Додаток 2. Технічне завдання

1. Предмет закупівлі

Предметом проведення даного конкурсу є придбання програмної продукції для забезпечення безпеки веб-додатків та послуг з супроводження програмної продукції для забезпечення безпеки веб-додатків (Imperva Cloud WAF) протягом 12 місяців та її супроводження.

1. Загальні вимоги до предмету закупівлі
2. Придбане право використання програмної продукції повинно забезпечувати ефективний захист не менше ніж 10 веб-додатків, протягом 12 місяців з дати укладання договору.
3. Програмна продукція для забезпечення безпеки веб-додатків повинна поставлятися в форматі хмарного сервісу (SaaS).
4. Програмна продукція для забезпечення безпеки веб-додатків повинна забезпечувати доступність сервісу на рівні SLA 99.999%
5. Програмна продукція для забезпечення безпеки веб-додатків повинна забезпечити пропускну здатність не менше ніж 100 Мбит очищеного трафіку.
6. Програмна продукція для забезпечення безпеки веб-додатків повинна тарифікуватися виключно по очищеному трафіку за системою 95-персентіля.
7. Програмна продукція для забезпечення безпеки веб-додатків повинна забезпечувати надійний захист не менш ніж 9 веб-ресурсів.
8. Програмна продукція для забезпечення безпеки веб-додатків повинна забезпечувати надійний захист від OWASP "Top 10".
9. Програмна продукція для забезпечення безпеки веб-додатків повинна забезпечувати ефективний захист веб-додатків від атак DDоS.
10. Програмна продукція для забезпечення безпеки веб-додатків повинна надавати можливість визначати та блокувати різні типи запитів від бонетів.
11. Програмна продукція для забезпечення безпеки веб-додатків повинна забезпечувати мережу доставки контенту (CDN) для оптимізації доставки трафіку і зниження навантаження веб-сервера.
12. Програмна продукція для забезпечення безпеки веб-додатків повинна забезпечувати гнучку систему апгрейда, для забезпечення максимальної відповідності поточним вимогам замовника.
13. Функціональні вимоги до захисту
14. Програмна продукція для забезпечення безпеки веб-додатків повинна підтримувати:

* перевірку і контроль HTTP трафіку, включаючи HTTP заголовки, поля форм, а також тіло запитів, що передаються;
* створення кастомних правил захисту, які застосовуються на основі відповіді веб-додатку (Status Code);
* декодування даних в запиті в текстовий вигляд з метою їх подальшого дослідження;
* перевірку для URL, форм, cookie, рядків запиту, прихованих полів і параметрів, методів HTTP, XML елементів і SOAP дій.

1. Програмна продукція для забезпечення безпеки веб-додатків повинна бути в змозі ідентифікувати тип клієнту за допомогою якого надіслано запит;
2. Програмна продукція для забезпечення безпеки веб-додатків повинна підтримувати як позитивну, так і негативну моделі безпеки.
3. Негативна модель безпеки повинна:

* визначати відомі сигнатури атак. Транзакції, вміст яких збігається з відомими сигнатурами атак, блокуються, всі інші дозволені;
* включати попередньо налаштований всеосяжний і точний список сигнатур атак;
* дозволяти виявляти відомі атаки на декількох рівнях, в тому числі на рівні мережі, операційної системи, програмного забезпечення веб-сервера і атак на рівні додатків.

1. Програмна продукція для забезпечення безпеки веб-додатків повинна підтримувати автоматичне оновлення списку сигнатур, забезпечуючи повний захист від новітніх загроз.
2. Позитивна модель безпеки передбачає, що дозволено все, що відомо, а решта блокується. Позитивна модель безпеки повинна включати в себе URL-адреси, каталоги, cookie, поля форм з параметрами і методи HTTP;
3. Програмна продукція для забезпечення безпеки веб-додатків повинна виявляти відомі шкідливі джерела автоматизованих атак і атак з використанням ботнетів, анонімних проксі, вузлів мережі TOR;
4. Програмна продукція для забезпечення безпеки веб-додатків повинна виявляти і блокувати / вимагати проходження додаткової перевірки (CAPTCHA, JavaScript Support) запитів користувачів за географічною ознакою;
5. Програмна продукція для забезпечення безпеки веб-додатків повинна забезпечувати функціонал захисту програмних інтерфейсів додатків (Application programming interfaces, API);
6. Програмна продукція для забезпечення безпеки веб-додатків повинна виявляти роботу шахрайських програм, що використовуються для виконання атак типу Man in the Browser;
7. Програмна продукція для забезпечення безпеки веб-додатків повинна розрізняти ботів від користувачів.
8. Функціональні вимоги до захисту від DDоS

Програмна продукція для забезпечення безпеки веб-додатків повинна забезпечувати :

* ефективний захист веб-додатків від атак DDоS;
* захист від атак DDoS 3/4 та 7 рівня;
* можливість кастомної конфігурації на основі очікуваної легітимної кількості запитів в секунду (RPS).

- можливість налаштування реакції WAF при виявленні DDoS та надання можливості додаткової перевірки шляхом проходження тесту (CAPTCHA, JavaScript Support) беред блокуванням запиту.

