SILENTDEFENSE™ ОГЛЯД

SilentDefense - це пасивна платформа мережевого моніторингу та аналізу, яка забезпечує миттєву видимість мереж Промислових Систем Управління (ICS) і систем SCADA, та їх захист від кібернетичних загроз.

SilentDefense захищає мережі ICS / SCADA від широкого діапазону загроз. Вона поєднує в собі запатентовану технологію глибокого пакетного огляду (DPI) та бібліотеку з понад 800 ICS-специфічних індикаторів загроз для захисту власників активів від кібератак, неправильних конфігурацій мережі та експлуатаційних помилок.

Інвентаризація активів та карта мережі

- Автоматична інвентаризація активів, комунікацій та вразливостей із повною реєстрацією параметрів пристроїв
- Інтерактивна візуалізація загроз та ризиків

Понад 800 ICS-специфічних показників загрози

- Понад 550 перевірок відповідності протоколу IT/ICS
- Більше 250 елементів управління мережею ICS, загрозами та ризиками в роботі та кібербезпеці

SDK для перевірки користувача

- Повний SDK для специфікації мережевих і технологічних перевірок
- Можливість подовжити підтримку протоколів під час виконання

Аномалії в мережевих та технологічних процесах

- Детальний DPI для протоколів IT & OT, моніторинг до обробки значень
- Самоналаштування, легка настройка мережі та обробка білих списків

Журнал реєстрації подій та аналізу

- Ведення журналу віддаленого доступу та аутентифікації, зв'язку DNS та файлових операцій
- Настроювані графіки та віджети для аналізу тенденцій та подій

Framework пошука загроз

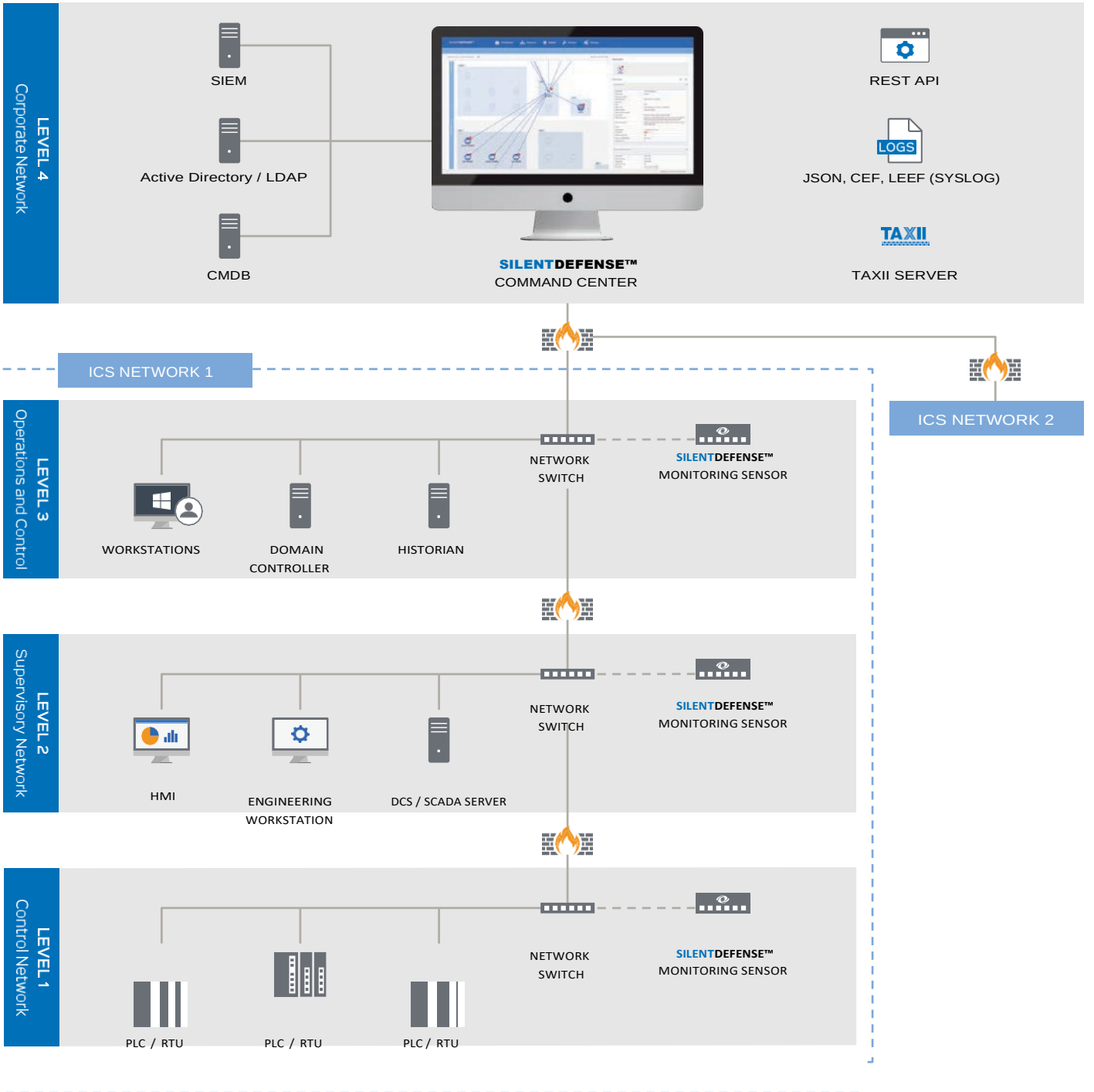
- Детальний пошук ознак інцидентів в трафіку мережі та протокольних повідомленнях
- Постійне повне завантаження трафіку для аналізу його в режимі реального часу

Панель інструментів та звітність

- Поточна та минула історія активності мереж та пристроїв
- Розгорнуті сповіщення про помилки, для всебічного аналізу інциденту та його причин

Компоненти та архітектура

SilentDefense дозволяє оглядати всю мережу ICS на одному екрані. Вона розгортається за лічені години, через підключення Сенсорів моніторингу до порту SPAN чи дзеркального порту мережевих комутаторів, які здатні передавати інформацію про активи, потоки та загрози в реальному часі до Командного центру. SilentDefense взаємодіє з корпоративними системами, такими як рішення SIEM, сервери аутентифікації та сторонні платформи.



