**Номер процедури закупівлі в електронній системі закупівель:**

UA-2021-08-18-002540-a**.**

Закупівля придбання ліцензій до SIEM ArcSight або еквіваленту (Послуги, пов’язані з програмним забезпеченням, код ДК 021:2015-72260000-5) здійснюється для забезпечення потреб Служби безпеки України.

Очікувана вартість закупівлі складає **38 053 000,00 грн.**

**ТЕХНІЧНЕ ЗАВДАННЯ**

###### на закупівлю послуг, пов’язаних з програмним забезпеченням

(Придбання ліцензій до SIEM ArcSight або еквіваленту)

Технічне завдання визначає запланований обсяг товарів, робіт чи послуг та їх важливі характеристики, що є обов'язковими для дотримання переможцем торгів. Повне та своєчасне виконаннявсіх викладених нижче вимог та запропонованих послуг є відповідальністю виконавця і контролюється Замовником.

Запропоновані послуги, які надаються, повинні бути сумісними з наявним програмним забезпеченням та обладнанням у замовника, а саме: віртуальне середовище VMware 6.5, серверна операційна система CentOS з оперативною пам'яттю не менш 384 Гб, НЖМД не менш 4 Тб та 8-ми ядерним процесором.

**Підсистема виявлення загроз та реагування у режимі реального часу за підтримки ефективного інтелектуального ПО з відкритим вихідним кодом повинна забезпечувати обробку 10 000 подій за секунду.**

**Підсистема управління журналами подій безпеки, забезпечення простого пошуку та відповідності нормам повинна забезпечувати обробку 10 000 подій за секунду.**

**Підсистема управління журналами з функціями аналізу та експертизи безпеки повинна забезпечувати обробку 5 000 подій за секунду.**

Гарантійний термін повинен складати не менше ніж 12 місяців.

Строк поставки запропонованих послуг Учасником – до 20 грудня 2021 року.

Ціни й загальна вартість запропонованих послуг наводяться Учасником торгів без ПДВ (згідно пп 26.1 підрозділу 2 розділу ХХ Податкового кодексу України програмна продукція звільняється від оподаткування податком на додану вартість) або з ПДВ та інших необхідних податків і зборів згідно із Додатком до цього Технічного завдання. Переможець зобов'язаний надати послуги, які є предметом закупівлі цих торгів, за цінами, які не перевищують ціни, вказані ним у тендерній пропозиції, протягом всього терміну дії договору. Всі розрахунки здійснюються Замовником по факту надання запропонованих послуг, або за умови відтермінування оплати.

Формуючи свою пропозицію претендент виходить з якісних, кількісних та технічних показників, зазначених у Загальних характеристиках до Системи до Технічного завдання які повинні відповідати запропонованим послугам.

Вартість запропонованих послуг включає всі поточні витрати - транспортування, розвантаження, заробітну плату обслуговуючого персоналу, а також всі податки і збори, що сплачуються або мають бути сплачені.

**Місце надання запропонованих послуг:**пров. Політехнічний, буд. 4, м. Київ, 03056.

**Строк надання запропонованих послуг:** до 20.12.2021 року.

Додаток

до Технічного завдання

**Загальні характеристики до Системи,**

**для якої здійснюється придбання ліцензій**

**Призначення та мета Системи**

**Призначення Системи**

Система збору, зберігання і аналізу подій інформаційної безпеки (далі – ІБ) призначена для автоматизації процесу реєстрації та розслідування інцидентів в області ІБ, що виникають в інформаційних автоматизованих системах Замовника.

**Мета Системи**

* зниження ризиків, пов'язаних з ІБ організації;
* підвищення якості інформаційного і аналітичного забезпечення діяльності співробітників організації при моніторингу ІБ;
* виконання вимог законодавства та нормативно-правових актів органів виконавчої влади, а також вимог стандартів в області забезпечення ІБ;
* виконання вимог «Політики інформаційної безпеки Замовника».

