Рішення Carbon Black EDR – відтепер частина Broadcom!

Компанія Broadcom об'єднала портфелі продуктів кіберзахисту Carbon Black і Symantec. Про переваги від цього об'єднання і про можливості одного з ключових рішень, Carbon Black EDR, розповідає Денис БАЗИЛЬСЬКИЙ, керівник департаменту Pre-sale компанії Oberig IT.

Восени 2023 року було остаточно закрито угоду щодо придбання VMware техногігантом Broadcom: згодом її назвали однією з найбільших IT-угод в історії. Разом із продуктами VMware до портфеля Broadcom додались рішення з кіберзахисту під брендом **Carbon Black**, якими володіла VMware.

Синергія Carbon Black і Symantec

До основних технологій, які використовуються у рішеннях Carbon Black, належать: **EDR** (Endpoint Detection and Response) – виявлення та реагування на загрози на кінцевих точках з використанням поведінкової аналітики; **NGAV** (Next-Gen Antivirus) – антивірус наступного покоління, що запобігає атакам за допомогою штучного інтелекту та машинного навчання; **App Control** – технологія білих списків для блокування неавторизованого ПЗ; **хмарна безпека** – інтеграція з хмарними середовищами для моніторингу та захисту віртуальних машин і робочих навантажень; та **аналіз загроз у реальному часі** – постійний моніторинг і збирання даних для швидкого реагування на інциденти. Ці технології забезпечують всебічний захист від сучасних кіберзагроз та дозволяють значно підсилити захищеність інфраструктури організацій.

Наразі Broadcom об'єднує два своїх портфоліо – Carbon Black і Symantec – для забезпечення повної гібридної хмарної кібербезпеки та створює новий підрозділ Enterprise Security Group. Обидва бренди орієнтовані на інновації та прагнуть надавати перевірені рішення з кібербезпеки та їх підтримку, вони створені для вирішення унікальних і вкрай складних завдань, що постають перед великими корпоративними клієнтами, які належать до сфер діяльності з найжорсткішим державним регулюванням. Broadcom робить значні інвестиції в обидва бренди і продовжить пропонувати обидва портфелі в рамках бізнес-підрозділу Enterprise Security Group, щоб допомогти захистити найбільші та найсучасніші підприємства світу.

Портфоліо Symantec, до якого входять одні з найкращих у світі технологій у галузі безпеки, зосереджене на захисті даних та мереж, тоді як щойно придбане портфоліо Carbon Black спеціалізується на виявленні загроз на кінцевих точках та реагуванні на них (EDR), а також на управлінні застосунками. Посилення Carbon Black телеметрією мереж та даних забезпечить користувачам більше прозорості та контролю. В рамках підрозділу Enterprise Security Group підприємства продовжуватимуть отримувати найкращі послуги з ще більшою, ніж дотепер, кількістю виділених ресурсів і цілеспрямованою підтримкою. Чого можна очікувати в найближчій перспективі? Давайте ближче познайомимося з планами та інноваціями.

Інновації

Фінансова стабільність Broadcom дає змогу впроваджувати масштабні інновації у продукти з портфоліо як Symantec, так і Carbon Black. Від цього виграють користувачі, які матимуть доступ до покращеного портфоліо корпоративного рівня та передових технологічних досягнень із неперевершеними сервісом і підтримкою.

Спочатку Broadcom інвестуватиме в дослідження та розробки (R&D) для покращення продуктів, що їх використовують клієнти як у локальних інфраструктурах, так і в гібридних хмарах, і продовження терміну експлуатації цих продуктів. Оскільки бренди доповнюють один одного, завдяки синергії технологій відкриваються нові можливості. Наприклад, Symantec має продукт для захисту традиційних робочих навантажень у датацентрах, а Carbon Black – додаткові рішення, такі як EDR, App Control та NGAV. Маючи доступ до обох наборів рішень, можна буде зробити захист інфраструктури ще кращим та якіснішим.

Що таке EDR?

Кіберзлочинці постійно вдосконалюють свої методи, тож організації стикаються з усе новими викликами щодо захисту своїх даних і інфраструктур. Зростає кількість складних загроз, таких як атаки з використанням штучного інтелекту, багатоступеневі атаки та новітні варіанти шкідливого ПЗ, які здатні обходити традиційні системи безпеки. Окрім цього, загрози націлюються на найбільш вразливі місця – кінцеві точки, через які зловмисники можуть отримати доступ до всієї корпоративної мережі. У відповідь на ці виклики з'явилися рішення типу EDR, які не лише запобігають атакам, але й забезпечують швидке виявлення і нейтралізацію загроз у реальному часі, допомагаючи організаціям ефективніше захищати свої активи.

EDR – це інтегроване рішення для захисту кінцевих пристроїв, яке поєднує безперервний моніторинг і збір даних з ендпойнтів у реальному часі з автоматизованим реагуванням та аналітичними можливостями на основі правил. EDR є другою лінією захисту після традиційних антивірусів, а також антивірусів нового покоління, що стає дедалі необхіднішим,

оскільки зловмисники використовують просунуті методи для обходу первинних засобів захисту.

EDR дозволяє командам безпеки швидко виявляти складні атаки та реагувати на них, розуміти, як зловмисники отримали доступ до системи, і налаштовувати політики для запобігання подібним атакам у майбутньому.

Як працює EDR

Розгляньмо основні сценарії використання систем EDR.

