ПРОЦЕСИ ВЗАЄМОДІЇ ІТ ТА ІБ КОМАНД ПІД ЧАС РОЗСЛІДУВАННЯ КІБЕРІНЦИДЕНТІВ

ESET Digital Security
Progress. Protected.

Нікіта Веселков

Провідний технічний спеціаліст

nikita.v@eset.ua

ОГЛЯД КОМАНД

ЗАГАЛЬНА СТРУКТУРА ІТ КОМАНД

ІТ Команда

ІБ Команда

SOCaaS

ПРОЦЕСИ РОЗСЛІДУВАННЯ ІНЦИДЕНТІВ ЗА КОМАНДАМИ

- Збір додаткових журналів для розслідування
- Налаштування систем та рішень
- Дослідження подій в IT-інфраструктурі на наявність аномалій
- Відновлення систем з бекапів (за потреби)
- Розгортання додаткових рівнів захисту (за потреби)

- Проведення первинного аналізу інциденту
- Пошук індикаторів компрометації
- Аналіз журналів, зразків загроз та образів систем (DFIR)
- Налаштування правил та сценаріїв реагування
- Розробка нових Playbooks на основі результатів розслідування

АВТОМАТИЗАЦІЯ ПРОЦЕСІВ РОЗСЛІДУВАННЯ

Автоматичний збір журналів з кінцевих точок у випадку аномальної активності

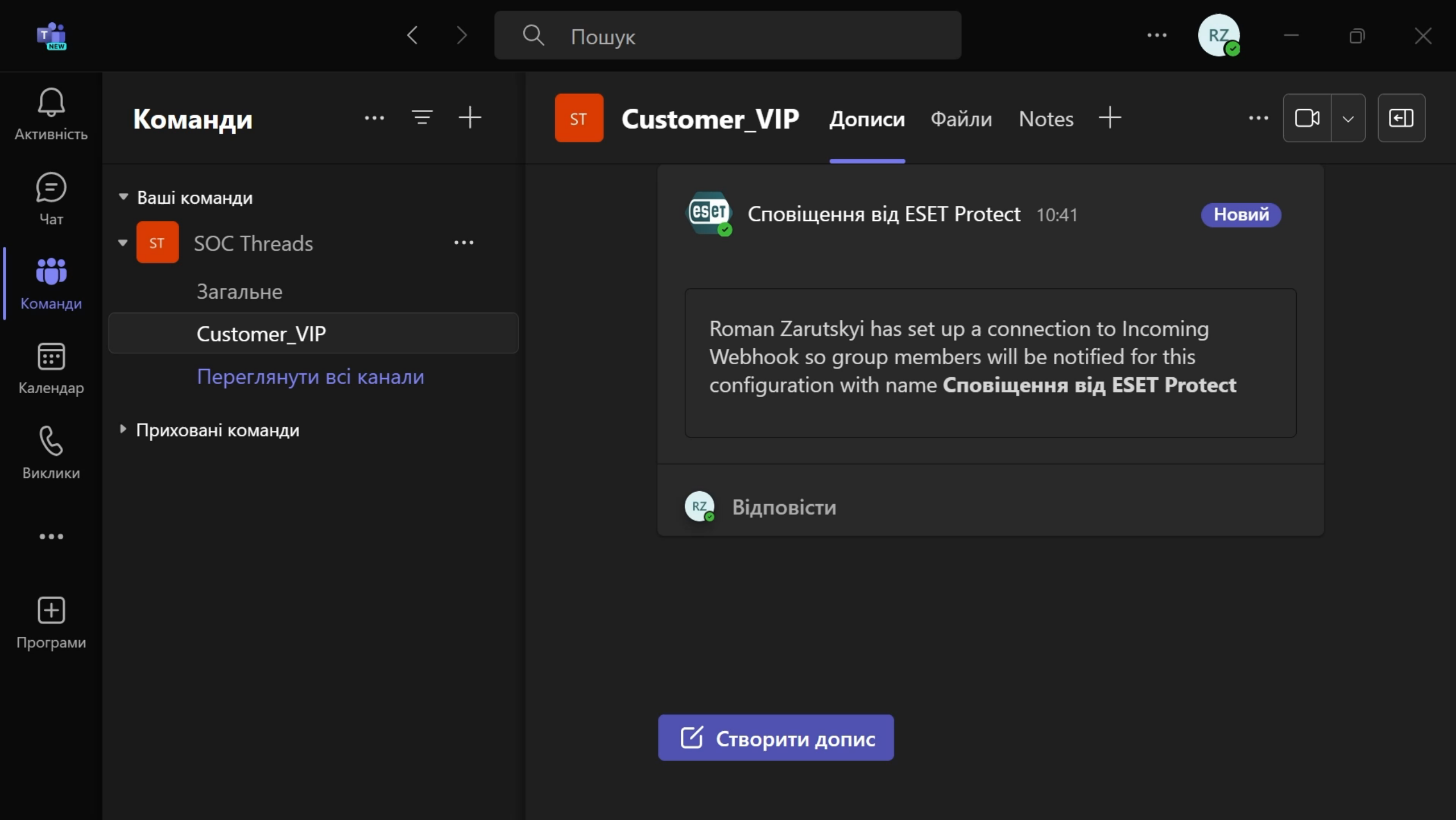
Автоматизація процесу розгортання додаткових рішень з безпеки