**Характеристика об'єкта автоматизації**

Об'єктом автоматизації Системи збору, зберігання і аналізу подій ІБ є наступні процедури:

* збір подій безпеки з журналів реєстрації інформаційних автоматизованих систем і засобів захисту інформації Замовника;
* аналіз зібраних подій безпеки і реєстрації інцидентів ІБ;
* оповіщення співробітників Замовника про зареєстровані інциденти ІБ;
* зберіганнязібраних подій безпеки і зареєстрованих інцидентах ІБ у єдиному централізованому архіві та надання можливостей по пошуку і перегляду збережених даних;
* підготовка звітів на підставі зібраних подій безпеки і зареєстрованих інцидентах ІБ;
* аналіз інцидентів ІБ.

**Загальні вимоги**

Ліцензування Системи повинне здійснюватися за усередненим значенням потоку подій, що збираються, за добу. Не повинне бути обмежень збору, обробки подій або доступу до інтерфейсів керування Системою при перевищенні ліцензованого потоку подій незалежно від тривалості перевищення.

Система має розроблений виробником вбудований контент, що дозволяє інтегрувати роботу Системи з MITRE ATT&CK Framework.

Всі компоненти Системи підтримують єдину метрику ліцензування. Ліцензування Системи не повинне обмежувати кількість, що розвертаються інстансів будь-яких компонентів.

Розв'язок повинний за замовчуванням забезпечувати інтеграцію із джерелами TI без додаткових витрат.

Рішення повинне забезпечувати власні функції виявлення погроз, які забезпечують прогнозовані аномалії без необхідності додаткового ліцензування функціонала.

**Перелік компонентів, їх призначення та основні характеристики**

До складу Системи збору, зберігання і аналізу подій ІБ включені наступні компоненти:

* модулі збору;
* модуль зберігання та звітності;
* модуль керування;
* модуль кореляції (менеджер);
* модуль керування інцидентами.

**Вимоги до функцій, виконуваних Системою**

**Вимоги до функцій модулів збору**

Модулі збору реалізують функції як системні служби операційної системи, що функціонують разом з іншими компонентами Системи на сервері(-ах) Системи збору,   
зберігання і аналізу подій ІБ або функціонуючі на виділеному сервері(-ах) модулів збору й/або на серверах цільових систем.

Модулі збору забезпечують виконання наступних основних функцій:

* збір подій безпеки з журналів реєстрації цільових систем;
* нормалізацію подій;
* категоризацію подій;
* збагачення подій додатковою інформацією;
* фільтрацію та агрегацію подій;
* пріоритизацію подій;
* тимчасове зберігання (кешування) подій у випадку неприступності одержувача даних;
* передачу подій.

*Збір*

Збір подій безпеки з журналів реєстрації цільових систем здійснються в наступних режимах:

* у режимі автоматичного опитування (періодичне читання подій з файлу, періодична вибірка подій з таблиць бази даних і т.і.);
* у режимі одержання повідомлень (одержання повідомлень про події ІБ по протоколу syslog, SNMP і т.п.).

Збір подій повинен виконуватися віддалено (без встановлення агентів на кінцеві системи) з використанням підтримуваних джерел протоколів передачі.

Збір подій повинен виконуватися в режимі близькому до режиму реального часу. Події безпеки повинні збиратися в Систему по мірі їх реєстрації, з мінімальною затримкою часу між реєстрацією події у вихідному журналі і його додаванням в Систему.

Модулі зборузабезпечують:

* повноту даних, що збираються (повинні збиратися всі події безпеки з журналів реєстрації цільових систем);
* функціонал фільтрації при зборі подій із джерел (можливість завдання користувацьких фільтрів для збору тільки необхідних подій);
* коректність (цілісність) даних, що збираються (події безпеки повинні збиратися без викривлень).

