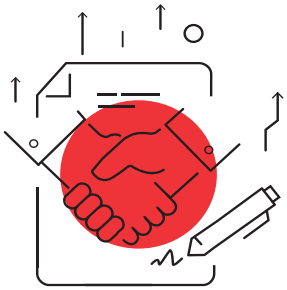


ПОПЕРЕДЖЕНИЙ - ОТЖЕ, ОЗБРОЄНИЙ!

СКАНЕР ВРАЗЛИВОСТЕЙ ДЛЯ КОМПАНІЇ УКРНАФТА



ІСТОРІЯ УСПІХУ

Канали зв'язку, вузли, сервери, робочі станції, бази даних, прикладне та системне програмне забезпечення, а також, дані - цінність для компанії будь-якого масштабу, яку потрібно захищати і правильно зберігати.

З розвитком інформаційних систем, зростає і кількість вразливостей. Надійний захист забезпечує правильно побудована система кібербезпеки, однією із складових якої є ідентифікація потенційних ризиків і виявлення загроз, перш ніж ними зможуть скористатися зловмисники. Для виявлення слабких місць вручну потрібні особливі знання, великий досвід і рідкісне чуття, а ще час та ресурси, оскільки це надзвичайно складний процес.

Більш продуктивний спосіб - автоматичні сканери, які дозволяють значним чином оптимізувати використання ресурсів для пошуку вразливостей. Сканери автоматизують аудит безпеки та аналізують вашу мережу на предмет потенційних ризиків для системи. Також вони можуть розміщувати ризики за пріоритетністю впливу, описувати вразливості і вживати заходи щодо їх усунення.

ПРО ПРОЕКТ

Замовник: ПАТ «Укрнафта»
Галузь: Нафтова промисловість
Рік: 2020
Масштаб проекту: 9 географічно-рознесених локацій по території України

ЗАМОВНИК

ПАТ «Укрнафта» – компанія №1 в Україні з нафтовидобувної промисловості, що володіє однією з найбільших мереж заправних станцій, - 537 АЗС.

Частка товариства у загальному видобутку нафти з газовим конденсатом складає 62,3%, станом на 2019 рік.

UKRNAFTA
УКРНАФТА

ПЕРЕДУМОВИ ПРОЕКТУ

Масштабна діяльність компанії Укрнафта передбачає і наявність у компанії масштабної інфраструктури, яка, до того ж, постійно оновлюється: додаються нові робочі станції, сервери та обладнання.

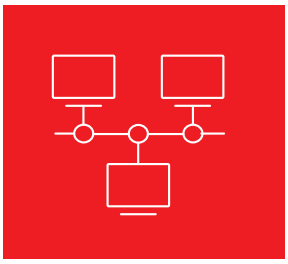
Сканування та пошук вразливостей здійснювалися вручну, лише на особливо критичних об'єктах. Така схема роботи виявилася досить ресурсоємною, потребувала багато часу та уваги з боку працівників. Спеціалізованого рішення з пошуку вразливостей та їхньої ліквідації не використовувалося. Ці проблеми послугували мотивацією до впровадження оптимального рішення з пошуку та усунення ризиків атак.

ЗАВДАННЯ ПРОЕКТУ

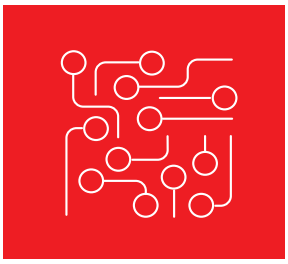
Ключова мета проекту – підвищення загального рівня інформаційної безпеки компанії.

Основне завдання проекту – впровадження надійної системи сканування, що охопила б 9 географічно-рознесених локацій без внесення змін у поточну інфраструктуру, з можливістю усунення знайдених вразливостей та інтеграцією зі сторонніми рішеннями класу SIEM і Service Desk.

