Cortex XDR:

стратегічний інструмент для кібербезпеки сучасного українського бізнесу

Юрій КОРОВАЙЧЕНКО, Deputy Head of Information Security Department SEETON (ТОВ «СІТОН ГРУП»), розповідає про можливості і переваги комплексної платформи кібербезпеки від Palo Alto Networks.

Що об'єднує більшість сучасних компаній?

Для 78% фахівців з кібербезпеки – це щонайменше один кіберінцидент або випадок компрометації конфіденційних даних в IT-системах протягом року. Про це йдеться в аналітичній статті Forrester «Top Cybersecurity Threats in 2024». Паралельно з цим кількість компаній, що зазнали шести й більше інцидентів, зросла на 13% порівняно з 2022 роком – що свідчить про збільшення частоти кібератак і ризик повторних інцидентів.

В цей же час, в умовах повномасштабної війни, українські підприємства стали однією з основних цілей для кіберзлочинців та протистоять безпрецедентній кількості кіберзагроз, що актуалізує потребу в ефективних рішеннях кібербезпеки. Традиційні методи, такі як антивірусні програми, міжмережеві екрани та системи IDS/IPS, вже недостатньо ефективні через складність та комплексність сучасних атак.

У відповідь на ці виклики було розроблено технологію Extended Detection and Response (XDR), що об'єднує дані з різних джерел для комплексного аналізу та ефективного протистояння новітнім кіберзагрозам. Одним з лідерів цього сегмента є платформа Cortex XDR від компанії Palo Alto Networks, яка демонструє високу ефективність у реальних сценаріях застосування.

Що таке Cortex XDR і які його принципи роботи?

Cortex XDR – це розширена платформа для виявлення загроз та інцидентів і реагування на них від Palo Alto Networks, яка виходить за межі традиційних EDR-рішень. Платформа об'єднує дані з кінцевих точок, мереж, хмар та інших джерел у єдину систему аналітики, забезпечуючи деталізований аналіз і ефективне виявлення загроз. Це не просто рішення з кібербезпеки, це — механізм забезпечення безперервності роботи бізнесу, який включає безпечне масштабування, управління ризиками та підвищення операційної стійкості.

Архітектура та можливості платформи Cortex XDR

Архітектура Cortex XDR базується на поєднанні хмарної інфраструктури, агентів на кінцевих пристроях і централізованих інструментів аналітики та реагування (**рис. 1**).

На пристрої користувачів встановлюються агенти, які працюють у фоновому режимі, не створюючи додаткового навантаження. Ці агенти безперервно фіксують інформацію про системні події, поведінку користувачів, активність програм та мережевий трафік. Отримані дані шифруються і передаються до централізованого хмарного сховища Cortex Data Lake для подальшого аналізу.

> *З Cortex XDR інцидент перестає бути «надзвичайною подією» — це чітко визначена ситуація з даними, контекстом і прогнозованими діями. Саме так має працювати XDR.*

Водночас, використовуючи передові методи штучного інтелекту, зокрема машинне навчання та аналіз поведінки, платформа ідентифікує аномальну активність і можливі загрози. Важливим елементом цієї системи є інтеграція з глобальною базою загроз Unit 42, яка регулярно поповнюється актуальними даними про нові типи кібератак, шкідливі програми та вразливості.

Однією з переваг Cortex XDR є автоматизоване реагування на інциденти. Платформа використовує заздалегідь створені сценарії (playbooks), що дозволяють миттєво ізолювати скомпрометовані пристрої, блокувати підозрілі IP-адреси та миттєво сповіщати команди з інформаційної безпеки про потенційні загрози. Це забезпечує швидку локалізацію інцидентів та мінімізує ризик поширення загроз у корпоративній мережі.

Важливим елементом платформи Cortex XDR є вбудована інтеграція не тільки з рішеннями Palo Alto Networks, а й з зовнішніми платформами безпеки, зокрема з рішеннями SIEM і системами автоматизованого реагування SOAR.

Платформа Cortex як основа інтегрованої системи безпеки

Сучасні загрози інформаційній безпеці потребують комплексного та інтегрованого підходу до захисту цифрових активів організації. Платформа Cortex — це ефективне рішення, яке поєднує в собі інноваційні технології аналітики загроз, машинного навчання та автоматизації процесів реагування на кіберінциденти (**рис. 2**). Завдяки повному циклу управління

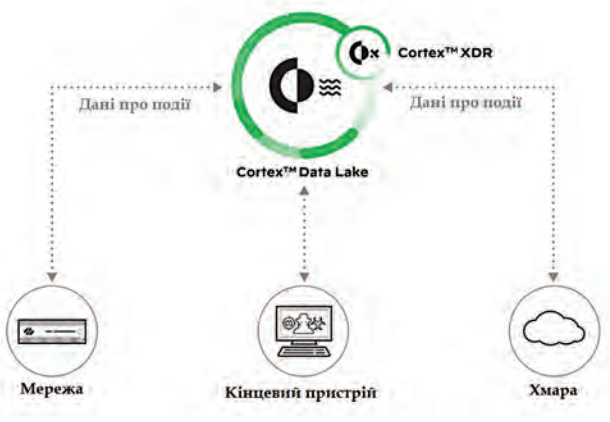

Рис. 1. Архітектура Cortex XDR

Рис. 2. Cortex XDR — платформа повного циклу управління кібербезпекою

безпекою Cortex дозволяє оперативно виявляти загрози, аналізувати потенційні ризики, координувати роботу команд у реальному часі та ефективно захищати робочі станції та сервери компанії. Основні функції платформи охоплюють такі ключові напрямки:

