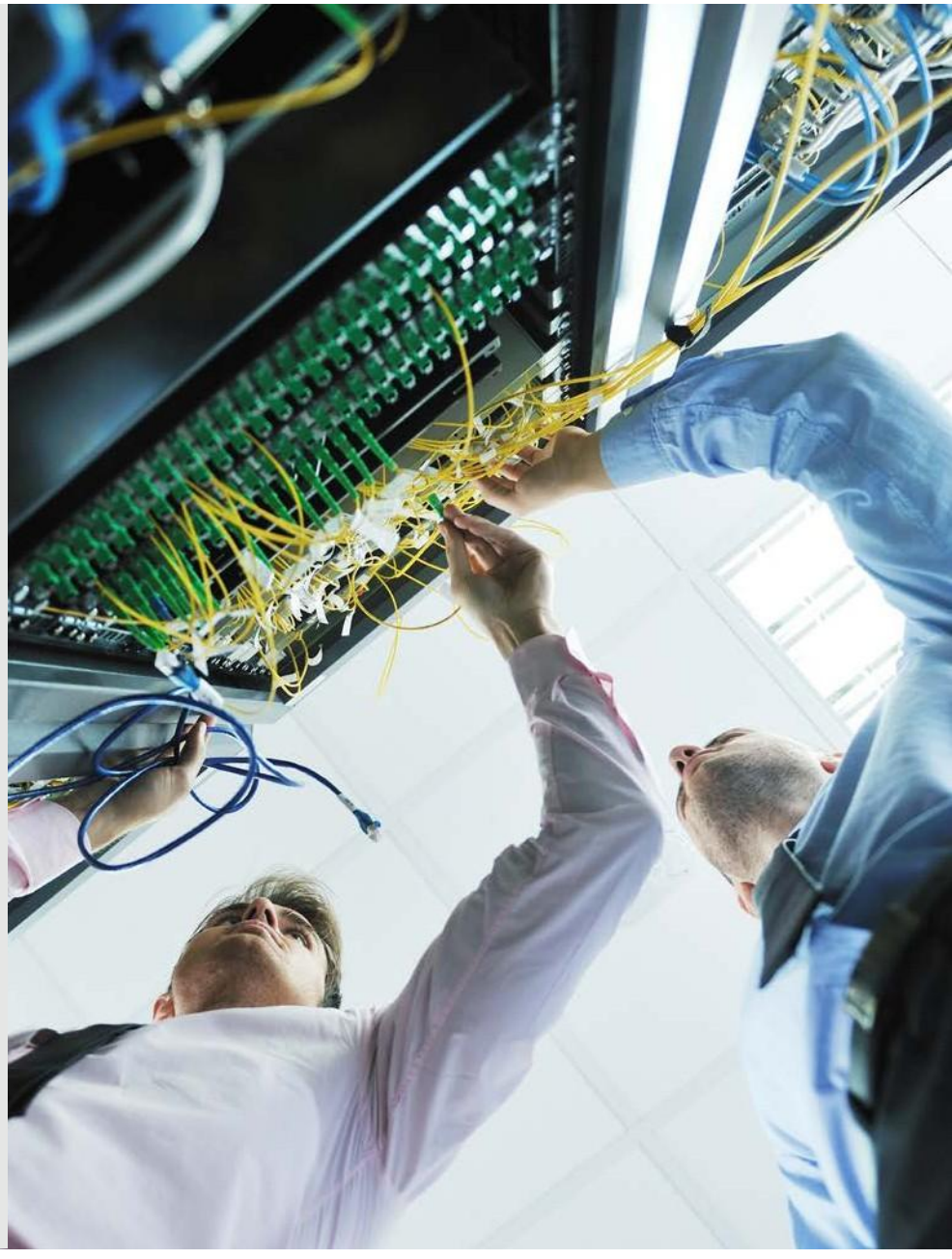
Інтеграція брандмауера Phoenix Contact mGuard з SilentDefense

Запобігання небажаному доступу та виявлення проблем в роботі і кібер-загроз для максимальної стійкості промислових мереж

Основні моменти

- Брандмауер Phoenix Contact mGuard дозволяє доступ до критичних мереж та систем лише авторизованим користувачам та службам.
- SilentDefense – платформа компанії SecurityMatters для пасивного моніторингу мережі, що виявляє проблеми в роботі, можливі кібер-загрози та сповіщає про них.
- Їх поєднання покращує рівень безпеки та стійкості мережі і значно скорочує час незапланованих простоїв та витрати на вирішення проблем.