Автоматичне створення інцидентів на основі аномальної активності

Автоматизовані сценарії для блокування аномальної активності

Автоматизація процесів пошуку IOC

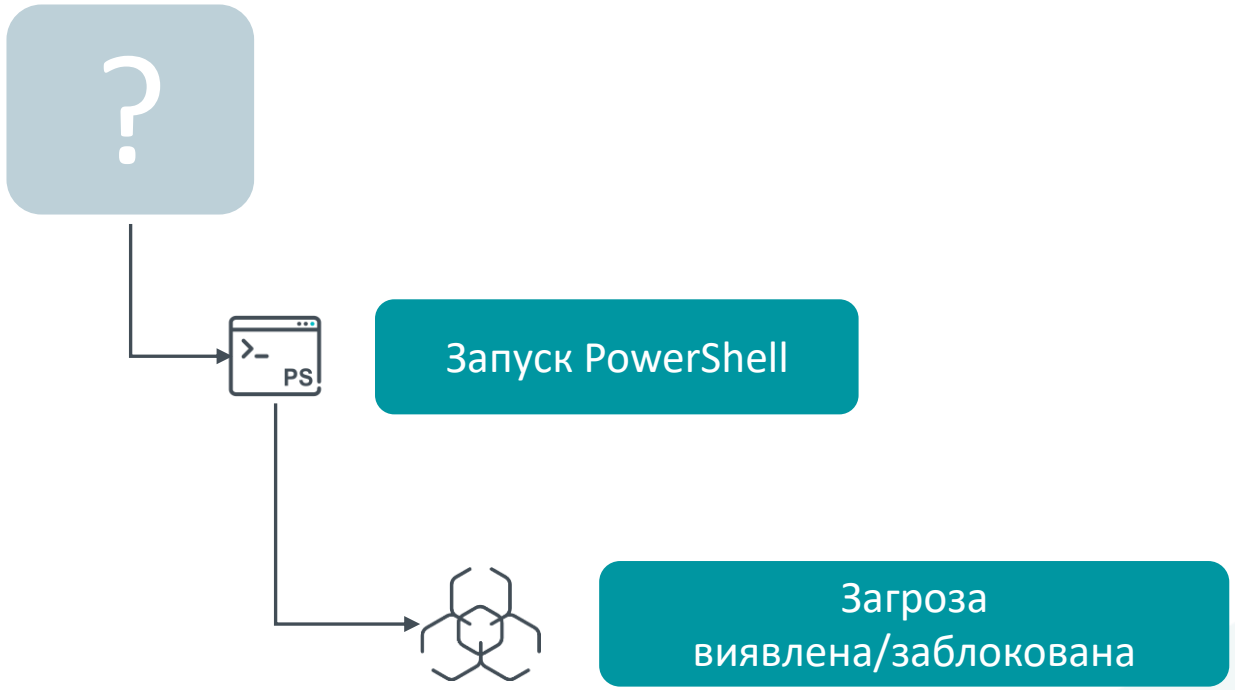
ПРИКЛАД ВЗАЄМОДІЇ КОМАНД


Пошук
RZ
Активність
Чат
Команди
Календар
Виклики
Програми
Команди
Ваші команди
ST
SOC Threads
Загальне
Customer_VIP
Переглянути всі канали
Приховані команди
ST
Customer_VIP
Дописи
Файли
Notes
Сповіщення від ESET Protect
10:41
Новий
Roman Zarutskyi has set up a connection to Incoming Webhook so group members will be notified for this configuration with name Сповіщення від ESET Protect
RZ
Відповісти
Створити допис

