

KONDRA

SIEM, MDR E CTI PER LE PMI

KONDRA:

MONITORAGGIO 24/7, SENZA UN SOC INTERNO.

Firewall, client Windows e tenant Microsoft 365 registrano già nei log tutto ciò che succede in azienda. Quasi nessuno li legge. Monitorarli 24/7 richiede un Security Operations Center (SOC) con analisti a turni, che poche PMI possono permettersi.

Così i log si accumulano e di solito ci si accorge di un'intrusione solo quando il danno è fatto.

Kondra raccoglie quei log, li indicizza in tempo reale e analizza il traffico di rete da una porta mirror (SPAN) dello switch. Regole di rilevamento e threat intelligence trasformano questa mole di dati in alert, che gli analisti EXYS gestiscono 24/7.

Tutto funziona su un'appliance installata in azienda. Gli analisti accedono ai dati lì dove si trovano: i log non escono dall'azienda.

SICUREZZA DA GRANDE AZIENDA.
COSTI DA PMI.

L'appliance analizza il traffico in modo passivo da una porta mirror dello switch, su oltre 20 protocolli di rete. Connessioni anomale, host mal configurati ed esfiltrazione di dati vengono rilevati anche sulle macchine senza agente.

Ombra, l'agente endpoint di Kondra, aggiunge ciò che la rete non vede: le applicazioni installate su ogni macchina e la sua configurazione. Anche le modifiche a utenti, gruppi e GPO di Active Directory vengono registrate, così la creazione di un nuovo account amministratore può generare un alert.

Dopo ogni incidente, auditor e autorità fanno le stesse domande: cosa è successo, quando e cosa è stato fatto. Con Kondra le risposte sono già documentate. Ogni evento è ricercabile, il SOC di EXYS apre un caso con i log e gli indicatori di compromissione (IoC) allegati, e il report forense viene generato dagli stessi dati. Il periodo di conservazione dei log è definito per ogni cliente, così restano disponibili per tutto il tempo richiesto da auditor, autorità o policy interne.

COSA È INCLUSO:

- Appliance on-premise dimensionata sul numero di endpoint: i log restano in sede
- Monitoraggio e risposta 24/7 da parte degli analisti del SOC di EXYS
- Monitoraggio passivo della rete da porta mirror dello switch, su oltre 20 protocolli
- Raccolta dei log da firewall di diversi produttori, Microsoft 365, eventi Windows, dispositivi di rete e IDS, più fonti personalizzate su richiesta
- Correlazione con threat intelligence open source e proprietaria
- Dashboard pronte all'uso, mappa di rete degli host problematici e alert multicanale
- Agente endpoint Ombra per l'inventario del software e della configurazione
- Tracciamento delle modifiche in Active Directory: utenti, gruppi, GPO e unità organizzative
- Gestione degli incidenti da parte del SOC di EXYS, con log, IoC e report forensi collegati
- Matrici MITRE ATT&CK e RE&CT che mostrano la copertura di rilevamento e risposta
- Analisi dei malware, con file in quarantena e catture PCAP conservate per le indagini
- Estensioni per il monitoraggio degli ambienti OT
- Conservazione dei log, controlli di integrità e backup per gli audit di conformità

CONTATTI

INDIRIZZO

EXYS SA
Strada Regina 16
CH-6934 Bioggio
Ticino, Svizzera

CONTATTO

Telefono +41 91 220 52 00

www.exys.swiss
office@exys.swiss

EXYS SA è certificata ISO/IEC 27001



EXYS
WHERE PASSION
MEETS TECHNOLOGY
EXYS7950 - KONDRA