Проблема

Четверта промислова революція внесла суттєві зміни у формування та управління промисловими мережами. Застарілі системи та протоколи замінюються комерційними (COTS) взаємопов'язаними пристроями та стандартними комунікаційними технологіями. Незважаючи на великі комерційні переваги, ця тенденція призвела до створення більш складних та різнорідних виробничих мереж, які працюють з **підвищеним ризиком виникнення проблем.**

Це призводить до кібер-атак та операційних інцидентів, що зазнали німецька металургійна фабрика в 2014 році, кілька виробників автомобілів у 2017 році та багато інших промислових об’єктів щодня. З сотнями пристроїв від різних постачальників стало важче підтримувати управління доступом до систем та інформації, відстежувати процеси та активність в мережі та ідентифікувати джерела несправностей. Незважаючи на це, необхідно забезпечувати безперервність роботи та рівень її продуктивності, а для цього мережа та її пристрої повинні бути захищені від несанкціонованого доступу та посилення зовнішніх та внутрішніх загроз.

mGuard

Компанія Phoenix Contact, як один зі світових лідерів та інноваторів у сферах електрифікації, електроніки та автоматики має розташований в Берліні центр досліджень з кібербезпеки. Опираючись на багаторічний досвід роботи в цьому середовищі, компанія розробляє індивідуальні продукти та рішення для мереж, завдяки яким реалізуються спеціальні вимоги для промислових об’єктів. Основою лінійки продукції для кібербезпеки є FL mGuard, що включає в себе серію промислових маршрутизаторів та брандмауерів.

Розгортання та Експлуатація

Пристрій mGuard пропонує універсальні функції маршрутизації, брандмауер з перевіркою стану та спеціальними розширеннями для використання в промисловості, а також модулі глибокого пакетного огляду (DPI) та функції VPN (Virtual Private Network). Пристрої захисту виготовлені без вентилятора та доступні в різних варіантах: для встановлення на DIN-рейку, PCI (e)-карта, десктоп або 19” сервер, що дає змогу використовувати їх в різних галузях промисловості. Продукти mGuard ідеально підходять для розподіленого захисту та безпечного дистанційного обслуговування виробничих цехів та окремих машин. Засоби техніки безпеки дозволяють реалізувати концепцію «Захист в глибині» на основі міжнародних стандартів ISA 99 та IEC 62443. Завдяки концепції децентралізованого захисту, виробничі потужності надійно захищені від саботажу виробничого процесу та пов'язаних з ним несправностей.

SilentDefense

SilentDefense - найсучасніша і досконала платформа моніторингу мережі та аналізу ситуації для промисловості. Вона використовує можливості Deep Packet Inspection (DPI) та бібліотеку з більш ніж **800 ICS-специфічних індикаторів загроз** (Industrial Threat Library™) для аналізу промислових протоколів та оповіщення в режимі реального часу про будь-які загрози безперервності робочого процесу. Наприклад такі, як проблеми з підключенням до мережі, несправність пристрою чи неправильна конфігурація, небезпечні робочі операції, використання незахищених протоколів та облікових даних по замовчуванню, розширених кібер-атак та спроб зламів.

Розгортання та Експлуатація

Платформа SilentDefense є «пасивним» рішенням, а тому не гальмує роботу та не впливає на мережу ,що контролюється та її пристрої. Система розгортається за лічені години і забезпечує безпосередню видимість існуючих проблем та загроз. SilentDefense використовує запатентовану технологію виявлення порушень, що дозволяє користувачам встановлювати базову мережеву комунікацію, мінімізуючи зусилля по конфігурації мережі. Для досягнення повного захисту мережі та ефективного реагування на існуючі та виникаючі загрози, інструменти SilentDefense можуть активуватися користувачем вибірково.

