Керований кіберзахист:

Провайдери послуг керованого кіберзахисту (MSSP) приходять на допомогу тим, хто не в змозі сам себе захистити.

Керований кіберзахист (Managed Security Services, MSS) є частиною IT-аутсорсингу — у даному разі провайдер керованих послуг (MSSP) бере на себе деякі або й усі функції захисту. Вони можуть відрізнятися за глибиною і охопленням: від діагностики, допомоги в налаштуванні і подальшої підтримки технічних рішень до віддаленого моніторингу, управління обладнанням клієнта і комплексного захисту з реагуванням на інциденти.

«МтБ» поцікавився, як працюють сервіси керованого захисту і з якими проблемами стикаються.

Що вміють MSSP

За визначенням Gartner, провайдер керованих послуг забезпечує за моделлю аутсорсингу моніторинг пристроїв та систем безпеки і управління ними. До поширених послуг належать управління мережевими екранами, системами виявлення вторгнень, віртуальними приватними мережами, скануванням вразливостей, антивірусом. MSSP використовують високодоступні центри управління кіберзахистом (або на власній території, або від операторів датацентрів) і забезпечують сервіс в режимі 25/7, метою якого є зменшення чисельності персоналу операційної безпеки, який підприємство мусить винаймати, навчати і утримувати для забезпечення адекватної безпекової готовності.

MSP (провайдери керованих послуг) надають більш широкий спектр послуг щодо управління IT-системами загалом, як-от: налаштування та оптимізація мереж, техпідтримка, віддалений моніторинг, резервне копіювання та відновлення, хмарні сервіси. MSP надають і послуги з кіберзахисту, але обмежені. MSSP забезпечують усеохопний захист від загроз, пропонуючи широкий спектр послуг на базі власного SOC (**див. табл.**).

Таблиця. Порівняння MSP і MSSP (джерело: Vivantio)

Аспект	MSP	MSSP
Головне призначення	Загальне управління IT й підтримка мережі	Виявлення загроз кіберзагроз і реагування на них
Пропоновані послуги	Технічна підтримка, адміністрування мережі, управління апаратним забезпеченням	Оцінювання ризиків, реагування на інциденти, управління дотриманням регуляторних вимог у сфері безпеки
Потреба для бізнесу	Підходить для підприємств, яким потрібна загальна підтримка IT	Необхідний для організацій, які потребують спеціалізованого управління кібербезпекою
Регуляторний комплаєнс	Обмежується загальним захистом даних і комплаєнсом	Дотримується суворих правил захисту даних і комплаєнсу

Рис. 1. Види діяльності і послуги MSSP (джерело: HTTPCS)

Які саме послуги пропонують MSSP? Вони можуть бути різноманітними (**рис. 1**).

MSSP беруть на себе керування цілим спектром інструментів безпеки, як-от SIEM, мережеві екрани, антивіруси, EDR, системи виявлення та знешкодження загроз в електронній пошті (Inbox Detection and Response — IDR) тощо. За допомогою інструментів моніторингу MSSP збирають і аналізують дані з різних мережевих джерел (серверів, комутаторів, мережевих екранів тощо), відстежують системи і програми на предмет підозрілої активності. Також вони допомагають замовникові встановити й налаштувати його системи, як-от мережеві екрани, VPN, сегментацію мереж і контроль доступу.

Провайдер може впроваджувати процеси й рішення для управління обліковими записами і доступом, процеси автентифікації й управління паролями, а надалі відстежувати підозрілі дії. MSSP розробляє і допомагає впровадити план реагування на інциденти, проводить їх розслідування і застосовує коригувальні заходи, такі як встановлення патчів, вдосконалення протоколів безпеки і навчання персоналу.

Популярними послугами є оцінювання ризиків і кіберрозвідка. У першому разі провайдер перевіряє існуючу систему кібербезпеки і надає рекомендації щодо можливих вразливостей. У другому він збирає інформацію про те, з якими загрозами стикалося чи стикається підприємство або може зіткнутись у майбутньому, а також які з цих загроз являють реальну небезпеку.

Переваги залучення MSSP — численні; тут знову звернемося до інфографіки від HTTPCS (**рис. 2**). По-перше, компаніям часто бракує власних фахівців з кібербезпеки, зате вони є у провайдера. Персонал MSSP має досвід протидії кібератакам, постійно навчається і опановує нові технології, слідкує за останніми трендами — як нападу, так і захисту. Передача кіберзахисту на аутсорсинг вивільняє персонал замовника для основної діяльності або ж дозволяє вирішити якесь окреме завдання.