БЕЗ ВИКОРИСТАННЯ ESET INSPECT

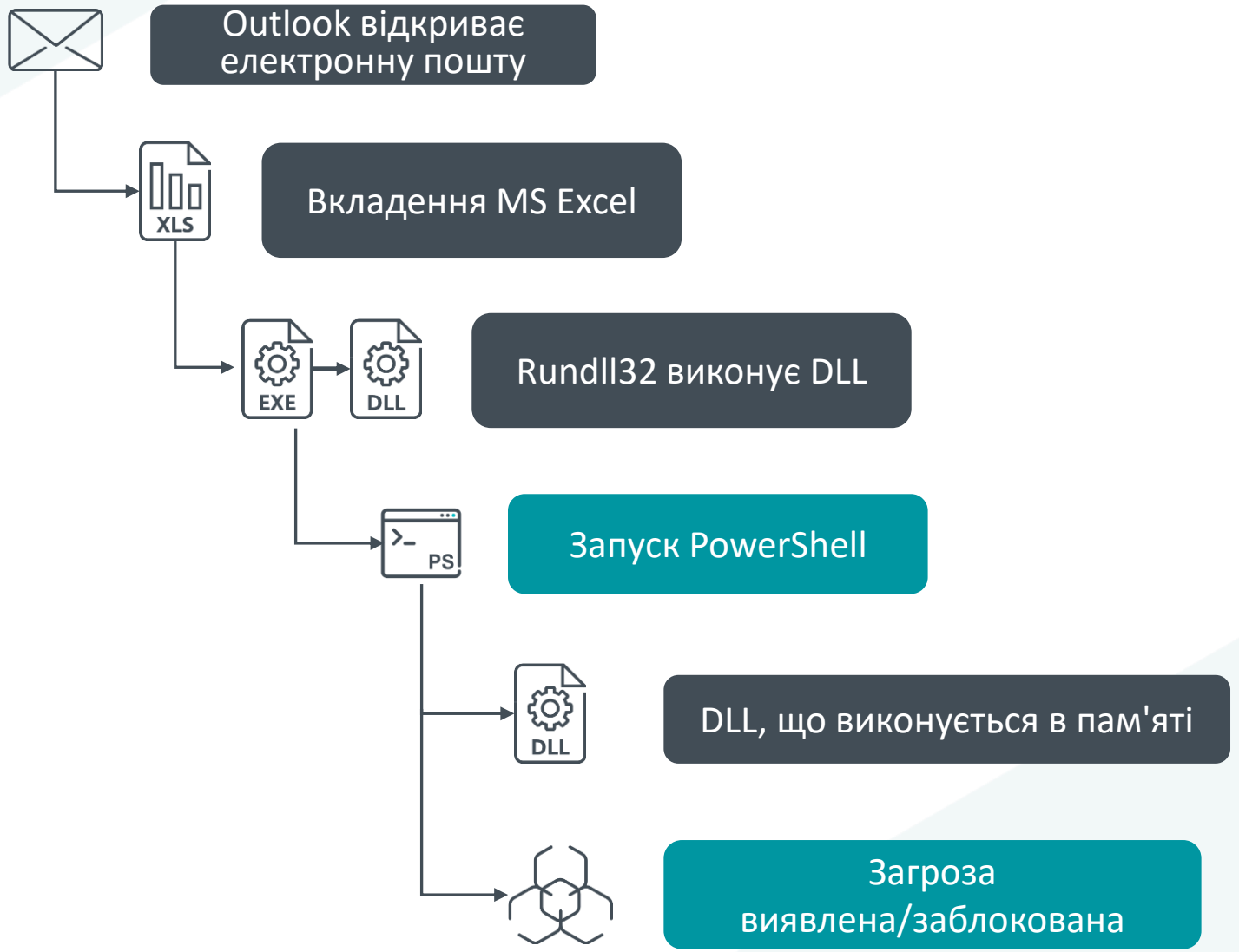
МІНІМАЛЬНА ВИДИМІСТЬ

НЕВИЗНАЧЕНІСТЬ

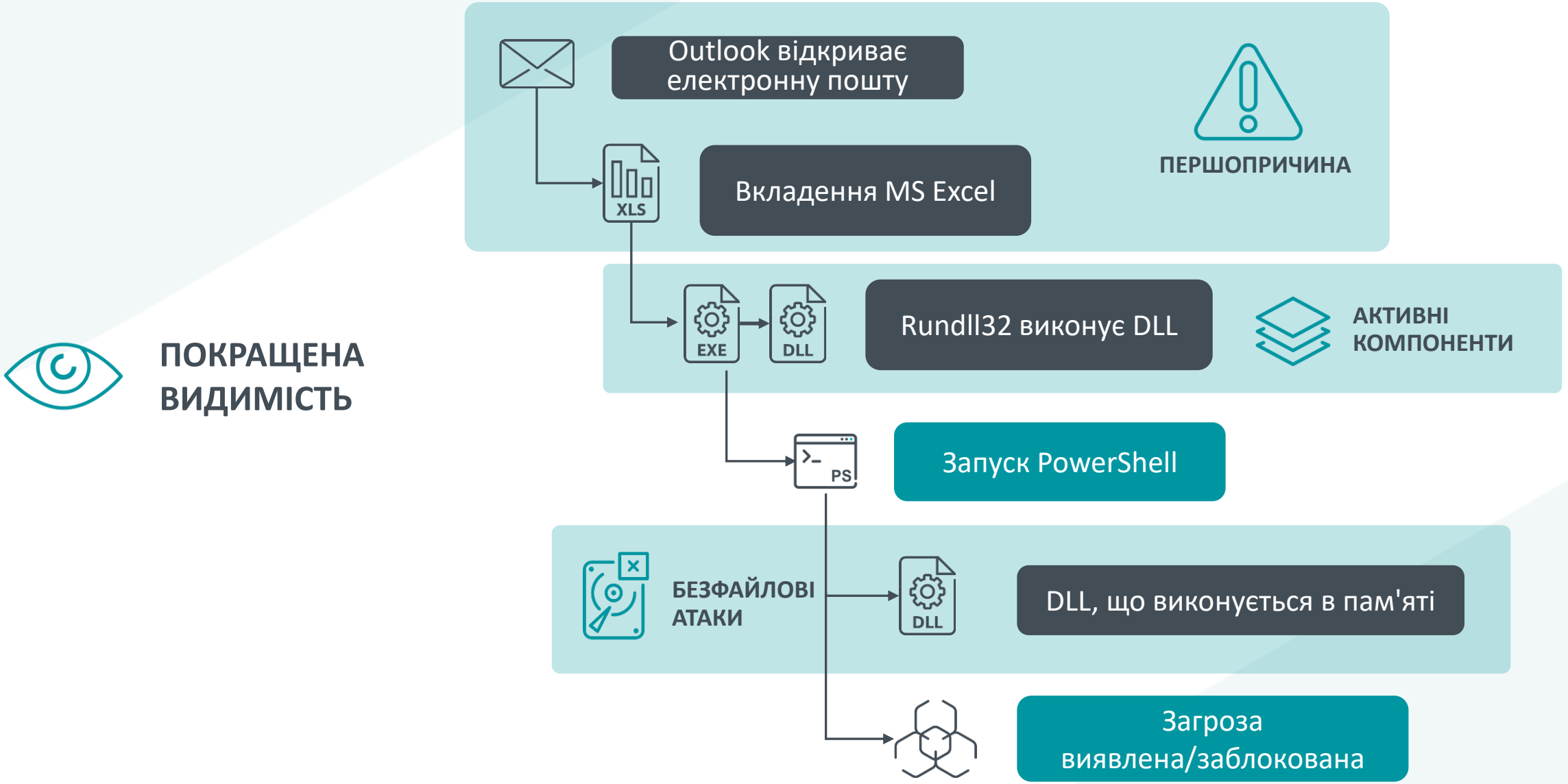


ЗА ДОПОМОГОЮ ESET INSPECT

ПОКРАЩЕНА ВИДИМІСТЬ



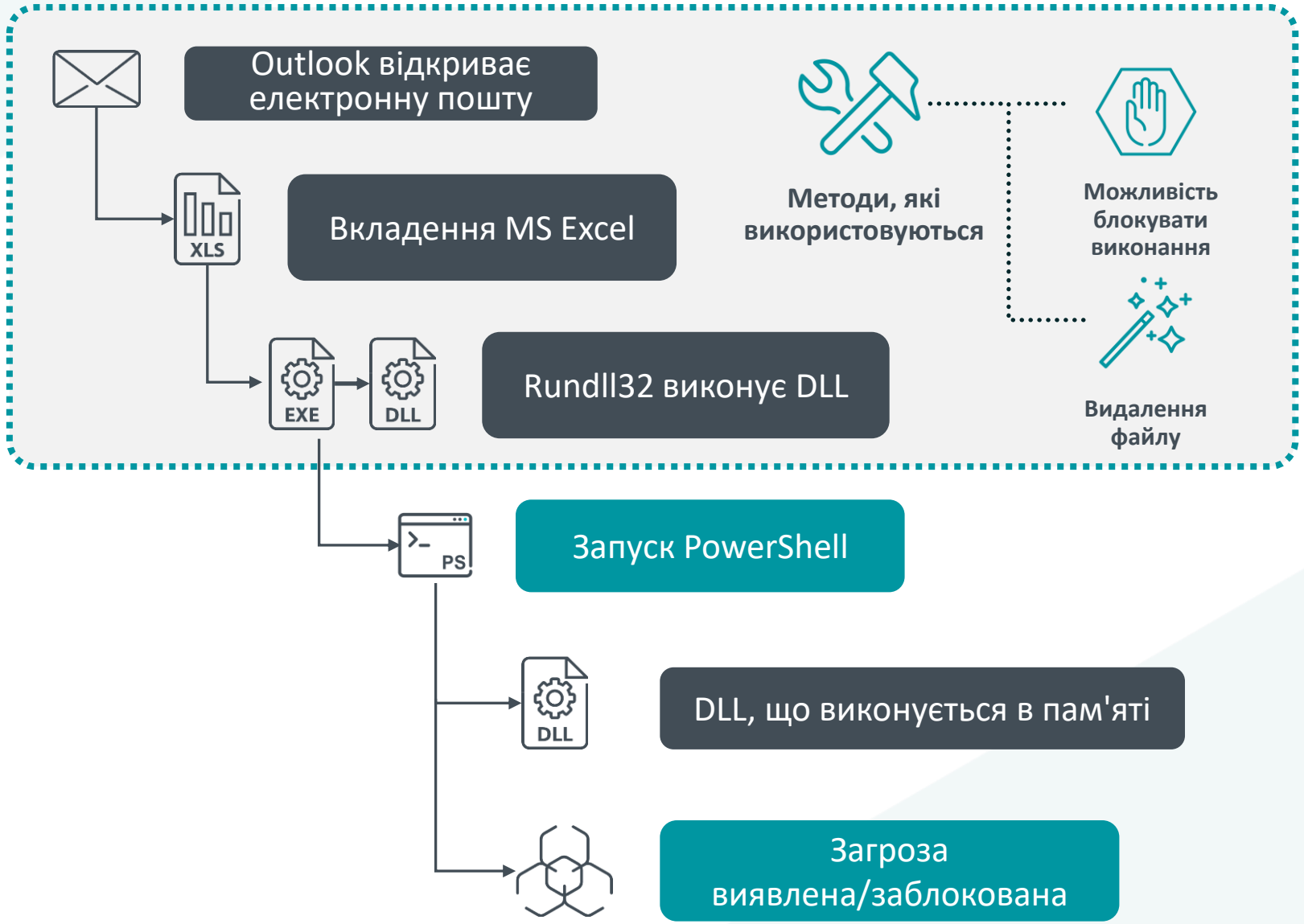
