СУЧАСНИЙ ПІДХІД ДО КІБЕРБЕЗПЕКИ

BDO DIGITAL

Кібербезпека стає нагальним питанням для організацій, які швидко впроваджують сучасні технології та переходять у цифровий простір

Організації, які працюють у цифровому середовищі, що постійно розширюється, стикаються зі все більшими складнощами в управлінні технологічно підготовленими працівниками, клієнтами і регуляторами, одночасно захищаючи свої технологічні платформи та дані від кіберзлочинців.

Прискорення вимог і доступних можливостей накладає на організації безпрецедентний тягар з погляду адаптації до швидко мінливих цифрових умов. Йдеться не про одну революційну технологію, а про зближення всієї діяльності людства зі значною цифровою залежністю за дуже короткий проміжок часу порівняно з попереднім століттям.

З погляду безпеки, кожна нова послуга, яку суспільство переміщує в цифровий простір, створює більший ризик для організації. Фахівці та програми з кібербезпеки намагаються не відставати, оскільки підприємства використовують удосконалені технології для прискорення зростання. Цю проблему ускладнюють реалії, пов'язані з набором кадрів з кадрового резерву, де пропозиція нижча, ніж попит, і постійні зусилля, необхідні для утримання наявних цінних кадрів. Ця доза реальності ускладнює організаціям завдання зберегти рівень і підтримати сильний рівень безпеки.

Хороша новина полягає в тому, що технологія, що забезпечує цифрове прискорення (наприклад, хмара) для бізнесу, тепер на шляху до того, щоб забезпечити безпеку в такий же ефективний спосіб. У цій статті досліджуються сфери, де використовується розумна кібербезпека, і як вона надає можливості організаціям захищати свій бізнес як ніколи раніше.

Спільна для нас всіх справа

Існує кілька причин, чому служби і організації у сфері безпеки намагаються оптимізувати правила безпеки. Нижче наведено кілька проблем, з якими стикаються всі організації в нинішньому середовищі:

Надмірно складні рішення – багато рішень можуть бути занадто складними, аби реалізувати їх оптимізованим та осмисленим чином. Неможливість правильно налаштувати та реалізувати рішення часто призводить до того, що організації звертаються до дорогих професійних послуг постачальників або додають технології, які заповнюють прогалини, що може призвести до розповсюдження технологій та збільшення витрат.

Розповсюдження технологій – додавання технологій для заповнення прогалин у візуалізації необхідно ретельно продумати. Чи зможе організація залучати людей та розвивати навички, необхідні для роботи з рішенням, і чи в результаті рішення створює інші проблеми? Чи враховуються витрати під час пошуку нового рішення?

Збільшення витрат – у міру того, як в організації зростають надлишковість і дублювання технологій, зростають і пов'язані з ними витрати на керування ними. Спроби раціоналізувати технології та усунути дублювання стають складними, оскільки інші вимоги бізнесу мають пріоритет. Цикл продовжується, що згодом веде до неефективності, яку ми не можемо собі дозволити, і може створювати сліпі зони у програмі безпеки.

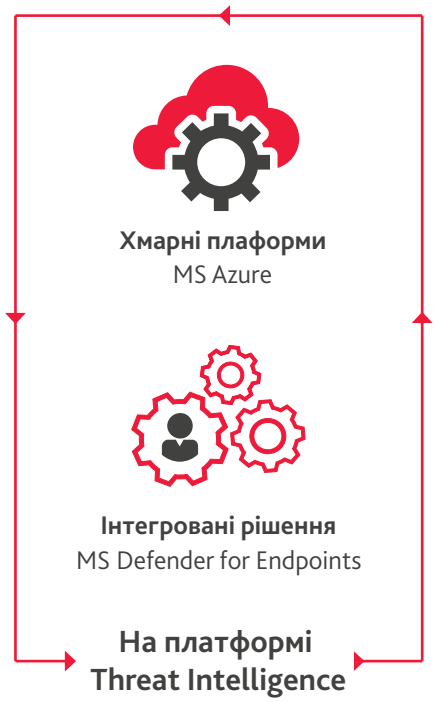
Розвиток навичок – залучення кваліфікованих фахівців з кібербезпеки є проблемою з погляду залучення, навчання та підтримки сильних талановитих кадрів у різних технологіях. Багато факторів є причиною дефіциту ресурсів безпеки, включно з браком кваліфікованих фахівців, зростаючим попитом, відсутністю попередніх інвестицій в бізнес, вигоранням персоналу через нестачу кадрів, збільшенням обсягу та складності загроз, а також новими викликами, пов'язаними з більшою автоматизацією та віддаленою роботою.