1. Реагування на інциденти

Швидка та впевнена реакція на виявлені інциденти безпеки (Incident Response, IR) може бути вирішальною для зменшення збитків для бізнесу. Належні стратегії та тактики реагування на інциденти є критично важливими для обмеження масштабу атак. Згідно зі «Звітом про збитки через витоки даних у 2023 році» від IBM, найбільш ефективною стратегією для швидшого виявлення та реагування є створення команди IR і тестування IR-плану перед його впровадженням. Це може зменшити час виявлення на 54 дні.

Рішення EDR можуть дуже допомогти, постійно записуючи та зберігаючи дані про активність кінцевих пристроїв, що надає вашій команді IR систему для відстеження доказів загроз і виявлення патернів поведінки.

2. Дистанційне відновлення

Після виявлення загрози дуже важливо діяти швидко та рішуче. Це може бути проблематично, якщо члени команд безпеки працюють з різних місць, зокрема з дому. Запитайте постачальників EDR, чи дозволяють їхні рішення безпечно та швидко виконати повне розслідування та здійснити відновлення з будь-якої точки світу. Найкращі рішення використовують хмарну архітектуру для надання адміністраторам віддаленого доступу, що забезпечує видимість кожного кінцевого пристрою в організації.

Рис. 1. Приклад візуалізації атаки та розслідування, частина криміналістичного дослідження з використанням Carbon Black EDR

3. Сортування та візуалізація сповіщень

Учасники команди SOC підтвердять, що втома від сповіщень – це серйозна проблема. Однією з найважливіших функцій для її подолання є візуалізації, які дають змогу аналітикам сортувати сповіщення. Правильні інструменти дозволяють швидко розуміти, що сталося під час атаки, і налаштувати політики для запобігання повторенню подібних атак. Вивчайте можливості візуалізації сповіщень, які пропонують постачальники EDR.

4. Полювання на загрози

Полювання на загрози (threat hunting) – це проактивний пошук у публічних і приватних хмарах, мережах та на кінцевих пристроях індикаторів компрометації (IOC), які можуть свідчити про злам або вторгнення. Для оптимізації процесу полювання на загрози шукайте рішення, які збирають дані та розвідувальну інформацію всебічно, забезпечуючи ефективність проактивного виявлення загроз.

5. Криміналістичні розслідування

Визначення того, як сталося вторгнення, включно з ідентифікацією тактик, технік і процедур (TTP) і розумінням дій зловмисників, є важливим для запобігання подібним атакам у майбутньому. Ваше рішення EDR повинно мати можливість візуалізувати весь ланцюг атаки, що полегшує виявлення основних причин інциденту (**рис. 1**).

Carbon Black EDR: посилені загрози потребують посилених засобів захисту

Наведені вище приклади підкреслюють важливість стратегічного вибору платформи EDR, тому багато організацій обирають визнане рішення EDR від Carbon Black, піонера в цій галузі, яке стало частиною портфоліо рішень Enterprise Security Group компанії Broadcom.

Carbon Black EDR виявляє складні атаки та реагує на них завдяки всебічному та інтегрованому підходу. Ви отримаєте негайний доступ до найповнішої інформації про атаку, що дозволяє скоротити час розслідування з кількох днів до лічених хвилин – це критична перевага, коли кожна секунда має значення. Команди безпеки можуть проактивно шукати загрози, виявляти підозрілу поведінку, переривати активні атаки та закривати прогалини в захисті. Carbon Black EDR надійно підтримує всі вищезгадані випадки використання – від реагування на інциденти до криміналістичних розслідувань (**рис. 2**), забезпечуючи всю видимість кінцевих точок і контекстну інформацію для швидкого реагування, щоб обмежити шкоду і запобігти латеральному руху зловмисників.

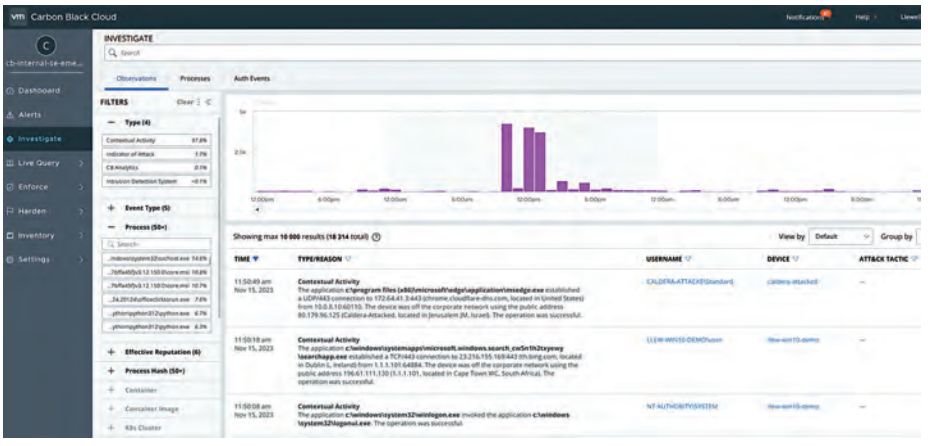

Рис. 2. Розслідування атаки в Carbon Black EDR

Oberig it

Щодо більш детальної інформації, технічних консультацій, проведення пілотних проєктів та впровадження рішень **Carbon Black** *звертайтесь до спеціалістів* **Oberig IT** *як офіційного дистриб'ютора рішень* **Broadcom**
+38 044 594–5461, info.ua@oberig-it.com