Як компанії можуть досягти лідерства в епоху нових кіберзагроз

Пилип Чуйко, співвласник та директор з розвитку бізнесу INTRASYSTEMS — про платформний підхід до кіберзахисту.

Цього року INTRASYSTEMS виповнилось 9 років — 9 насичених і плідних років зростання, нарощення компетенції, постійної адаптації до сучасних реалій, еволюції та здобуття довіри клієнтів. Як системний інтегратор із багаторічним досвідом, ми реалізували багато успішних проєктів разом з лідируючими світовими вендорами, зокрема на базі рішень одного зі світових лідерів у напрямку кіберзахисту — Trend Micro. Завдяки глибокій експертизі та тісній співпраці з цим вендором ми допомагаємо нашим замовникам ефективно виявляти, оцінювати та мінімізувати кіберризики, забезпечуючи стійкість і відповідність вимогам безпеки сьогодення.

У сучасному цифровому світі організації мають справу з небаченим рівнем складності управління комп'ютеризованим середовищем: хмарні сервіси, віддалена робота, IoT, generative AI та, звісно, кооперація з локальною IT-інфраструктурою. Широкий перелік доступних сервісів та способів взаємодії з ними астрономічно збільшує «потенційну поверхню атаки» через використання зловмисниками множинних точок входу та безконтрольне поширення всередині гібридних інфраструктур. У відповідь на ці виклики Trend Micro пропонує компаніям вдосконалити їхню глобальну концепцію побудови системи інформаційної безпеки, забезпечивши перехід від «використання розрізнених інструментів кіберзахисту» до «платформного підходу», при якому всі впроваджені рішення протистояння кіберзловмисникам виступають як складові єдиної уніфікованої платформи кібербезпеки. Завдяки такому підходу дані, зібрані з підзахисної інфраструктури, аналізуються консолідовано, як єдине ціле, чого в принципі не можливо досягнути при використанні окремих продуктів — хоч і високоефективних у своїй ніші, однак все ж різних виробників, — оскільки у цьому випадку кожен з продуктів аналізує події та телеметрію відособлено. А це, в свою чергу, породжує так звані «сліпі зони», багатократні сповіщення на одні й ті самі події та призводить до затримки реагування на кіберінциденти. Аналіз загроз у таких умовах стає повільним, а здійснення заходів протидії кібератакам — малоефективним.

Сервіси на основі штучного інтелекту (ШІ) як виклик і як перевага

Аналізуючи поточні тенденції розвитку виробничих процесів, варто зазначити, що засоби з елементами ШІ вже використовуються не лише захисниками, а й кіберзловмисниками: для розроблення сценаріїв та інструментів кібератак на основі фішингу, «діпфейків», автоматизованого сканування на наявність вразливостей публічних ресурсів тощо. По суті, цей інструмент став могутнім важелем надзвичайно деструктивного масштабування тіньових сервісів надання шкідливого ПЗ та інструкцій за моделлю Crime as a Service, сприяючи реалізації різноманітних кібератак навіть малодосвідченими кіберакторами.

Захист, у свою чергу, має відповідати актуальним викликам, тож повинен бути настільки ж інтелектуальним: автоматизовані алгоритми на основі ШІ, зважуючи численні показники підзахисних інфраструктур, повинні приймати рішення в реальному часі щодо запобігання початку або поширенню кіберактивностей вже без участі людини.

Як це працює на практиці

- **Консолідація даних** з якомога ширшого переліку цифрових активів організацій (кінцевих точок, мереж, пошти, хмарних сервісів, ШІ-асистентів тощо).

- **Інтелектуальна кореляція:** реагування на послідовності подій ще до фактичного залучення шкідливого ПЗ; наприклад, підозріла email-активність + аномальна поведінка пристрою чи корпоративного облікового запису = автоматичне

блокування акаунту та завершення всіх активних сесій/скидання паролю.

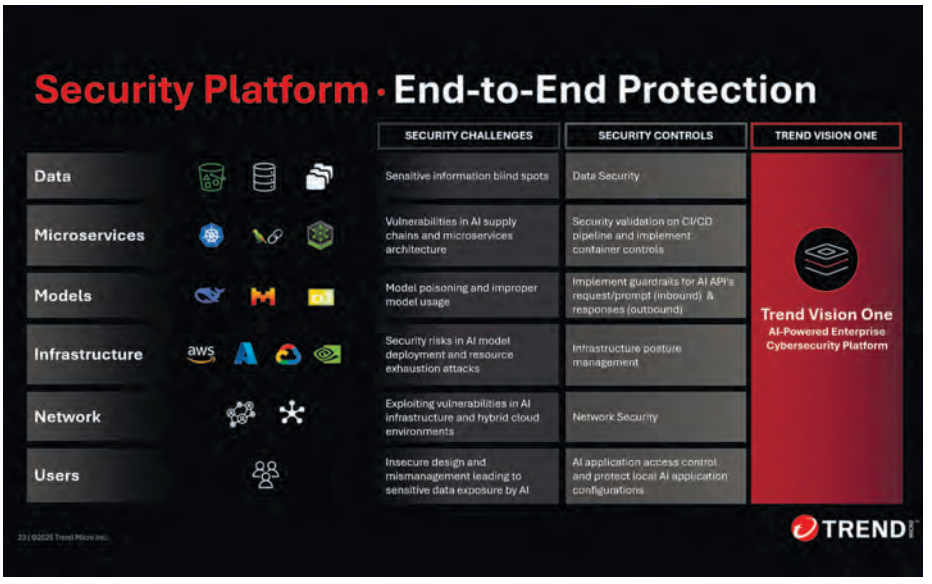
➢ **Превентивні дії:** блокування, ізоляція, зміна політик безпеки — запускаються ще до того моменту, як атака досягне деструктивної фази.