1. Вимоги до репутаційних джерел
2. Необхідно, щоб у політиках безпеки програмної продукції для забезпечення безпеки веб-додатків була можливість блокування запитів за критерієм приналежності IPv4 адреси до репутаційних спискам
3. Необхідно, щоб програмної продукції для забезпечення безпеки веб-додатків містила репутаційні списки за наступними категоріями:

* проксі-анонімайзери;
* розповсюджувачі спаму;
* географічне розміщення;
* IP C&C розповсюджувачів зловмисного ПО;
* IP помічені в розповсюдженні фішингу;
* відомі вузли TOR.

1. Вимоги щодо розгортання і використання
2. Програмна продукція для забезпечення безпеки веб-додатків повинна підтримувати режим впровадження шляхом перенаправлення DNS (заміни оригінального DNS веб-додатку);
3. Програмна продукція для забезпечення безпеки веб-додатків повинна бути в змозі працювати з HTTP і HTTPS (SSL) трафіком веб-додатків;
4. Для захисту веб-додатків повинна бути передбачена можливість імпорту SSL сертифікатів і закритих/відкритих ключів веб-серверів;
5. Для захисту веб-додатків без наявного SSL-сертифікату у програмної продукції для забезпечення безпеки веб-додатків повинна бути присутня можливість генерації тимчасового сертифікату шляхом підтвердження прав на володіння доменом;
6. Для захисту SSL веб-додатків програмна продукція для забезпечення безпеки веб-додатків повинна буде термінувати і розшифровувати клієнтські з'єднання, інспектувати трафік на предмет відповідності політикам безпеки і, в залежності від режиму, може повторно його зашифровувати при з'єднаннях з веб-серверами;
7. Програмна продукція для забезпечення безпеки веб-додатків повинна підтримувати можливість балансування трафіку між декількома серверами (Load Balancing) та автоматичного переключення всього трафіку на доступний веб-додаток у випадку недоступності іншого (Fail-Over режим);
8. Модулі комплексу можуть бути розташовані як на локальному сервері так і в хмарному середовищі.
9. Вимоги до адміністрування
10. Програмна продукція для забезпечення безпеки веб-додатків повинна мати веб-інтерфейс для адміністрування.
11. Конфігурація повинна бути простою і інтуїтивно зрозумілою.
12. Доступ до панелі управління повинен надаватися за допомогою 2 FA.
13. Вимоги до підтримки інтеграцій
14. Програмна продукція для забезпечення безпеки веб-додатків повинна мати АРІ для автоматизації рутинних задач.
15. Програмна продукція для забезпечення безпеки веб-додатків повинна мати можливість інтеграції з системами управління подіями безпеки SIEM.
16. Програмна продукція для забезпечення безпеки веб-додатків повинна мати можливість інтеграції з системами управління розподілу навантаження.
17. Вимоги до моніторингу та звітності
18. Програмна продукція для забезпечення безпеки веб-додатків повинна підтримувати належний облік і можливість журналювання:

* можливість формування звіту про події за допомогою стандартних механізмів, наприклад, в системний журнал або через SNMP;
* рівні ведення журналу і фільтри повинні встановлюватися адміністратором;
* WAF повинен бути в змозі формувати табличні або графічні звіти;
* звіти повинні бути доступні як на вимогу, так і за розкладом і поширюватися по протоколу SMTP;
* інтерфейс управління програмної продукції для забезпечення безпеки веб-додатків повинен мати графічну панель, що інформує про стан системи і активності (показники трафіку, спрацювання політик захисту) на всіх підключених веб додатках.

1. Вимоги до послуг з супроводження програмної продукції для забезпечення безпеки веб-додатків (Imperva Cloud WAF)
2. Виконавець договору повинен налаштувати постійний моніторинг доступності веб-додатків, що знаходяться під захистом та сповіщення замовника про їх недоступність.
3. Виконавець договору повинен забезпечити моніторинг сертифікатів та попередження адміністраторів про необхідність заміни за 30, 7 та 3 дні.
4. Виконавець договору повинен організувати проведення регулярних сканувань на вразливості веб-додатків, що знаходяться під захистом, виявлення вразливостей, що не можуть бути закритими WAF та формування пріоритетів по усуненню для розробників.
5. Виконавець договору повинен організувати процес постійного аналізу показників трафіку (пропускна здатність, об’єм переданого трафіку, кількість спроб авторизації) виявлення аномалій та сповіщення адміністраторів;
6. Забезпечення постійного аналізу існуючих правил, перевірка їх працездатності та оптимізація;
7. Щомісячно надавати узагальнений звіт по веб-додаткам, що містить інформацію про:

* Доступність веб-ресурсу та інтервали недоступності для клієнтів.
* Характеристики трафіку веб-сайту: об’єми, кількість візитів, % ботів.
* Атаки на веб-ресурс, їх тип та характеристики, вжиті заходи по виявленим інцидентам.
* Оцінка вразливостей веб-ресурсу, рекомендації щодо усунення вразливостей з урахуванням критичності та можливості ізоляції вразливості за допомогою WAF.
* Ключові параметри налаштування WAF: конфігурація правил безпеки, сценарії автоматичного реагування

1. Кваліфікаційні критерії до Учасників

До участі в процедурі закупівлі приймаються пропозиції від Учасників, які відповідають наступним вимогам:

* Зареєстровані на території України.
* Мають право на поставку зазначеної програмної продукції.
* Мають необхідне обладнання, кваліфікований персонал та досвід в даному напрямку не менше 1 року.