Модулі збору підтримують можливість одержання подій з нестандартних, тобто непідтримуваних виробником рішень, джерел подій для наступних загальноприйнятих протоколів передачі та зберігання даних аудита:

* Syslog (UDP, TCP, TLS);
* SNMP;
* Текстові файли (однорядкові та мультирядкові);
* Структуровані файли (XML і JSON);
* Різні СУБД (MS SQL, Oracle, Mysql, Postgresql);
* REST API

При зборі подій з баз даних не вимагатися створення додаткових вистав (VIEW). Підтримується можливість використання довільних користувацьких запитів з можливістю об'єднання інформації з декількох різних таблиць (JOIN).

*Нормалізація подій*

Модулі зборуздійснють нормалізацію зібраних подій ІБ. При нормалізації зібраних подій ІБ повинен виконуватися розбір вихідних подій ІБ на поля та запис отриманих полів у поля уніфікованого формату. При нормалізації зібраних подій ІБ в одному з полів нормалізованої події при необхідності повинна зберігатися вихідна подія.

Модулі збору повинні надавати можливість створення власних правил нормалізації, а також функціонал по перевизначенню логіки роботи вбудованих правил.

Система повинна надавати графічні інструменти для створення власних правил нормалізації.

Зберігання подій у Системі повинне здійснюватися в нормалізованому виді з можливість збереження подій у вихідному форматі.

Система повинна надавати доступ до реалізованим виробником правилам нормалізації подій.

*Категоризація*

Модулі збору повинні привласнювати подіям категорії, що дозволяють однозначно визначати в тому числі тип джерела, техніку атаки, поведінка, результат і важливість події. Додавання нових типів джерел подій у такий спосіб не повинне вимагати зміни існуючих правил кореляції й пошукових запитів, що використовують категорії. Модулі збору повинні підтримувати користувацьке перевизначення вбудованих правил категоризації, а також створення нових.

*Збагачення*

Модулі збору повинні підтримувати збагачення подій у процесі збору за допомогою запитів до інфраструктурних сервісів і стороннім даних, що налагоджуються довідники, а також мати вбудовану обновлювану базу GEO-IP. Функціонал, що налагоджується, збагачення повинен підтримувати використання регулярних виражень (regex) у якості умов реалізованої логіки.

*Фільтрація та агрегація*

Модулі збору повинні надавати можливість настроювання фільтрації нормалізованих подій ІБ незалежно для кожного призначення (системи, що одержує події від модулів збору). Фільтрація повинна здійснюватися на підставі правил, що налагоджуються, по різним полям подій в уніфікованому форматі. Рішення про видалення або пропущення події повинна ухвалюватися на основі порівняння поля нормалізованого події ІБ із заданою умовою фільтра. Повинна існувати можливість поєднувати умови для окремих полів за допомогою логічних операторів AND, OR і NOT.

Модулі збору повинні надавати можливість агрегування нормалізованих подій ІБ. Агрегування повинне здійснюватися на підставі правил, що налагоджуються. При агрегуванні подій послідовність подій ІБ, зібраних за заданий інтервал часу та відповідних до заданих критеріїв, повинна замінятися однією агрегованою подією. У полі «кількість подій» даного агрегованої події повинна бути зазначена кількість вихідних подій ІБ.

Параметри фільтрації та агрегації повинні містити в собі як значення полів, так і тимчасових діапазонів (для агрегації).

Параметри фільтрації та агрегації повинні настроюватися як через централізований графічний інтерфейс, так і через локальний інтерфейс на кожному модулі збору.

*Пріоритизація*

Модулі збору повинні виконувати пріоритизацію нормалізованих подій ІБ. Пріоритизація повинна здійснюватися шляхом порівняння значень полів нормалізованої події ІБ із заданими умовами та призначення події одного з наступних пріоритетів:

* дуже низький;
* низький;
* середній;
* високий;
* дуже високий.

Модулі збору повинні надавати користувачеві можливість перевизначення вбудованої пріоритизації.