ЗА ДОПОМОГОЮ ESET INSPECT



ЗА ДОПОМОГОЮ ESET INSPECT

ПОКРАЩЕНА ВИДИМІСТЬ

ДОДАТКОВИЙ КОНТРОЛЬ

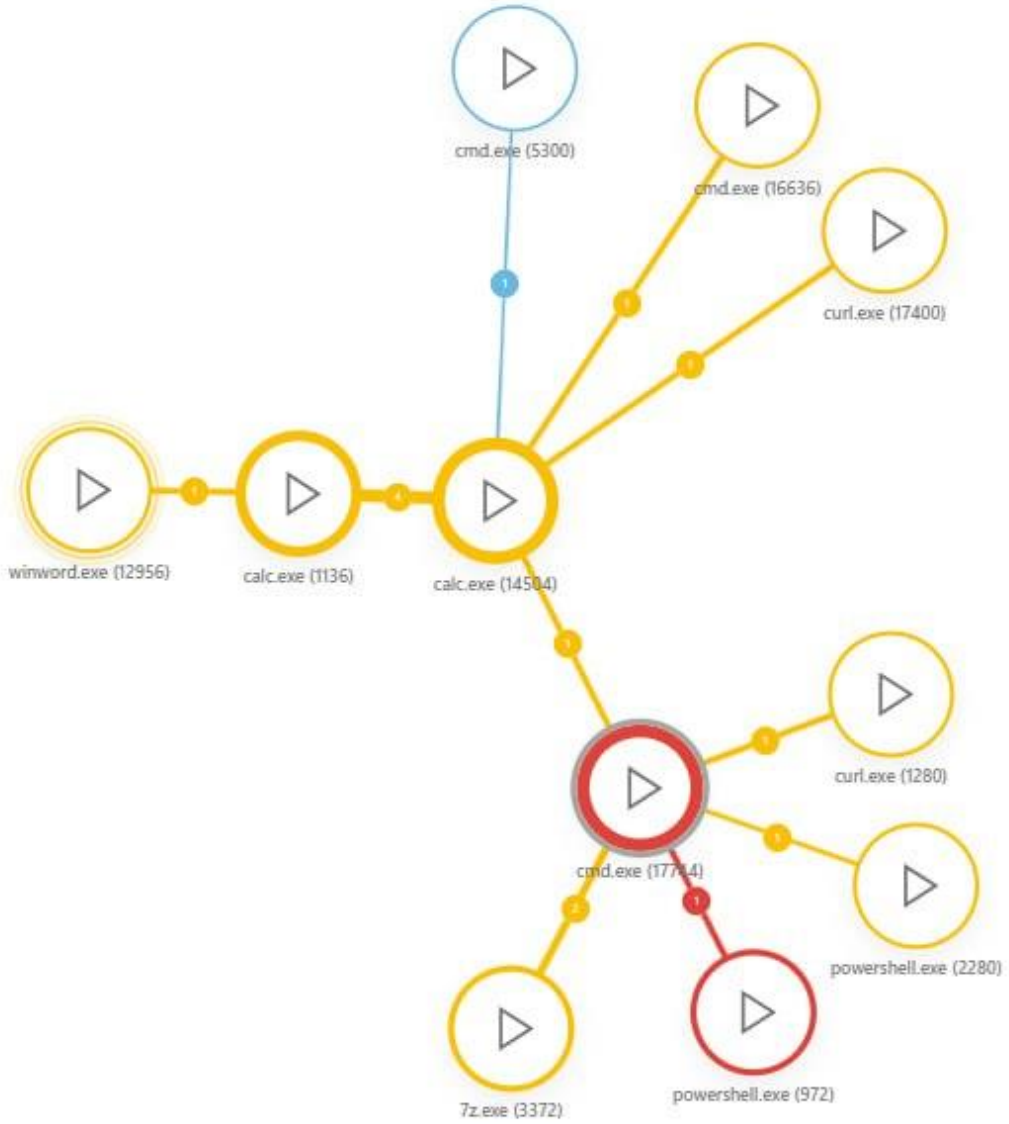


ЗА ДОПОМОГОЮ ESET INSPECT

ПОКРАЩЕНА ВИДИМІСТЬ

ДОДАТКОВИЙ КОНТРОЛЬ

ГРАФІК ІНЦИДЕНТУ



ШЛЯХИ ОТРИМАННЯ СПОВІЩЕНЬ КОМАНДАМИ