Одним з таких завдань є забезпечення дотримання регуляторних вимог (комплаєнсу). Передача цієї роботи в MSSP зменшує ризик юридичних наслідків і репутаційних втрат у разі витоку інформації. Провайдер перевіряє пристрої та інфраструктуру компанії і визначає, які зміни потрібні для дотримання вимог. Також MSSP мають досвід та ресурси для вирішення інцидентів безпеки у спосіб, який відповідає законодавству.

MSSP постійно вкладаються в найновіші технології захисту, які невеликі компанії не можуть собі дозволити. Це, своєю чергою, забезпечує захист від найновіших загроз. Окрім того, провайдер може запропонувати спеціалізовані послуги, такі як захист від кіберздирників і безпеку хмарних даних, які компанії самостійно впровадити не можуть.

Рис. 2. Вигоди, які приносить компаніям залучення MSSP (джерело: HTTPCS)

Як і загалом в аутсорсингу, передача завдань кібербезпеки в MSSP дозволяє заощадити кошти на навчання і утримання персоналу, закупівлю і обслуговування технічних рішень. Замовник купує лише той обсяг послуг, який йому потрібен. На додачу MSSP може убезпечити замовника від збитків, віднайшовши вразливості раніше, ніж ними скористаються злочинці.

MSSP гарантують моніторинг і реагування в режимі 24/7, що важливо для бізнесів, які працюють цілодобово, а також дозволяє швидко нейтралізувати інциденти, тим самим зменшуючи збитки і час простою. Також провайдер може вдосконалити загальний стан кібербезпеки на підприємстві шляхом виявлення вразливостей, проведення тестів на проникнення, навчання персоналу і покращення контролю доступу.

Світовий ринок MSS

За даними компанії Markets&Markets, світовий ринок керованих послуг кіберзахисту у 2023 році становив $30,6 млрд і до 2028-го дорасте до $52,9 при середньорічному темпі 11,5%. Mordor Intelligence називає цифри схожого порядку: у 2025 році розмір ринку становитиме $38,85 млрд і зростатиме по 12,24% на рік, сягнувши у 2030-му суми в $69,2 млрд.

Головними чинниками зростання є поширення хмарної інфраструктури й сервісів, а також пристроїв IoT. Markets&Markets називає невпинне ускладнення ландшафту кіберзагроз і брак досвідченого персоналу для боротьби з ними. Попри стрімке збільшення числа загроз, дуже небагато людей є достатньо навченими, щоб розуміти і зупиняти комплексні атаки. А оскільки організації погано обізнані з сучасними загрозами, вони недостатньо вкладаються в захист, що призводить до великих втрат через витоки.

Mordor Intelligence формулює трохи інакше: ключовим чинником зростання ринку MSS є потреба в кіберрозвідці і завчасному виявленні загроз, оскільки в наш час компанії оперують величезними обсягами чутливої інформації.

За оцінками Markets&Markets, найбільшим сегментом на ринку послуг MSS є SIEM і управління логами, вони ж журнали. В багатьох галузях діють суворі правила щодо захисту чутливих даних, і сервіс керованого SIEM та управління логами допомагає організаціям забезпечити комплаєнс. Mordor Intelligence на перше місце ставить сегмент запобігання загрозам (Threat Prevention), а найшвидше зростання (14%) бачить у сегменті керованого IDS/IPS.

У галузевому розрізі — знову-таки через потребу захисту даних — Markets&Markets називає найбільшим споживачем сервісу керованого кіберзахисту сектор банківських, фінансових і страхових послуг. Mordor Intelligence вважає лідером сектор IT і телекомунікацій, на який у 2024 році припало близько чверті ринку, пов'язуючи це з тим, що телеком-оператори дедалі більше перетворюються на постачальників хмарних послуг і стикаються з більшими ризиками кібератак. Фінансовий же сектор демонструє найбільше зростання (ті-таки 14%).

Щодо самих MSSP, то понад половини з них (59%) належать до постачальників IT-послуг, тоді як найшвидше зростає (13%) телеком-сектор — це обумовлено тим, що великі оператори диверсифікують свій бізнес і або купують фірми з галузі кібербезпеки, щоб вийти на ринок MSS, або розвивають вже існуючі можливості. Локальне розгортання є найбільш популярною моделлю (приблизно 57% ринку) через збільшення уваги до безпеки даних і конфіденційності, питання продуктивності і бажання компаній — особливо з галузей, де діє жорстке регулювання — мати більший контроль за чутливими даними. Водночас швидко зростає сегмент хмарних керованих послуг, які забезпечують гнучкість, масштабованість і оптимізацію витрат.