- Security Orchestration & Automation — автоматизоване управління заходами безпеки;
- Case Management — організація керування інцидентами;
- Threat Intelligence — використання актуальних даних про загрози для їх своєчасного виявлення;
- Real-Time Collaboration — забезпечення ефективної взаємодії між членами команд безпеки;
- Investigation & Response — детальний аналіз інцидентів та швидке реагування на них;
- ML-based threat detection — виявлення потенційних загроз за допомогою штучного інтелекту;
- Endpoint Protection — захист пристроїв компанії від атак та шкідливих програм.

Переваги Cortex XDR для українського бізнесу

Впровадження платформи Cortex XDR відкриває суттєві стратегічні переваги для українських компаній, які прагнуть зміцнити власну кібербезпеку та підвищити загальну ефективність бізнес-процесів. Використання даного рішення дозволяє досягти оптимального балансу між високим рівнем захищеності та розумною економією ресурсів, що є особливо актуальним в умовах українського ринку.

Cortex XDR забезпечує такі основні бізнес-переваги.

- Використання інтегрованої платформи дозволяє зменшити витрати на підтримку окремих інструментів кіберзахисту до 30%. Це досягається за рахунок централізації управління та уніфікації процесів безпеки.
- Cortex XDR забезпечує автоматизоване виявлення, аналіз та блокування потенційних кіберзагроз, що суттєво скорочує час на реагування та мінімізує можливі негативні наслідки атак.
- Рішення допомагає компаніям дотримуватись ключових міжнародних нормативів, зокрема стандартів GDPR, HIPAA, а також має експертний висновок ДССЗЗІ. Це дозволяє компаніям впевнено вести бізнес як на внутрішньому ринку, так і на міжнародному рівні, не ризикуючи отримати штрафні санкції чи регуляторні зауваження.
- Своєчасне та ефективне управління кіберінцидентами, що надається Cortex XDR, дозволяє мінімізувати ризики витоку конфіденційних даних та інших наслідків атак, запобігаючи втраті репутації та забезпечуючи високий рівень довіри серед клієнтів і партнерів.

Таким чином, інтеграція Cortex XDR є стратегічним кроком для українських компаній, які прагнуть залишатися конкурентоспроможними, забезпечуючи високий рівень кібербезпеки при оптимальних витратах власних ресурсів.

XSIAM: наступний етап розвитку XDR

Рис. 3. Cortex XSIAM від Palo Alto — платформа кібербезпеки, що поєднує різні інструменти

XSIAM – це платформа від Palo Alto Networks, яка консолідує інструменти кібербезпеки в єдину систему, керовану штучним інтелектом (**рис. 3**). Вона оптимізує роботу центрів безпеки (SOC), об'єднуючи функції XDR, SOAR, ASM (управління поверхнею атак) і SIEM. Завдяки штучному інтелекту XSIAM забезпечує покращене виявлення загроз, автоматизоване реагування та мінімізацію людського фактора.

Наприкінці квітня компанія Palo Alto Networks представила Cortex XSIAM 3.0 – оновлену платформу для SOC. У ній з'явились такі функції, як модуль Cortex Exposure Management, що скорочує хибно-позитивні виявлення вразливостей на 99% за допомогою використання штучного інтелекту, та Cortex Advanced Email Security, що використовує великі мовні моделі штучного інтелекту (LLM) для протидії фішингу.

Завдяки інноваційним рішенням платформа XSIAM залишається лідером у своєму сегменті впродовж двох років свого існування. У 2-му кварталі 2025 фінансового року продажі Cortex XSIAM сягнули $1 млрд.

Комплексна безпека для нової реальності

Cortex XDR – це не просто інструмент для реагування на інциденти, а цілісна екосистема кіберзахисту, яка поєднує аналітику, автоматизацію та гнучке управління загрозами. У контексті українського бізнесу, що працює в умовах зростання кіберзагроз, дане рішення дозволяє суттєво підвищити рівень захищеності без надмірного навантаження на команди кібербезпеки.

У подальшому Cortex XDR може стати основою для переходу до більш комплексного рішення – Cortex XSIAM, яке об'єднує всі дані безпеки в єдину аналітичну систему. Це дозволить не лише оперативно реагувати на загрози та автоматизувати прийняття рішень, а й проактивно запобігати кібератакам завдяки інноваційним технологіям штучного інтелекту.

seeton

А якщо вас зацікавило рішення Cortex XDR або Cortex XSIAM і у вас з'явилося бажання випробувати його у власній інфраструктурі, — напишіть нам на пошту cs@seeton.pro, і команда **CyberSecurity** *компанії* **Seeton** *допоможе вам у проведенні тестування та впровадженні даного рішення.*