Доступні конфігурації

В SilentDefense Командний центр та Сенсори моніторингу можуть бути надані в різних конфігураціях:

- Для розгортання у виробничому середовищі Командний Центр може бути встановлений на стійковому сервері або гіпервізорі VMware ESXi, тоді як Сенсори моніторингу встановлюються на спеціальне устаткування.
- Для розгортання в лабораторному середовищі та демонстрації, Командний центр та один Сенсор моніторингу можуть бути надані як фізично, так і віртуально в комплектній конфігурації.

Командний центр також пропонується в налаштуваннях високої доступності.

Вимоги Командного центру

	Мале розгортання (до 5 сенсорів)	Середнє розгортання (до 20 сенсорів)	Велике розгортання (більше 20 сенсорів)
Модель / гіпервізор	 vmware		
Форм-фактор	Стійковий сервер 19” або віртуальний пристрій		
Процесор	4-core (Intel) CPU 64 bits	6-core (Intel) CPU 64 bits	6-core (Intel) CPU 64 bits ≥ 2.4GHz
Розмір пам'яті	≥ 12 GB	≥ 16 GB	≥ 32 GB
Жорсткий диск	500 GB - 1 TB		
Інтерфейс управління	Інтерфейс для зв'язку сенсорів та доступу до web-програм		

Вимоги Датчиків моніторингу

	Мале розгортання (до 20 Mbps)	Середнє розгортання (до 500 Mbps)	Велике розгортання (до 1 Gbps)
Приклад моделі			
Опис розгортання	Розгортання в малих мережах та агресивному середовищі	Розгортання в середніх мережах та агресивному середовищі	Розгортання в великих мережах та центрах обробки даних
Форм-фактор	Промисловий PC малого розміру/ Кріплення на DIN-рейку	Промисловий PC середнього розміру	Стійка сервера 19” 1U
Процесор	2- or 4- core (Intel) CPU 64 bits	6-core (Intel) CPU 64 bits	6-core (Intel) CPU 64 bits ≥ 2.4GHz
Розмір пам'яті	≥ 4 GB	16 GB	≥ 16 GB
Жорсткий диск	64 GB - 500 GB		
Інтерфейс моніторингу	До 4 портів моніторингу	До 4 портів моніторингу	До 8 портів моніторингу
Інтерфейс управління	Інтерфейс керування сервером та підключенням до Командного центру		

Протоколи

SilentDefense підтримує аналіз та детальну інспекцію пакетів (DPI) протоколів IT та OT, які наведені в таблиці нижче. Додаткові протоколи можуть бути інтегровані на постійній основі за запитом клієнтів.

Стандартні OT протоколи	Власні OT системи / протоколи	IT протоколи
• BACnet	• CSLib (ABB 800xA)	• AFP
• DNP3	• DMS (ABB AC 800F)	• BGP
• EtherNet/IP + CIP	• MMS (ABB AC 800M)	• DHCP
• Foundation Fieldbus HSE	• PN800 (ABB)	• DNS
• IEC 60870-5-104	• ADS/AMS (Beckhoff)	• FTP
• ICCP TASE.2	• CygNet SCADA (CygNet)	• HTTP
• IEC 61850 (MMS, GOOSE, SV)	• DeltaV (Emerson)	• IMAP
• IEEE C37.118 (Synchrophasor)	• Ovation (Emerson)	• Kerberos
• Modbus/TCP	• SRTP (GE)	• LDAP
• OPC-DA	• Experion (Honeywell)	• LDP
• OPC-AE	• ADE (Phoenix Contact)	• MS-SQL
• PROFINET (RPC, RTC, RTA, DCP and PTCP)	• CIP extensions (Rockwell/AB)	• NTP
	• OASyS (Schneider Electric)	• NetBIOS
	• Modbus/TCP extensions (Schneider Electric)	• OpenRDA
	• Telnet extensions (SEL)	• POP3
	• Step7 (Siemens)	• PVSS
	• S7COMM+/OMS+ (Siemens)	• Radius
	• Vnet/IP (Yokogawa)	• RDP
		• RFB/VNC
		• RPC/DCOM
		• RTSP
		• SMB / CIFS
		• SMTP
		• SNMP
		• SSDP
		• SSH
		• SSL
		• SunRPC
		• Telnet
		• TFTP




SECURITY MATTERS

SecurityMatters empowers critical infrastructure and manufacturing organizations with the ability to identify, analyze, and respond to industrial threats and flaws, minimizing troubleshooting costs and unexpected downtime. We leverage ICS-specific knowledge and understanding to provide visibility into critical assets and their activity, and detect operational problems and cyber security threats. Our revolutionary network monitoring platform has been successfully deployed by customers worldwide.

www.secmatters.com | info@secmatters.com