Надсилання сповіщень та інформації поштою

Надсилання сповіщень та інформації через Webhook

Передача інформації напряму або через спеціальні чати

SOC Demo Platform: Панель ін

eu01.inspect.eset.com/console/dashboard/incidents

PROTECT & INSPECT

УСІ КОМП'ЮТЕРИ | ДОПОМОГА | CUSTOMER SOC | ВИЙТИ

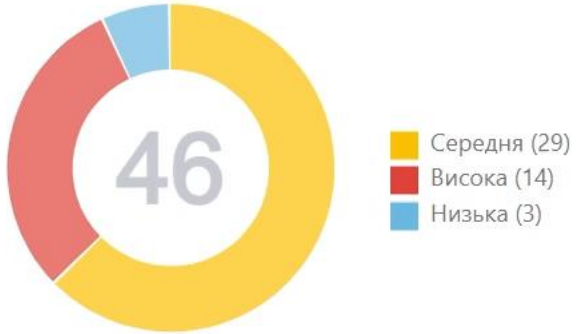
- ПАНЕЛЬ ІНСТРУМЕНТІВ
- КОМП'ЮТЕРИ
- ІНЦИДЕНТИ
- ПОШУК
- Виявлені об'єкти
- Виконувані файли
- Сценарії
- Питання
- Докладніше...
- ЗГОРНУТИ

