

АВТОМАТИЗАЦІЯ ПРОЦЕСІВ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ЗА ДОПОМОГОЮ РІШЕНЬ ESET



Нікіта Веселков

Керівник SOC-команди

nikita.v@eset.ua

У ЦІЙ ПРЕЗЕНТАЦІЇ

АВТОМАТИЗАЦІЯ РОБОЧИХ ІТ-ПРОЦЕСІВ

Автоматизація
звітності

Автоматизація
ІТ-процесів

Автоматизація
оновлень

АВТОМАТИЗАЦІЯ ПРОЦЕСІВ МОНІТОРИНГУ

Автоматизація
сповіщень

Автоматизація
обміну інформацією

АВТОМАТИЗАЦІЯ ПРОЦЕСІВ РЕАГУВАННЯ

Автоматизація
збору журналів

Автоматична ізоляція
кінцевої точки

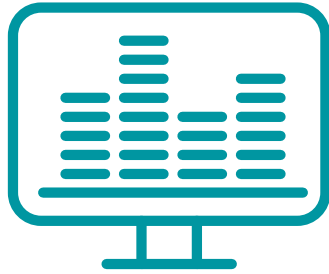
АВТОМАТИЗАЦІЯ ПРОЦЕСІВ РОЗСЛІДУВАННЯ

Автоматизація
відновлення
зашифрованих файлів

Автоматичне
створення звіту

АВТОМАТИЗАЦІЯ РОБОЧИХ ІТ-ПРОЦЕСІВ

АВТОМАТИЗАЦІЯ РОБОЧИХ ПРОЦЕСІВ



**Автоматизація
звітності**



**Автоматизація
ІТ-процесів**



**Автоматизація
оновлень**

Working with Vulnerabilities

АВТОМАТИЗАЦІЯ ПРОЦЕСІВ МОНІТОРИНГУ, РЕАГУВАННЯ ТА РОЗСЛІДУВАННЯ

АВТОМАТИЗАЦІЯ ПРОЦЕСІВ МОНІТОРИНГУ



Автоматичне блокування
шкідливої і аномальної активності



Сповіщення для офіцерів
безпеки та/або інших команд



Обмін інформацією про
індикатори з іншими системами



Автоматичне виявлення нового ПЗ
в інфраструктурі



Автоматичне виявлення
некоректних налаштувань
систем захисту

АВТОМАТИЗАЦІЯ ПРОЦЕСІВ РЕАГУВАННЯ



Автоматичний збір журналів
з кінцевих точок у випадку
аномальної активності



Автоматизація процесу
розгортання додаткових рішень
з безпеки



Автоматичне
блокування сесії
користувача



Автоматичне створення інцидентів
на основі аномальної активності



Автоматичне блокування
індикаторів активності

АВТОМАТИЗАЦІЯ ПРОЦЕСІВ РОЗСЛІДУВАННЯ



Автоматичне відновлення
зашифрованих файлів



Автоматичний збір інформації
для подальшої оцінки ризиків
інфраструктури



Автоматичне
наповнення інцидентів
під час розслідування



Автоматизовані сценарії
для пошуку
додаткової інформації



Автоматичне формування
звітів про активність



ESET Threat Intelligence

- Хмарна і локальна телеметрія
- Моніторинг DarkNet та APT активності
- Збагачення систем захисту актуальними індикаторами та техніками