Втома від сповіщень – служби безпеки витрачають занадто багато часу на відстеження сповіщень, що призводить до неефективності. Це часто є результатом неправильного налаштування датчиків або занадто широких порогів сповіщень. Неузгоджене відстеження завдань з низькою пріоритетністю відволікає команди від сповіщень, збільшуючи ризик порушення та плинності кадрів.

Справа, описана вище, є широко розповсюдженою у сфері кібербезпеки. Організації швидко усвідомлюють, що жоден постачальник чи рішення не можуть монополізувати ринок з погляду усунення всіх ризиків. Однак за допомогою підходу до програмування забезпечення безпеки, що ґрунтується на оцінці ризику, можна отримати значну перевагу в безпеці, використовуючи потужні технології (наприклад, Microsoft Security Solutions), потужні процеси (наприклад, управління інцидентами) і сильні кадри (наприклад, кваліфіковані фахівці з роботи з інструментами).

ЩО МОЖЕ ЗРОБИТИ ОРГАНІЗАЦІЯ?

Сучасні хмарні платформи, штучний інтелект і рішення з підтримкою інтелекту допомагають організаціям здобути впевненість і ще більше знизити ризики, використовуючи простоту та доступність безпеки в сучасному IT-середовищі. Ця конвергенція забезпечує безпрецедентний рівень можливостей кібербезпеки. Далі в цій статті описано, як новітні технології змінюють парадигму і як розумні процеси можуть полегшити навантаження без великих витрат і складнощів.



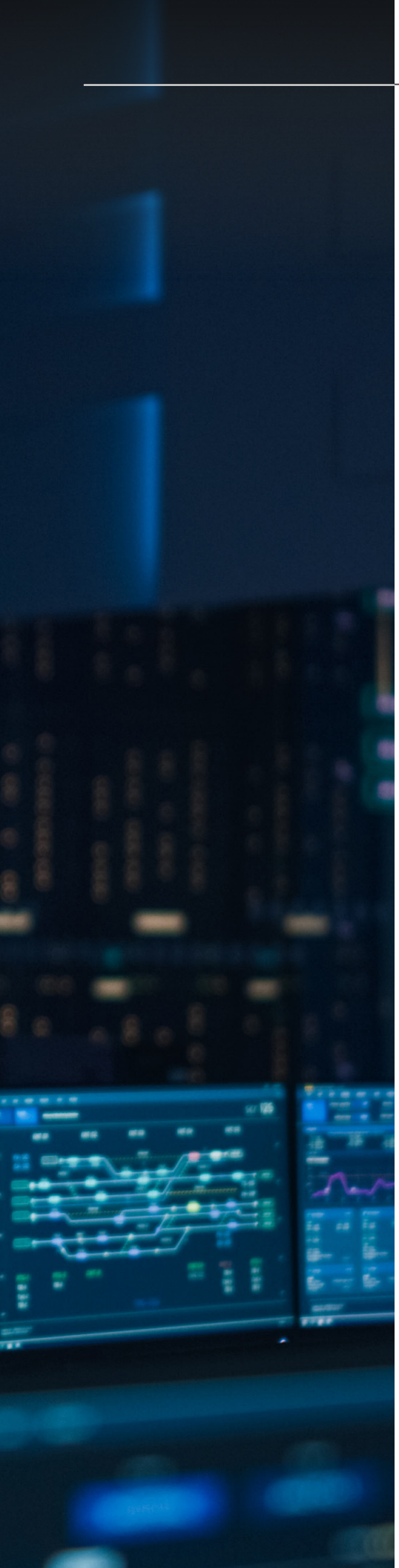
НОВІ МОЖЛИВОСТІ МОЖУТЬ ДОПОМОГТИ

Хмарні платформи – вибір найкращої у своїй категорії хмарної платформи, такої як Microsoft Azure, є наріжним каменем для створення сучасної, доступної та функціональної програми хмарної безпеки. Важко переоцінити лідерство хмарної платформи в операціях з безпеки. Постачальники таких послуг пропонують клієнтам найсучасніші стандарти і методи безпеки, надаючи перевагу можливостям виявлення платформи, а не стороннім постачальникам, не кажучи вже про бюджет для надання комплексних рішень. Важко зробити так, щоб інші постачальники рішень могли знати більше про Microsoft Azure, ніж про Microsoft.

