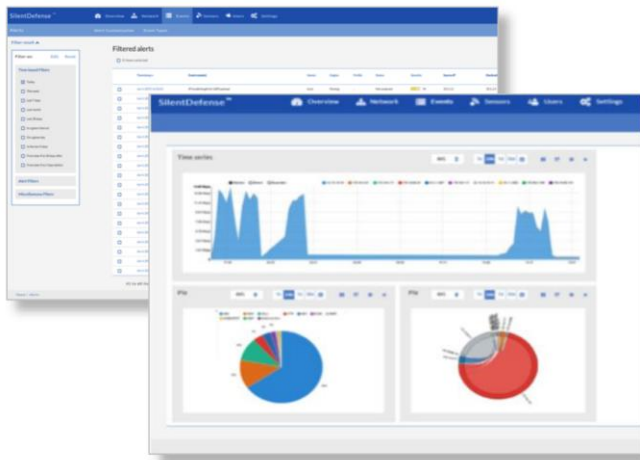


SilentDefense ICS Інформація про продукт



SilentDefense ICS – мережева платформа моніторингу та аналізу, що робить промислові системи управління та комунікаційні мережі кібер-стійкими.

SilentDefense ICS, завдяки прихованій присутності всередині промислових мереж та процесів, захищає їх від широкого діапазону проблем. Завдяки унікальній властивості розпізнавання та аналізу промислових протоколів зв'язку і розвиненим засобам стеження, платформа гарантує виявлення будь-якої небажаної чи підозрілої активності в мережі. Кібератаки, проблеми з обладнанням та помилки оператора більше не залишаться непоміченими.

Особливості

Автоматичне профілювання роботи мережі

- Способів підключення до мережі
- Протоколів та команд
- Поля та значення протоколу

Забезпечення визначених користувачем перевірок

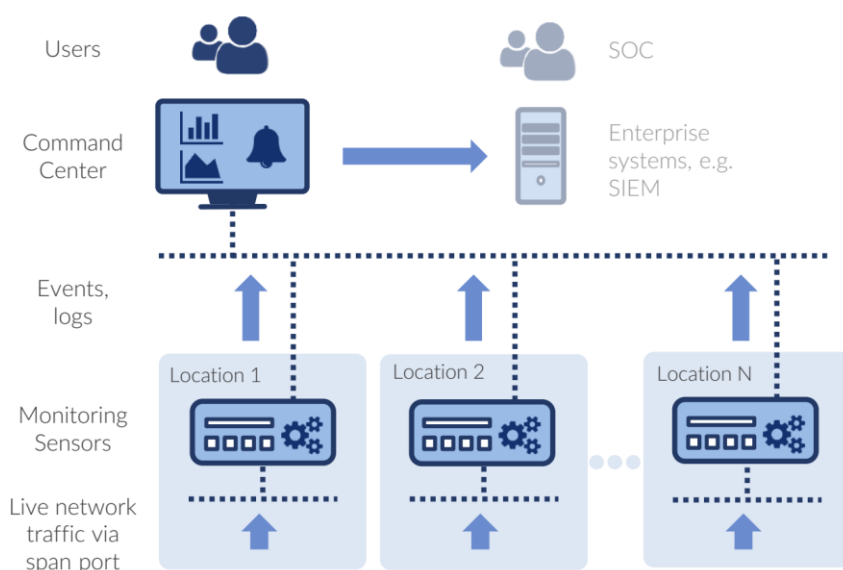
Потужна візуальна аналітика в режимі реального часу та експертна оцінка

Розширене виявлення загроз

- Пошкодження промислових протоколів
- Помилкових налаштувань або несправності мережевих пристроїв
- Помилки оператора
- Системних зловживань з боку персоналу або сторонніх осіб
- Спроб вторгнення
- Відомих атак та атак «нульового дня»

Компоненти та архітектура

SilentDefense ICS складається з командного центру та одного або декількох сенсорів моніторингу



Командний центр

- Візуальна аналітика
- Управління сенсорами та подіями
- Інтерфейс для систем сторонніх виробників

Сенсор моніторингу

- Засоби виявлення з алгоритмом самонавчання
- Нульовий вплив на мережу
- Доступність в різних версіях

Конфігурація апаратного забезпечення

Центри управління SilentDefense ICS і сенсори моніторингу можуть бути встановлені на самому апаратному забезпеченні, в залежності від того, що саме підлягає моніторингу.

Стандартне апаратне забезпечення

- Стійкість
- Висока ефективність



Для Дата-центрів та кімнат управління



DELL PowerEdge or HP ProLiant

Вбудований ПК

- Відсутність рухомих частин
- Широкий діапазон робочих температур
- Широкий діапазон живлення



Для жорстких умов, таких як виробничі цехи, електричні підстанції і т.д.



SEL 3355 Advantech ARK-3500F

Віртуалізація

- На VMWare ESXi



Для тестового середовища та тимчасового розгортання
Також для розгортання виробництва

Протоколи

- Відкриті ICS протоколи 10+, включаючи IEC 104, DNP3, IEC 61850 (MMS & GOOSE), ICCP, Synchrophasor, Modbus/TCP, EtherNet/IP, MMS, OPC-DA
- Власні протоколи ABB та Siemens
- IT протоколи 20+, включаючи SMB/CIFS та DCOM

Інтеграція з корпоративними системами

- SIM/SIEMs: HP ArcSight (CEF), IBM QRadar (LEEF), McAfee Nitro, Alien Vault, Splunk
- Authentication: Active Directory/LDAP
- Check Point Smart Event
- Syslog

Застосування

SilentDefense ICS побудована задля захисту критичних процесів у всіх секторах автоматизації промисловості та інфраструктури. Потужні та здатні до самонавчання засоби аналізу і виявлення проблем роблять її придатною для використання в різних додатках, таких як:

- Оцінка та аудит мережі
- Моніторинг та захист мережі в режимі реального часу
- Інкрементальні мережі та валідація процесів
- Відповідність міжнародним і регіональним стандартам та керівним вказівкам (наприклад IEC 62443, NERC CIP, NIST і т.д.)



Дистриб'ютор в Україні:

ТОВ «СОЛІТОН» | www.soliton.com.ua

м. Київ, вул. Академіка Туполева, 19

тел. (044) 503-09-20 | e-mail: soliton@soliton.com.ua

SecurityMatters is an international company delivering cutting-edge industrial network monitoring, intelligence and protection technology.

SecurityMatters has installations across two continents in all major critical infrastructure sectors.

SecurityMatters Europe

De Zaale 11, 5612 AJ Eindhoven

SecurityMatters USA

626 E. Broad Street, Ste 200,

Richmond, VA 23219

www.secmatters.com

info@secmatters.com