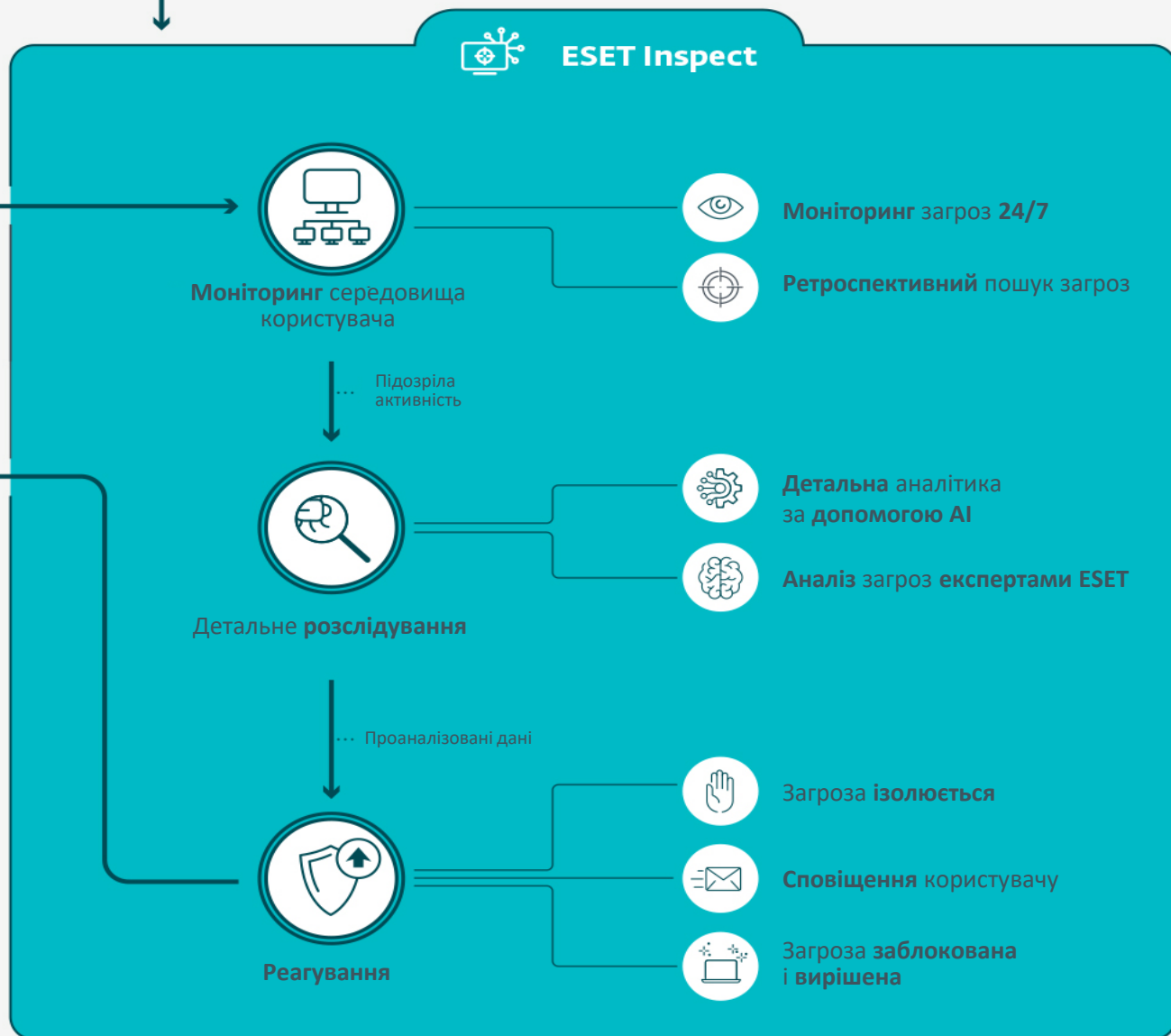
Користувач



DETECTION & RESPONSE ULTIMATE

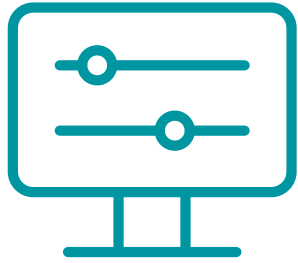


Детальні звіти про інциденти та їх аналіз

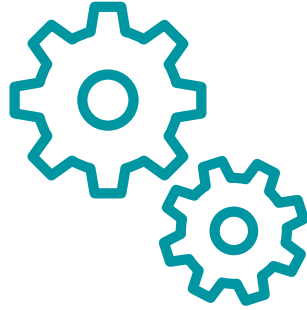


ІНСТРУМЕНТИ ДЛЯ АВТОМАТИЗАЦІЇ

ОСНОВНІ ІНСТРУМЕНТИ ДЛЯ АВТОМАТИЗАЦІЇ



Вбудовані інструменти



API



Плагіни

ПЛАГІНИ ДЛЯ СТОРОННІХ СИСТЕМ



Плагін
ConnectWise



Плагін
Kaseya



Плагін
Datto



Плагін
N-ABLE



Digital Security
Progress. Protected.



+380 44 545 77 26
(цілодобово)



support@eset.ua



TELEGRAM-КАНАЛ НОВИН



ОФІЦІЙНИЙ САЙТ