Markets&Markets пише, що фактором, який, навпаки, стримує зростання ринку, є острах перед аутсорсингом. Організації звертаються до стороннього провайдера, якщо не мають власних фахівців або обмежені фінансово. При цьому вони оцінюють як послуги, що їх надає MSSP, так і його власну інфраструктуру, яка повинна бути захищеною від найостанніших загроз. Оскільки MSSP зберігає чутливі дані багатьох організацій, він може ставати об'єктом постійних і складних атак, що викликає в компаній небажання передавати йому свою інформацію. Іноді керівництво не хоче віддавати на сторону контроль за ключовими елементами своєї інфраструктури. Організації підозрюють, що якщо MSSP, який керує всіма їхніми системами, сам зазнає атаки, то це буде ще гірше.

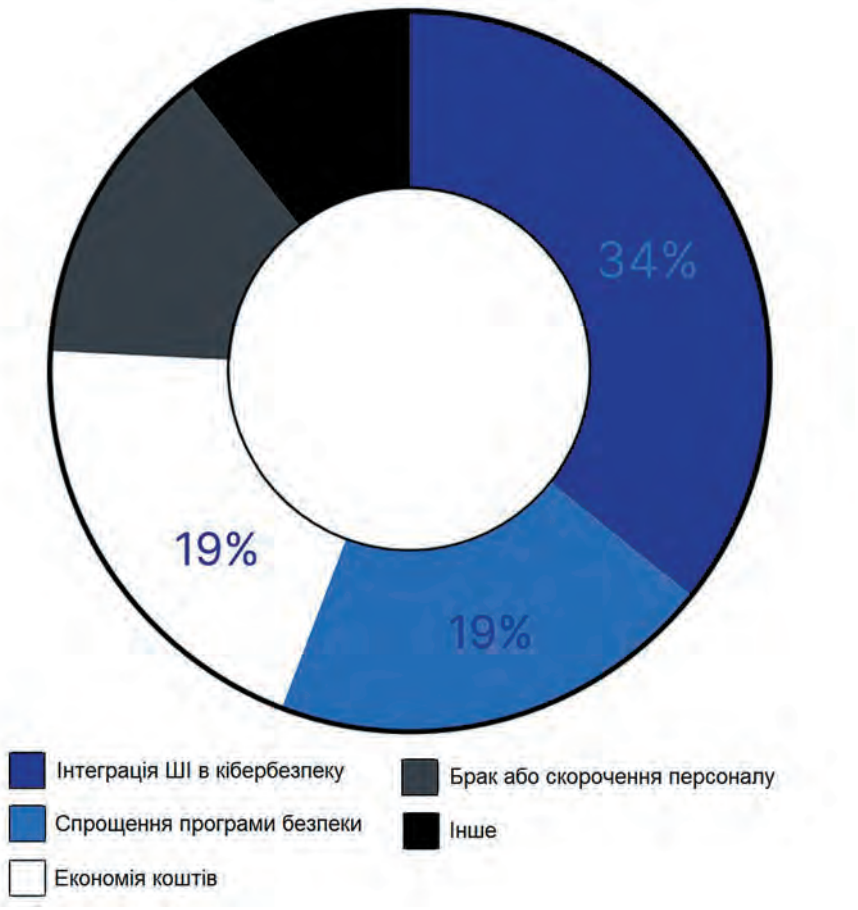

Рис. 3. Головні проблеми, вирішення яких потребують клієнти MSP і MSSP (джерело: OpenText)

Штучний інтелект і адміністративна рутина

Влітку минулого року компанія OpenText Security опублікувала результати дослідження, проведеного серед понад півтори тисячі директорів, вищих керівників і фахівців з кібербезпеки MSP і MSSP США, Канади, Британії, Франції, Німеччини та Австралії. Опитування показало, що 80% цих компаній вже надають клієнтам послуги з використанням ШІ для виявлення загроз, вразливостей тощо, а з решти 62% планують запровадити такі сервіси протягом року. Готуючись до впровадження ШІ, більшість MSP/MSSP проводять навчання персоналу, зосереджуючись насамперед на розумінні генеративного ШІ.

Загалом понад 90% MSP/MSSP вважають інвестиції в штучний інтелект і надання послуг з його використанням головними чинниками, які стимулюватимуть зростання в 2025 році. 67% передбачають, що збільшення інтересу до ШІ призведе до зростання їхнього бізнесу на 11–30%. 90% готові допомагати клієнтам з впровадженням ШІ вже у них.