*Кешування*

Модулі збору повинні забезпечувати можливість тимчасового зберігання зібраних подій ІБ (буферизацію). При втраті зв'язку з іншими модулями Системи всі зібрані події повинні розміщуватися в буфер модулів збору. Модулі збору повинні надавати можливість настроювання розміру буфера для зберігання зібраних подій ІБ. Модулі збору повинні використовувати незалежні буфери для кожного модуля призначення.

*Передача*

Модулі збору повинні здійснювати передачу нормалізованих, відфільтрованих, агрегованих і пріоритизованих подій ІБ іншими модулям Системи. Ініціаторами передачі подій ІБ повинні бути модулі збору. Модулі збору повинні передавати події менеджерові пакетами по заданому тимчасовому інтервалу й/або максимальній кількості зібраних подій. Модулі збору повинні надавати можливість настроювання параметрів передачі подій ІБ.

Компоненти збору повинні мати можливість передачі подій, що збираються, як в основну систему, так і в сторонні системи по стандартних протоколах.

Передача подій, що збираються, від компонентів збору повинна виконуватися з використанням захищених протоколів передачі без істотного впливу на продуктивність   
Системи.

Модулі збору повинні підтримувати можливість маскування полів даних, що збираються, а також інтеграцію з рішенням шифрування даних для захисту значень полів, що налагоджуються нормалізацією подій до їхньої передачі по каналах зв'язку та при наступному їх зберіганні.

Модулі збору повинні мати механізм балансування навантаження, який забезпечує наступні функції, принаймні для даних в syslog:

* Розподіл переданих подій між декількома модулями збору;
* Автоматичний перерозподіл подій між модулями при неприступності частини з них.

**Вимоги до функцій модуля зберігання та звітності**

Модуль зберігання та звітності повинен бути реалізований у якості набору системних служб операційної системи, що функціонують на виділеному сервері(-ах).

Модуль зберігання та звітності повинен забезпечувати виконання наступних основних функцій:

* одержання подій;
* зберігання подій;
* функції пошуку та візуалізації;
* звітність по збережених подіях;
* передачу подій в інші модулі системи.

Модуль повинен забезпечувати можливість розподілу користувачем обчислювальних ресурсів відповідно до заданої рольової моделі.

*Одержання подій*

Модуль зберігання та звітності повинен ухвалювати події від модулів збору й/або модуля передачі, а також повинен підтримувати одержання подій прямо від джерел.

При одержанні подій прямо від джерел повинні підтримуватися наступні формати і протоколи:

* CEF syslog (UDP, TCP);
* Syslog (UDP, TCP);
* Текстові файли з мережних сховищ (NFS, CIFS, SAN);
* Текстові файли з віддалених серверів (SCP, SFTP, FTP).

При читанні інформації з текстових файлів повинні підтримуватися події аудита як в однорядковому, так і в багаторядковому форматі.

*Зберігання подій*

Модуль повинен гарантувати цілісність збережених подій і надавати в інтерфейсі функціонал перевірки цілісності файлів даних.

Модуль зберігання повинен підтримувати поділ подій, що збираються, на логічні групи (по джерелах подій) і налагодженню для них різних політик за часом зберігання. Налагодження політики зберігання повинна дозволяти керувати як строком зберігання подій у режимі онлайн, так і зберігання архівних подій.

Модуль повинен використовувати індексацію полів і повнотекстову (full-text) індексацію для збільшення продуктивності пошуку. Адміністратору Системи повинна надаватися можливість налагодження полів, що індексуються. Модуль зберігання повинен підтримувати функціонал “superindexing” для обмеженого набору полів.

Система повинна забезпечувати високий ступінь стискання збережених подій (не менш п'ятикратного) без втрати функціонала пошуку по них і історичної кореляції. Модуль зберігання повинен підтримувати розподілене зберігання подій на декілька інстансах і зберігати можливість пошуку за всім даними з єдиного інтерфейсу.

*Пошук і візуалізація*

Модуль повинен надавати можливість пошуку по збережених подіях і їх візуалізації, у тому числі по ненормалізованих подіях.