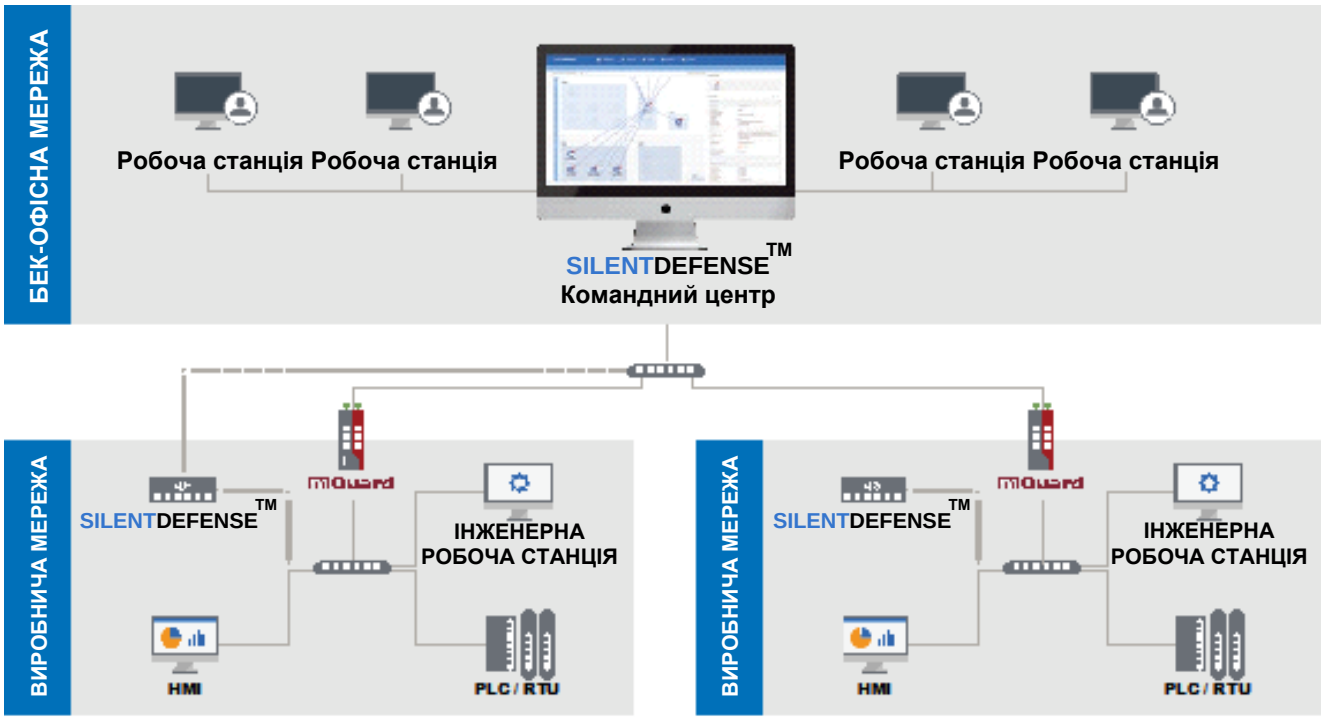
mGuard & SilentDefense

Інтеграція mGuard з SilentDefense робить промислові мережі більш стійкими до кібер-атак та дає користувачам змогу швидко ідентифікувати та реагувати на мережеві збої та неправильні налаштування. Брандмауери mGuard захищають критичні мережі та пристрої від несанкціонованого доступу блокуючи всі повідомлення від нелегітимних пристроїв та не дозволяючи внутрішнім системам підключатися до шкідливих зовнішніх серверів. SilentDefense доповнює цей захист, відслідковуючи спроби вторгнення та інші можливі причини порушення робочого процесу.

Функції автоматичного конфігурування та розширені можливості виявлення загроз SilentDefense надають цій інтеграції додаткові переваги. Здатність SilentDefense автоматично генерувати «білий» список правил мережі може використовуватись для прискорення стартового налаштування mGuard або для налаштування правил брандмауера після зміни конфігурації процесу. Інтеграція також може блокувати зв'язок при виявленні нових загроз і тимчасово блокувати доступ до мережі з некритичного сервера, який здається пошкодженим.

Переваги Інтеграції

- Повна видимість мережі та пристроїв
- Захист критичних мереж та пристроїв від несанкціонованого доступу
- Мінімізація векторів атаки
- Більш швидке налаштування конфігурації брандмауера та реакція на зміни в ній
- Виявлення мережевих та операційних загроз на ранньому етапі
- Спрощений аналіз основних причин проблем та інцидентів
- Динамічна реакція (блокування) на виникаючі загрози і їх джерела
- Зменшення часу вирішення проблем, усунення недоліків та витрат на це
- Максимальні тривалість та продуктивність роботи
- Відповідність міжнародним стандартам та найкращим методам забезпечення захисту (наприклад IEC 62443 та NIST Cybersecurity Framework)



[1] https://ics.sans.org/media/ICS-CPPE-case-Study-2-German-Steelworks_Facility.pdf

[2] https://www.forbes.com/sites/peterlyon/2017/06/22/cyber-attack-at-honda-stops-production-after-wannacry-worm-strikes/#1ab5c91c5e2b

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