Дослідники встановили, що головною серед проблем, з якими стикаються корпоративні і СМБ-замовники і з вирішенням яких MSP/MSSP сподіваються їм допомогти, є інтеграція штучного інтелекту в кібербезпеку. Окрім того, опитані компанії вважають, що їхні клієнти потребують допомоги зі скороченням витрат, спрощенням програм безпеки і подоланням проблеми нестачі персоналу (**рис. 3**). При цьому компанії називають головною вигодою від впровадження генеративного або іншого ШІ у безпекові програми клієнтів не заміну людей, а доповнення можливостей персоналу і платформ.

Також дослідження показало, що для половини клієнтів (56%, на 10% більше, ніж у 2023-му) головною причиною, заради якої вони звертаються до MSP/MSSP, є забезпечення усеохопної безпеки (comprehensive security). При цьому 27% клієнтів надають перевагу моновендорному підходові.

Канадська компанія D3 Security, яка оприлюднила результати власного опитування, проведеного серед MSSP, у вересні минулого року, також присвятила значну увагу автоматизації і штучному інтелекту. Це дослідження теж підтверджує зацікавленість провайдерів у ШІ, але є нюанс. Опитування виявило, що провайдерів найбільше непокоїть навіть не власне кіберзахист, а адміністративна рутина. На запитання про те, з якою головною проблемою вони стикаються, респонденти найчастіше обирали варіант «ефективна комунікація і співпраця з клієнтами». А на запитання про те, на які завдання витрачається більшість часу в організації, трьома найпоширенішими відповідями були підготовка звітності, ознайомлення і підключення клієнтів (онбординг) і комунікація з ними. Найбільш часовитратна безпекова діяльність була лише четвертою за частотою згадування: а саме пошук загроз (threat hunting).

Опитані компанії зазначили, що кібербезахист залишається виснажливою роботою: 80% вказали, що, на їхню думку, стрес від цієї роботи негативно впливає на якість життя працівників.

82% респондентів вказали, що їхні компанії мають високий або середній рівень автоматизації, 87% — що автоматизація позитивно впливає на задоволення від роботи, 67% — що вона допомагає збільшити дохід, 64% — покращити маржинальність, 64% — набути конкурентну перевагу. Лише 4% респондентів повідомили, що використовують автоматизацію як заміну працівників.

Що стосується ШІ, то його в тій чи іншій формі використовують 80% MSSP, але часто не в кіберзахисті, а знову-таки для бізнесових функцій, як-от продажі та маркетинг.

Нарешті, переважна більшість MSSP (80%) планує збільшувати прибуток шляхом створення нових послуг для існуючих клієнтів, тоді як 69% — шляхом залучення нових клієнтів. 67% повідомили, що планують розширюватися у сфери аутсорсингу управління інфраструктурою (MSP) і IT-послуг.

Проблеми MSSP та їх вирішення

У 2023 році данська компанія Logpoint спільно з італійською Target Research розпитали американських та європейських MSSP щодо проблем, які їх найбільше хвилюють. З'ясувалося ось що.

Ціна. Однією з головних причин, які спонукають компанії переходити на аутсорсинг кібербезпеки, є зниження витрат. Але якщо MSSP використовують платформи з ліцензуванням за об'ємом (за кількістю сповіщень, гігабайтів, подій або подій на секунду), кінцевий чек може виявитися непередбачуваним або навіть непідйомним, особливо якщо бізнес розвивається і користувачі та системи захисту генерують дедалі більше даних. Це стосується насамперед керованих SIEM, але ще більше SOAR та UEBA. Якщо перекладати проблему зростання витрат на клієнта, можна його втратити.

Взаємодія з клієнтами. Клієнти поділяються на три групи: одним достатньо базових послуг, інших цікавлять розширені пакети, і є ті, кому потрібна експертна допомога для вирішення специфічного завдання. Базовий сервіс загалом автоматизований і не вимагає значного залучення клієнта, який загалом задовольняється розумінням того, що він захищений, і не вважає за потрібне читати звіти, які йому надсилають. Такі клієнти, які рідко контактують з провайдером, легко від нього йдуть, і часто кошти на їх онбординг і конфігурування не окупаються. З іншого боку, клієнти, які знаходяться в контакті з провайдером, зазвичай поновлюють контракт і можуть замовляти додаткові послуги, однак для взаємодії з ними потрібен персонал, якого завжди бракує.