Модуль повинен підтримувати складання пошукових запитів по нормалізованим полям, а також використовуючи повнотекстовий (fulltext) пошук. Повинне підтримуватися складання пошукових запитів з використанням спеціальної мови і з використанням графічного конструктора.

Функціонал пошуку повинен підтримувати використання вбудованих операторів для реалізації наступного набору аналітичних можливостей:

* графічна відображення даних;
* наявність базових аналітичних функцій (count, sum, avg, min, max, stdev, percent);
* функції агрегації та угруповання за довільними критеріями;
* виключення повторюваних значень;
* вказівка виключень до критеріїв пошуку (по полях);
* обмеження результатів виводу (head, tail);
* сортування результатів за довільними критеріями;
* можливість використання зовнішніх списків як критеріїв пошуку і для збагачення виведених результатів;
* можливість використання регулярних виразів (regex) у якості критеріїв пошуку;
* функції добування (нормалізації) полів, при роботі з raw-подіями.

При використанні архітектури розподіленого зберігання модуль повинен надавати можливість як локального, так і розподіленого пошуку.

Модуль повинен забезпечувати можливість збереження результатів пошуку. Результати повинні бути доступні без необхідності повторного виконання пошукового запиту.

Модуль повинен дозволяти виконувати кілька одночасних пошуків в одному сеансі користувача.

Модуль повинен забезпечувати можливість перетворювати Ip-Адреси в географічне положення та створювати карти у звітах.

Модуль повинен забезпечувати можливість порівняння декількох подій у вікні пошуку.

Модуль повинен дозволяти виконувати пошук залежно від часу, коли відбулася подія або коли подія була отримана.

Модуль повинен надавати передвстановлені ресурси для візуалізації. Користувач повинен мати можливість кастомізації наданих ресурсів і формування власних.

Модуль повинен відображати статус компонентів до, під час і після виконання пошуку, а також створювати події внутрішнього аудита при старті, закінченні та у процесі виконання пошукового запиту.

Модуль повинен дозволяти одночасне використання декількох вкладок, для відображення результатів пошуку, а також надавати можливість іменувати пошук.

Модуль повинен надавати панель пошуку, щоб відображати активні пошуки,

*Звітність*

Модуль повинен забезпечувати можливість створення звітів за даними які збираються, що настроюються варіантами графічних відображень.

Модуль повинен забезпечувати інтеграцію з бібліотеками Python для додаткової обробки інформації про зібрані дані ІБ при формуванні звітності.

Модуль повинен надавати передвстановлені ресурси для формування звітності. Користувач повинен мати можливість кастомізації наданих ресурсів і формування власних.

Модуль повинен надавати функціональну можливість створення та контролю панелей візуалізації і звітів щодо відповідності стандартам (compliance): PCI-DSS, HIPAA, SOX, ISO27001, FISMA, тощо за допомогою додаткових пакетів (CIP).

**Вимоги до функцій модуля збору, аналізу та кібер-криміналістики**

Модуль кібер-криміналістики має дозволяти аналітикам SOC розпочати пошук та розслідування з консолі SIEM.

Модуль кібер-криміналістики повинен підтримувати вбудовані ролі користувачів, такі як Адміністратор, користувач SOC (Рівень 1, Рівень 2, тощо), Гостьовий режим та дозволи на розподіл цих ролей користувачів відповідно.

Модуль кібер-криміналістики повинен підтримувати колончату (стовпчату) базу даних для забезпечення ефективного функціонування та аналізу великої кількості подій.

Модуль кібер-криміналістики має надавати можливість зручно створювати власні інформаційні панелі та візуалізації для виявлення закономірностей, аномалій та зв’язків подій безпеки.

Модуль кібер-криміналістики повинен підтримувати обробку як структурованих статичних даних (логів), так і неструктурованих.