Панель інструментів

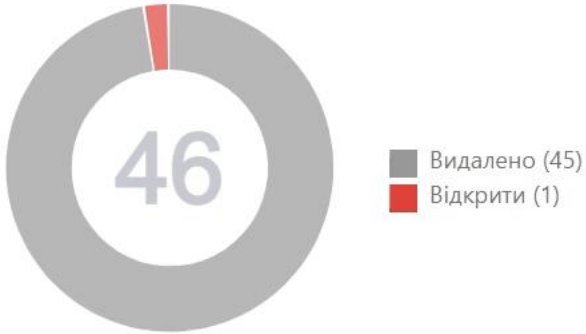
Додати фільтр

Інциденти | Виявлені об'єкти | Виконувані файли | Комп'ютери | Докладніше

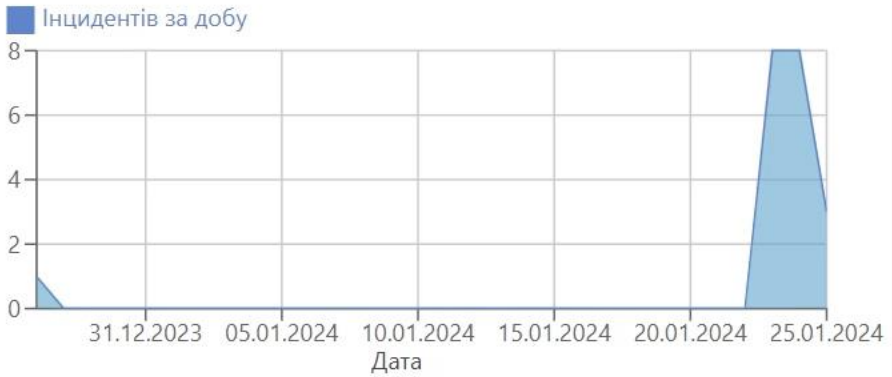
Інциденти за критичністю



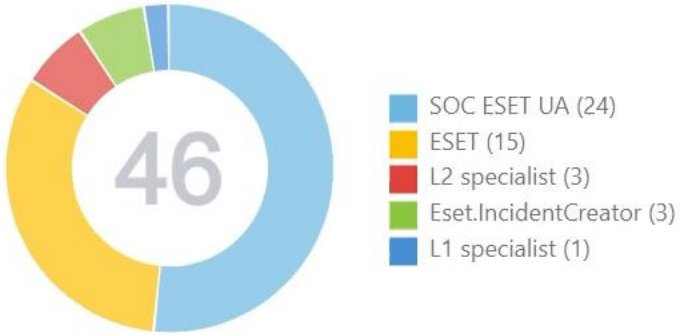
Інциденти за статусом



ESET INSPECT інциденти



Інциденти за автором

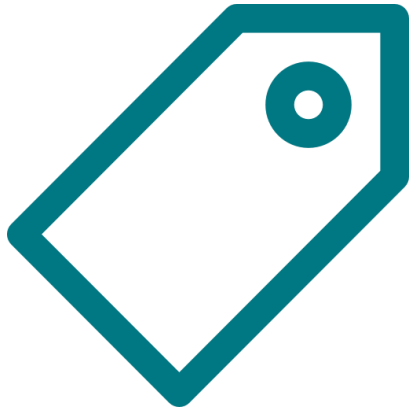


- Схожі фрагменти файлів

MALICIOUS EXTRACTS	FIRST SEEN	COUNT	SIMILARITY	SHA1
[*] Python/Filecoder.MC trojan football.exe	2022-06-15	1 to 10	91%	4F3EFA852BA7ECA556303F 6CE3C4DCBE8D8B377A
[*] Python/Filecoder.MC trojan football.exe	2022-06-15	1 to 10	91%	4F3EFA852BA7ECA556303F 6CE3C4DCBE8D8B377A
[*] Python/Filecoder.MC trojan football.exe	2022-06-15	1 to 10	89%	4F3EFA852BA7ECA556303F 6CE3C4DCBE8D8B377A
[*] Python/Filecoder.MC trojan football.exe	2022-06-15	1 to 10	89%	4F3EFA852BA7ECA556303F 6CE3C4DCBE8D8B377A
[*] Python/Filecoder.MC trojan football.exe	2022-06-15	1 to 10	89%	4F3EFA852BA7ECA556303F 6CE3C4DCBE8D8B377A
[*] Python/Filecoder.MC trojan football.exe	2022-06-15	1 to 10	88%	4F3EFA852BA7ECA556303F 6CE3C4DCBE8D8B377A
a variant of Win64/Agent.CSV trojan mpclient.dll	unknown	unknown	76%	6591042BADF00F34A989F4 9AF75A984AEC8BCFE3
a variant of Win64/Agent.DBU trojan tedutil.dll	unknown	unknown	76%	19E3148F6A259EE458C569E960549105O663CA2B
[*] Python/Filecoder.MC trojan football.exe	2022-06-15	1 to 10	85%	4F3EFA852BA7ECA556303F 6CE3C4DCBE8D8B377A
[*] a variant of Win64/WinDivert.A potentially unsafe application MaxTotalSecurityX64.exe	2021-04-19	10 to 100	83%	932AA5299A65DD3A1308DF F131F6644948A5772D

ВЕДЕННЯ ОБЛІКУ РОБІТ ЩОДО РОЗСЛІДУВАННЯ

Коментування елементів розслідування



Тегування важливих подій

Формування звітів про перебіг розслідування

КОМЛЕКСНИЙ ЗАХИСТ З ВИЯВЛЕННЯМ ТА РЕАГУВАННЯМ У СКЛАДІ

- Консоль управління
- Захист робочих станцій
- Захист файлових серверів