Постійна нестача персоналу. Кваліфікованих аналітиків важко знайти і ще важче втримати, і зі збільшенням числа клієнтів навантаження на них зростає. За іронією, технологічні інновації, які мали б підвищити ефективність роботи аналітика, на практиці можуть її ускладнювати, бо клієнти очікують, що позаяк запроваджено автоматизацію і антивірус чи EDR спрацьовує в реальному часі, то і провайдер повинен опрацьовувати інциденти в реальному часі. Питання полягає в тому, чи потрібна повна автоматизація на базі SOAR, чи ці рішення краще використовувати як допомогу аналітикам в обробленні повідомлень, що надходять від сотень клієнтів.

Розмаїття підходів. Деякі клієнти бажають, щоб MSSP повністю забезпечував кіберзахист без їхньої участі; правила та плейбуки їх не цікавлять, їм лише потрібно, щоб їх інформували про те, як їх захищають. Інші хочуть, щоб MSSP спроєктував і налаштував їм SOC, який клієнт надалі експлуатує сам, а провайдера залучають у разі потреби для розслідування інцидентів і більш складної роботи на кшталт пошуку загроз. Багато клієнтів просять MSSP узяти на себе якусь конкретну функцію — наприклад, комплаєнс, — для якої місцевим фахівцям бракує знань або часу. Це вивільняє персонал замовника і водночас гарантує, що все буде зроблено коректно. Для провайдера ж це може бути точкою входу до замовника, який часто потім купує додаткові сервіси.

Хмарне чи локальне розміщення. Для MSSP працювати повністю в хмарі — це прогресивно і ефективно, але, як йшлося вище, багато організацій бажають або змушені зберігати дані про безпекові події локально. Усі опитані MSSP пропонують локальне розгортання з керуванням через хмару і заявили про неможливість подальшої співпраці з тими виробниками SIEM, які повністю перейшли на хмарні пропозиції, тому що після такого трюку локальну платформу доводиться або підтримувати своїми силами, або вимкнути.

Вибір оптимальних інструментів. Обираючи платформи та інструменти, MSSP стараються ретельно перевіряти їх постачальників, щоб не залишитися з вендором, який їх задовольняє в короткостроковій перспективі, але не в довгостроковій — див. попередній пункт. Також для MSSP дуже важливі інтеграції «з коробки» і гнучкий набір функцій, оскільки це позбавляє потреби самостійно розробляти і впроваджувати ці функції для кожного клієнта. Інтеграції «з коробки» дають змогу підключати технічні рішення, які вже є у клієнта, на кшталт мережевого екрана чи EDR. Водночас, з досвіду MSSP, найкращими функціями «з коробки» є ті, які уможливлюють гнучке конфігурування й налаштування під індивідуального клієнта.

Ті MSSP, які мають відповідних власних фахівців, «допилюють» вендорські рішення або розробляють власні задля забезпечення точно тих функцій, які їм потрібні. Наприклад, замість купувати цілий SOAR і налаштовувати його конфігурації та плейбуки, багато MSSP автоматизують окремі процеси або створюють специфічні сценарії спільно зі своїми клієнтами.

Реальність проти ажіотажу. MSSP мають справу з сотнями вендорів, які постійно намагаються їм продати найостанніші технологічні новинки, тому провайдери мусять ігнорувати хайп і дивитись, на що справді здатні ці рішення. Наприклад, усі згодні, що автоматизація прискорює процеси і розвантажує аналітиків, однак автоматизувати виявлення загроз і реагування на них в одній компанії — це не те саме, що зробити автоматизацію для сотні замовників. Опитані MSSP повідомили, що автоматизацію реагування впроваджують далеко не завжди. По-перше, оптимальні дії для компанії з персоналом у 50 осіб не обов'язково підійдуть для компанії з 5 тис. працівників. По-друге, провайдерові потрібно отримати дозвіл клієнта на те, щоб такі дії, як зміна пароля, активація облікового запису або ізоляція комп'ютера, виконувались автоматично. Більшість компаній натомість покладаються на досвід своїх аналітиків.

Загалом більшість MSSP хочуть мати можливість об'єднувати функції безпеки в один пакет, який можна пропонувати як локально, так і в хмарі; щоб інструменти інтегрувались один з одним і з рішеннями, які є в користувачів; щоб були прості і зручні дашборди, на яких клієнти могли б бачити, як їх захищають; щоб вендори співпрацювали з ними, пояснюючи тонкощі роботи своїх платформ і коригуючи дорожні карти під потреби, що постають.

Василь ТКАЧЕНКО, **МтБ**