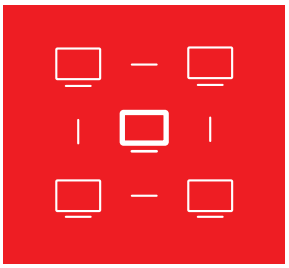
Принципові вимоги до рішення



Мінімальне навантаження на мережу



Інтеграція з наявною інфраструктурою



Можливість **управління** з однієї консолі

РЕАЛІЗАЦІЯ

На старті проекту розглядалися рішення кількох виробників, включаючи й **Rapid7**.
На підставі детального аналізу кожного з них, а також тестового використання різних програмних продуктів було обрано **InsightVM** від **Rapid7**.
Отже, на кожній локації було встановлено Scan Engine, що передає інформацію в єдину консоль управління рішенням.

З консолі налаштовуються політики сканування: глибина, розклад, формування звітів.

RAPID7 INSIGHT VM

Принцип роботи рішення - пошук вразливостей шляхом симуляції атаки в реальному контрольованому середовищі.

Такий підхід дозволяє повністю оцінити усі можливі ризики атак для компанії, виявити та усунути знайдені вразливості.

RAPID7 - лідер в галузі кібербезпеки, що допомагає отримати повне уявлення про безпеку інформаційної інфраструктури організації, шляхом розробки рішень для пошуку та управління вразливостями, тестуванням на проникнення.

Компанія надає послуги більш ніж 9 100 клієнтам по всьому світу, в тому числі 45% із списку Fortune 100. зі зниження ризиків, зупинення атак і вдосконалення процесів безпеки.

Платформа **Rapid7 Insight** об'єднує в собі бібліотеку **Rapid7**, робота якої спрямована на дослідження вразливостей, глобальної поведінки зловмисників, та формування звітності в режимі реального часу, щоб забезпечити повністю доступний, масштабований і ефективний спосіб збору даних про вразливості і отримання відповідей про їхнє усунення.

InsightVM використовує ці дані для аналізу вразливостей і кінцевих точок в реальному часі, шукає шляхи вирішення проблем і мінімізує ризики.

ПЕРЕВАГИ РІШЕННЯ

- Здійснює постійний моніторинг та пошук/виявлення вразливостей з можливістю управління з однієї консолі
- Забезпечує видимість вразливостей в IT-середовищі, включаючи всі види інфраструктур
- Дає можливість індивідуального налаштування процесу щодо усунення знайдених вразливостей
- Дозволяє аналізувати та встановлювати пріоритетність кожної з вразливостей для бізнесу
- Скорочує час на пошук потенційних вразливостей
- Легко інтегрується з вже існуючими сторонніми рішеннями

РЕЗУЛЬТАТИ ПРОЕКТУ

Желудков Олексій, CISO: «Цей проект можна демонструвати у якості прикладу, як це має бути».



- 9 локацій з встановленим Scan Engine рішенням
- єдина консоль управління
- 160 годин проведених робіт
- 1000 IP з перспективою розширення до 4000 IP
- повна інтеграція з наявною інфраструктурою

InsightVM дає чітке уявлення про те, як саме вразливості призводять до бізнес-ризиків і які з них з найбільшою ймовірністю стануть об'єктами атак зловмисників. Аналіз даних про активність і вразливості дозволяє визначити окремі заходи, які можна вжити для зниження ризиків.

Рішення, впроваджене компанією **ITIS** дозволило замовнику побачити цілісну картину функціонування системи безпеки та значно скоротити час пошуку потенційних загроз. І, найголовніше, - здійснювати процес аудиту безпеки далеко за периметр однієї локації.

ПРО ITIS

Найбільш динамічний системний інтегратор України та партнер більше сорока світових вендорів-виробників обладнання та програмних рішень. ITIS надає повний комплекс IT-послуг, від оцінки потреби та проектування рішень до покращення досвіду використання та сервісного обслуговування.

+38 044 334 42 35
marketing@itis.net.ua
itis.net.ua
вул. Кирилівська, 121-а
БЦ «Концепт», Київ