- Розширений аналіз у хмарі (хмарна пісочниця)
- Повнодискове шифрування
- **Виявлення та реагування (XDR)**
- Захист хмарних додатків
- Захист поштових серверів
- Управління уразливостями та виправленнями
- Багатофакторна автентифікація

Digital Security
Progress. Protected.

СЕРВІСИ

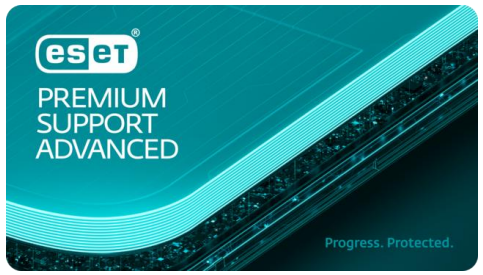
СЕРВІСИ ESET

СЕРВІС З ВИЯВЛЕННЯ ТА РЕАГУВАННЯ

- ✓ Швидке реагування на запити у режимі 24/7
- ✓ Розслідування, виявлення та знешкодження загроз
- ✓ Допомога у реагуванні на виявлені інциденти
- ✓ Мінімізація ризиків виникнення збоїв у роботі
- ✓ Індивідуальний підхід

СЕРВІС З УПРАВЛІННЯ ВИЯВЛЕННЯМ ТА РЕАГУВАННЯМ

- ✓ Цілодобовий безперервний моніторинг загроз, пошук, та сортування спеціалістами
- ✓ Індивідуальні звіти про інциденти та стан середовища
- ✓ Виділений спеціаліст з реагування на інциденти
- ✓ Відстеження потенційних загроз
- ✓ Розгортання та модернізація рішень



ПРЕМІУМ-ПІДТРИМКА

- ✓ Швидке реагування – протягом 2 годин на критичні питання
- ✓ Допомога у розгортанні та модернізації рішень
- ✓ Пріоритет в черзі на виклик та у розгляді запитів розробниками
- ✓ Виділений спеціаліст
- ✓ Віддалене підключення для швидшого вирішення проблем

КОМПЛЕКСНИЙ ПІДХІД ДО ЗАХИСТУ

- Консоль управління
- Захист робочих станцій
- Захист файлових серверів
- Розширений аналіз у хмарі (хмарна пісочниця)
- Повнодискове шифрування
- Виявлення та реагування (XDR)
- Захист хмарних додатків
- Захист поштових серверів
- Управління уразливостями та виправленнями
- Багатофакторна автентифікація

Продукти, які входять до складу

- Сервіс з управління виявленням та реагуванням ESET Detection And Response Ultimate
- Преміум-підтримка ESET Premium Support Advanced

Сервіси, які входять до складу

Digital Security
Progress. Protected.

+380 44 545 77 26
(цілодобово)

support@eset.ua

TELEGRAM-КАНАЛ НОВИН

ОФІЦІЙНИЙ САЙТ