Інтегровані рішення. Визначення необхідності відходу від виявлення на основі сигнатур і до виявлення на основі поведінки, щоб забезпечити більш глибокий рівень видимості, постачальники рішень інтегрували свої можливості, щоб зробити їх розумнішими та надійнішими, що призводить до кращих результатів. Виявлення та відповідь кінцевої точки (Endpoint Detection & Response,EDR) є прикладом інтегрованої технології, де кореляція та виявлення підозрілої активності відбувається поза центральним рішенням Управління інформацією та подіями безпеки (Security Information and Event Management, SIEM). Зосереджуючись на поведінці кінцевих точок, проти сигнатур і наповнюючи це інформацією про загрози, якість сповіщень і впевненість сповіщень підвищуються.

Розвідка про загрози. Правильне використання інформації про загрози допомагає організаціям визначити пріоритетність інвестицій в безпеку, оскільки воно дає уявлення про найбільш ймовірні та найнебезпечніші загрози, з якими стикається організація. Ця обізнаність і визначення пріоритетів допомагають керувати тим, на чому слід зосередити ініціативі й інвестиції в кібербезпеку, щоб підвищити рівень безпеки, прискорити усунення проблем та інформувати нас про атаки, які могли залишитися непоміченими.


Scr 125



ПРАКТИЧНИЙ ПІДХІД ДО ЗМЕНШЕННЯ НАВАНТАЖЕННЯ

Ми часто бачимо, що організації використовують короткостроковий тактичний підхід під час надання можливостей безпеки. Зазвичай це відбувається на основі реагування на порушення, аудитів, порад постачальників або професійних послуг тощо. Цей підхід несе значний ризик з погляду загальної ефективності, витрат, укомплектованості персоналом, і може призвести до зниження рівня безпеки.

BDO Digital пропонує наступний підхід до забезпечення безпеки організації.

Проведення розслідувань. Насамперед, необхідно вирішити, чи є у вас доступ і можливості для ефективного розслідування та вжиття заходів щодо будь-якої проблеми безпеки, про яку вам стало відомо. BDO Digital готує середовище щодо цього, щоб забезпечити наявність, доступність і своєчасність інформації, необхідної для відстеження загроз.

Визначення пріоритетів інтегрованих сповіщень. Пріоритет віддається найточнішим та найінтегрованим наборам технологій, щоб забезпечити максимальну видимість у максимально широкій апертурі. Ми віддаємо пріоритет інтегрованим технологіям, таким як хмарні платформи, EDR та рішення, які містять фільтрацію інформації про загрози.

Поліпшення операційних процесів. Для того, щоб допомогти забезпечити якість, стійкість і хороші організаційні результати, однією з важливих сфер є вимога до внутрішнього процесу. За наявності якісних сповіщень, організація має бути готова до дій. Наприклад, без задокументованого та зрозумілого процесу реагування на інциденти безпеки, організаціям може знадобитися більше часу для стримування та відновлення.

Розширені сценарії використання. Після того, як основні принципи надійно встановлені, BDO Digital розширює апертуру безпеки, додаючи додаткові рівні спостереження, такі як застосунки, бізнес-логіка або інсайдерські загрози. Ми розгортаємо індивідуальні сценарії використання, щоб виявити загрози на всіх поверхнях атак, що може максимально збільшити контроль подій безпеки в організації.

Забезпечення стійкості. BDO Digital постійно оцінює ринок, використовуючи набір технологій, щоб забезпечити максимальну ефективність, результативність і цінність для клієнтів. Забезпечення стійкості є основним аспектом підтримки відповідного рівня безпеки, відповідної кваліфікації та інструментаріїв. Поглиблений захист має вирішальне значення для успіху будь-якої програми безпеки, тому знати, коли слід змінити конфігурацію або замінити технологію на основі ситуації на ринку та конкретного положення організації, дуже важливо.

Суттєвого поліпшення вже можна досягти і воно відбувається. Розумніші технології повністю змінюють підхід галузі до безпеки. Сучасні програми безпеки змінюються швидше, ніж будь-коли, а використання сучасних технологій разом з розумним підходом і досвідченими консультантами, такими як BDO Digital, допомагають прискорити темпи змін і вдосконалення для тих, хто це приймає.

КОНТАКТИ

БРЕД ЕЛЛІСОН
Керуючий директор, Група керованих послуг
630-286-8196 / bellison@bdo.com
СТІВ КОМБС
Директор групи щодо інфраструктурних рішень
713-576-3417 / scombs@bdo.com
АНДРІЙ БОРЕНКОВ
Директор БДО Консалтинг в Україні
+380 50 380 96 01 / aborenkov@bdo.ua

РОККО ГАЛЛЕТТО
Партнер, керівник національної кібербезпеки
BDO Lixar
416-729-2609 / rgalletto@bdo.ca
РОБ ФІЛПОТТС
Директор відділу управління кіберзагрозами
BDO Lixar
437-237-3502 / rphilpotts@bdo.ca