➢ **Оцінювання ризику:** система надає кількісні показники ступеню ризиків як консолідовано по організації в цілому, так і по кожному з виявлених цифрових активів, що надзвичайно важливо для своєчасного корегування та пріоритезації зусиль/ресурсів керівниками департаментів.

Платформний підхід, реалізований у Trend Vision One™, дозволяє зібрати всі компоненти безпеки (endpoints, мережа, хмара, середовища контейнеризації, безсерверні обчислення, електронна пошта, облікові записи, захист взаємодії з платформами ШІ, інші типи активів та пов'язані з ними ризики) в одну централізовану систему, де всі події обробляються як єдине ціле, що значною мірою вдосконалює як технічну сторону, так і адміністрування потенційних кіберризиків та дозволяє вивірено реагувати на інциденти.

Ще одне важливе нововведення, яке було реалізовано у Trend Vision One™ — перехід від «реактивної» до «проактивної» безпеки. Чому ж, власне, «проактивні» інструменти необхідні поряд із «реактивними»?

Реактивні інструменти (EPP/EDR/XDR) важливі, але цього вже недостатньо. Атаки стають надто швидкими та багатогранними, тож для виявлення передумов, що можуть сприяти несанкціонованому зовнішньому впливу — потрібно вживати певного комплексу заходів, які на основі кількісних оцінок поточного стану захищеності інфраструктури зможуть передбачати та пріоритезувати виявлені «слабкі місця». Саме так працює прогресивний сервіс Trend Micro Cyber Risk Exposure Management (C.R.E.M.).



Переваги Trend Micro C.R.E.M.

Безперервне виявлення активів — локальні та хмарні, тіньове IT, облікові записи, поява корпоративних даних у DarkNet і багато іншого (платформа постійно розвивається, зокрема постійно додаються нові інтеграції для інвентаризації).

Оцінювання ризиків у контексті — що важливіше для бізнесу, те й під захистом насамперед.

Прогнозування атак — моделювання та схематична візуалізація векторів проникнення, роз'яснення можливих негативних наслідків у разі НЕусунення виявлених ризиків.

Автоматичне реагування — набір власних засобів у складі Trend Vision One та/або інтеграція з SOAR, ITSM, XDR.

Аудит та відповідність стандартам — зрізи поточного стану захищеності інфраструктури з переглядом динаміки змін протягом минулих часових періодів, уніфіковані звіти для керівництва, перевірка відповідності впроваджених заходів кіберзахисту світовим галузевим стандартам (NIST, PCI-DSS, ISO/IEC, FedRAMP) тощо.

Синергія проактивного та реактивного підходів — основа кіберстійкості

Підхід	Основна функція	Результат
EDR/XDR	Виявляє і ліквідує вже активні атаки	Зменшення шкоди, локалізація інциденту
CREM	Передбачає і запобігає атакам	Усунення ризиків ще до фактичного початку кібератак/інцидентів

Висновок

Майбутнє ринку засобів забезпечення інформаційної безпеки компанія Trend Micro вбачає виключно у переході до «платформного підходу», коли всі елементи екосистеми кібербезпеки становлять «єдине ціле», а аналіз метаданих здійснюється консолідовано. Задля реалізації такого підходу обов'язково необхідно доповнювати наявні засоби «реактивного» захисту — інструментами «проактивного». Побудована у запропонований спосіб екосистема може суттєво мінімізувати потенційні ризики ще до моменту їх фактичного використання кіберзловмисниками, а це, в свою чергу, допоможе у значно ефективніший спосіб використовувати наявні ресурси, що неодмінно сприятиме підвищенню стійкості вашого бізнесу в новій епосі кіберзагроз.

Ми знаємо, що майбутнє — за тими, хто бачить загрози раніше, ніж вони виникають. Співпраця з Trend Micro дозволяє нам пропонувати сучасні механізми кіберзахисту, які працюють на випередження цих загроз. Далі — ще більше інтеграцій, ще більше безпеки.

Зв'яжіться з нами та дізнайтесь, як **Trend Micro** *може захистити саме вашу IT-інфраструктуру!*

info@intrasystems.ua
www.intrasystems.ua

INTRA SYSTEMS