Компонент для аналітики системи має дозволяти аналітикам безпеки створювати запити без необхідності вивчати спеціфичну мову запитів та схему;

Модуль кібер-криміналістики повинен підтримувати інтеграцію з технологією Kafka та збір даних декількох джерел за допомогою єдиного кластеру на базі технології Kafka;

**Вимоги до функцій модуля керування**

Модуль керування повинен бути реалізований у якості набору системних служб операційної системи, що функціонують на віддаленому сервері(-ах).

Модуль керування повинен забезпечувати виконання наступних основних функцій:

* моніторинг стану модулів збору, передачі, зберігання і звітності, джерел подій;
* адміністрування модулів збору, передачі, зберігання і звітності.

*Моніторинг стану*

Модуль повинен підтримувати централізований моніторинг і візуалізацію у веб-інтерфейсі стану модулів збору, передачі, зберігання та звітності, а також джерел подій.

Модуль повинен забезпечувати можливість відправлення повідомлень у випадку відхилень у метриках працездатності.

Модуль повинен надавати можливість настроювання правил і повідомлень для контролю вступників із джерел подій даних.

Модуль повинен надавати можливість візуального відображення потоків даних для всієї платформи.

*Адміністрування*

Модуль повинен надавати можливість централізованого керування параметрами конфігурації всіх компонентів платформи збору та зберігання.

Модуль повинен надавати можливість централізованого відновлення контенту на компонентах збору.

Модуль повинен надавати можливість вилученого розгортання (інсталяції та налагодження) нових компонентів збору.

Модуль повинен надавати можливість централізованого керування модулями зберігання та звітності: керування архівами (активація, деактивація, реіндексація), параметрами зберігання подій, фільтрами, настроюваннями мережної конфігурації.

**Вимоги до функцій модуля кореляції (менеджера)**

Модуль кореляції (далі – менеджер) повинен бути реалізований у якості набору системних служб операційної системи, що функціонують на віддаленному сервері(-ах).

Модуль кореляції повинен забезпечувати виконання наступних функцій:

* одержання подій ІБ від модулів збору/модуля передачі даних/модуля зберігання;
* аналіз отриманих подій ІБ та автоматичну реєстрацію інцидентів ІБ при вступі певних подій ІБ або послідовності подій за допомогою попередньо настроєних правил (правил кореляції);
* автоматичне оповіщення, що налагоджується відповідальними співробітниками Замовника про зареєстровані інциденти ІБ;
* зберігання подій безпеки та зареєстрованих інцидентів ІБ відповідно до політики, що налагоджується;
* надання графічного інтерфейсу для вибірки і перегляду всіх типів збережених подій
* формування звітів;
* надання функцій керування інцидентами;
* керування модулями збору;
* надання графічного користувацького інтерфейсу для настроювання та керування режимами роботи.

Менеджер повинен підтримувати горизонтальне масштабування та розподілену кореляцію в єдиному контексті з метою підвищення продуктивності кореляції.

Менеджер повинен підтримувати різні вбудовані функції перетворення полів даних, що збираються, а також можливості їх збагачення зі сторонніх джерел.

Менеджер повинен мати можливість імпорту інформації про мережну топологію для використання цих даних у кореляції.

Менеджер повинен підтримувати модель активу (ассета) з можливістю його наповнення інформацією зі сторонніх джерел (наприклад звітів сканерів уразливостей), а також можливість використання цих даних у кореляційній логіці.

Повинна забезпечуватися можливість використання вбудованих функцій для обробки даних різних типів (строкові, числові, дати та ін.) на рівні різних типів ресурсів модуля кореляції (правила, звіти, графічні панелі, фільтри та ін.)

Менеджер повинен мати можливість використання табличних списків з декількома ключовими полями. Табличні списки повинні підтримувати можливість імпорту в них даних із зовнішніх джерел.

Менеджер повинен мати можливість використання значень із табличних списків значного обсягу як критеріїв правил кореляції.

Кореляційні умови повинні підтримувати основні оператори Булевої логіки: AND, OR, NOT.

