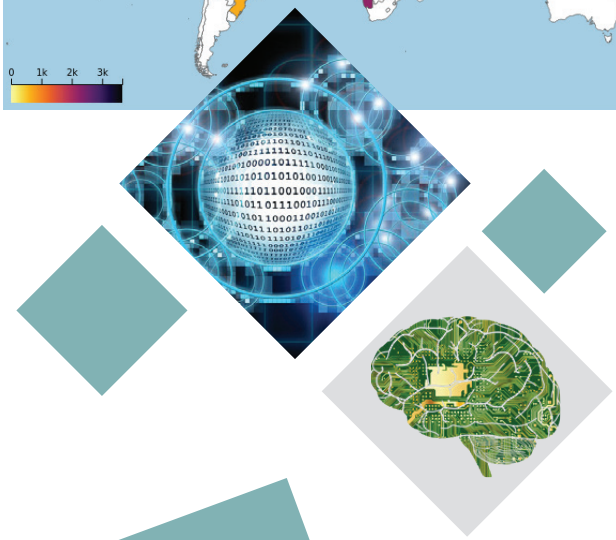
Today's rapid development of ICT systems (information, industrial and communication technologies), their governance requirements and their multi-faceted structure imposes adequate security events detection and analysis instruments. Yet the growing complexity of these systems makes such instruments quickly obsolete, calling for a constant monitoring and a continuous review and improvement of specific detection and prevention capabilities.

EXYS7950 is a flexible SIEM (Security Information and Event Management) and NDR (Network Detection and Response) framework implementing several analysis engines that make it unique in its genre, empowering professionals in their data-driven decision making. Thanks to both passive and active data collection capabilities, EXYS7950 provides IT and OT managers a holistic view of their security posture: vulnerabilities, risks, threats and an understanding of their implication in a corporate environment.

As attackers will undoubtedly continue to evolve their tactics and the complexity of potential threats increases, the first characteristics that an all-encompassing solution must have are flexibility, scalability and extensibility.
Second, the solution has to be affordable. Too many small businesses realize the need for more security, but are unable to afford it. The high prices and impact on the business structure often prevents organizations with limited resources from implementing a security monitoring solution. Thanks to artificial intelligence algorithms and a powerful alerting sub-system, EXYS7950 guarantees moderate prices and reduced operational costs.
An optional module of the framework enables security incident case management, starting with incident correlation and reporting, to allow security analysis to add related logs, indicators of compromise (IoC) or other findings during the incident management life cycle.







LIST OF EXYS7950 KONDRA SERVICES:

- Passive network monitoring, able to detect anomalies, misconfigurations, data exfiltration and other unwanted traffic
- Event log collector and indexing engine for several third-party solutions, including Microsoft AD services, on premise or in cloud Microsoft 365, firewalls, databases, web servers, etc.
- Log and event management tool for data aggregation, alerting and cross correlation with open-source and proprietary indicators and databases
- Rich pre-built dashboards and multi-channel, multi-standard alerting system
- Principles of SIRP (Security Incident Response Platform) and SOAR (Security Orchestration Automation Response)
- Flexible big-data indexing system, extensible to interface with alternative platforms used by the customer
- Multi-layered GUI studied for use from 3 distinct profiles: administrators, service managers and service users
- Incident investigation and reporting tool allowing very user-friendly and efficient creation of forensic reports
- Extensions for OT event management
- CTI module for the definition of ATT&CK and RE&CT matrices for SOC analysts to visualize defensive coverage and actionable Incident Response techniques.
- Extensions for the management of binary files (detected and isolated viruses , PCAP files, ...)
- Malware analysis module and reporting tool
- Data integrity check and backup module

CONTACT US

ECLEXYS

Address
ECLEXYS Sagl
Via dell' Inglese 6
CH-6826 Riva San Vitale (TI)
Switzerland

Contact
Phone +41 91 600 00 00
Fax +41 91 600 00 01
www.eclexys.com
office@eclexys.com

EXPERIENCE SUPPORT NETWORK DLT TSP CYBER SECURITY IOT MOBILE COM. CLOUD