Кореляційні умови повинні налагоджуватися в графічному інтерфейсі з підтримкою функцій drag'n'drop, без необхідності використання спеціалізованих мов запитів.

Менеджер повинен забезпечувати можливість тестування створюваних правил кореляції на історичних даних до застосування цих правил у режимі реального часу.

Менеджер повинен виконувати оцінку пріоритету/критичності подій на основі аналізу критичності події в цільовій системі, важливості ресурсу в інфраструктурі та у Системі (чи було зафіксоване сканування портів, чи є інформація про уразливості і т.і.), історичних даних про актуальність поточного події (чи атакувалося джерело раніше, чи відомий зловмисник і т.д.).

Менеджер повинен забезпечувати можливість редагування коефіцієнтів формули розрахунків критичності кореляційного інциденту, а також завдання довільної формули розрахунків критичності.

Менеджер повинен здійснювати зберігання зібраних подій безпеки та зареєстрованих інцидентів ІБ в оперативному і в архівному режимі доступу.

Перенесення даних про зібрані події безпеки та зареєстрованих інцидентах ІБ з оперативного сховища в архів повинен виконуватися автоматично, за заданим розкладом. Менеджер повинен надавати можливість настроювання глибини зберігання архіву історичних даних і розкладу перенесення даних з оперативного доступу в історичний архів.

Менеджер повинен надавати можливість вибірки та перегляду всіх типів збережених подій за допомогою графічних користувацьких інтерфейсів. Можливість вибірки та перегляду повинна забезпечуватися як для даних, збережених в оперативному архіві, так і для даних, збережених в історичному архіві.

Повинна забезпечуватися можливість збагачення результатів запитів інформацією з табличних списків.

Менеджер повинен надавати гнучкі можливості створення звітів з використанням, що настроюються графічних шаблонів, а також динамічних вхідних параметрів, що задаються в момент побудови звітів.

Менеджер повинен забезпечувати можливість побудови звітів зі збагаченням подій з табличних списків і ассетів (активів).

Менеджер повинен забезпечувати можливість автоматичної підготовки періодичних звітів і їх відправлення на задані адреси електронної пошти.

Менеджер повинен надавати функції керування інцидентами:

* призначення інцидентів на користувачів системи для проведення розслідувань;
* відстеження стану всіх оброблюваних інцидентів;
* ланцюжок, що настроюється, ескалації інцидентів;
* можливість настроювання полів картки інциденту.

Менеджер також повинен надавати можливості по інтеграції зі сторонніми системами керування інцидентами.

Керування модулями збору, а також настроювання менеджера та керування режимами роботи менеджера повинні здійснюватися за допомогою графічного користувацького інтерфейсу.

Модуль повинен забезпечувати можливість створення користувачів з кастомізованим набором прав у Системі, а також можливість розмежування доступу користувачів до збережених подій.

**Вимоги до функцій модуля керування інцидентами**

Модуль повинен забезпечувати одержання подій (алертів) від модуля кореляції і сторонніх джерел. При необхідності повинен здійснюватися збір базових подій, які привели до спрацьовування кореляційного контенту, і збагачення інформації про інциденти відомостями від сторонніх систем.

На підставі отриманих даних модулем повинні створюватися інциденти. При цьому повинна бути реалізована можливість коректування рівня критичності створеного інциденту.

Модуль повинен забезпечувати виконання заданих користувачем, а також передвстановлених послідовностей дій (playbooks) при виникненні інциденту. При цьому повинна бути реалізована можливість як автоматичного (без участі користувача), так і ручного (очікування підтвердження, дії) керування ходом виконання послідовності.

Створення послідовностей дій для реагування на інцидент не повинне вимагати застосування мов програмування і розробки скриптів. Повинні бути доступні засоби візуального програмування.

Повинна бути реалізована можливість автоматичної реакції з виконанням заданих дій на джерелах подій. Для використання модуля не повинне вимагатися придбання додаткових ліцензій.