СКЛАДНІСТЬ ТА НЕБЕЗПЕЧНІСТЬ СУЧАСНИХ ЗАГРОЗ ТА КІБЕРАТАК

Олександр Іллюша

Технічний директор

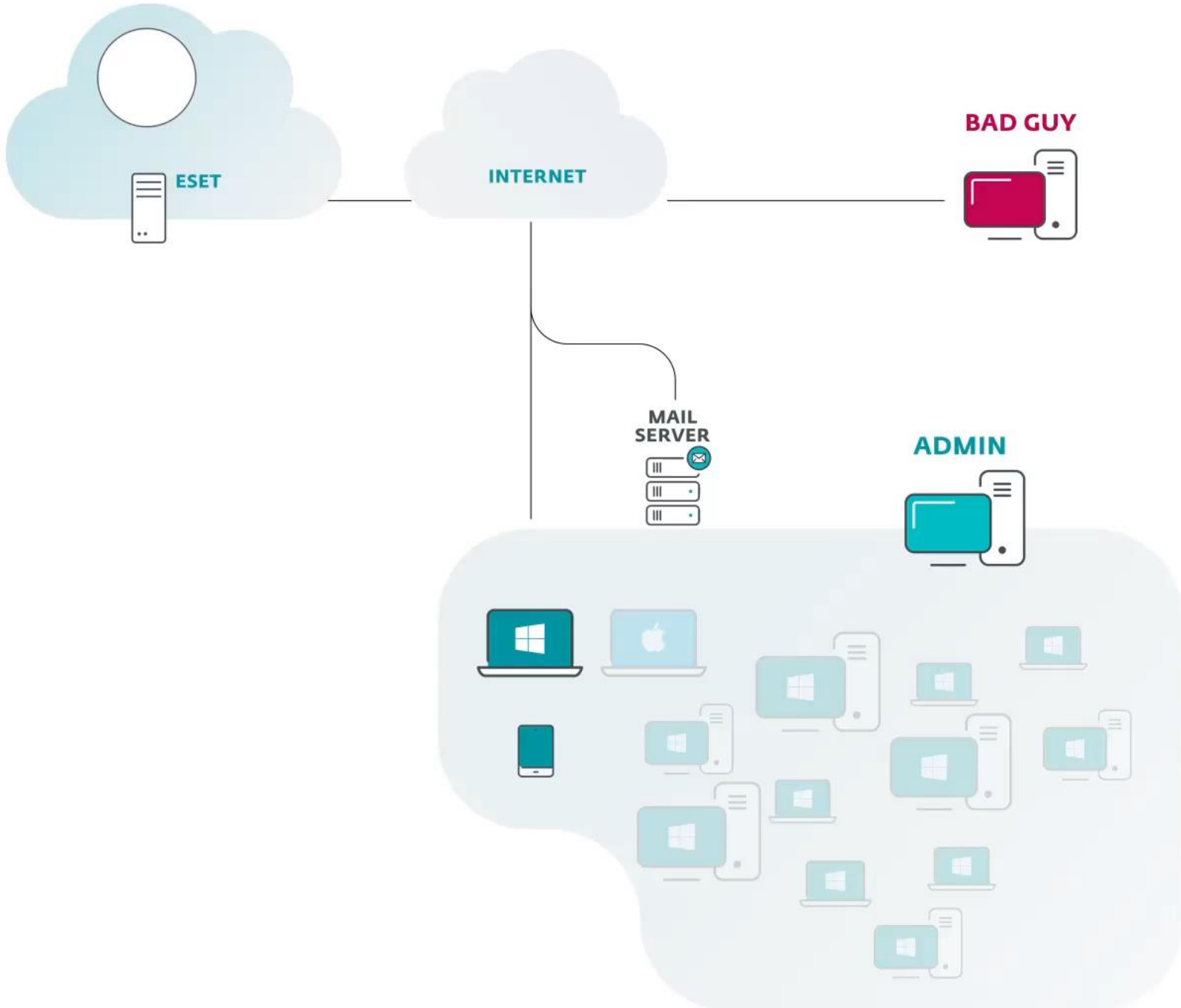
alex@eset.ua

Особливості сучасних загроз та кібератак

Особливості сучасних загроз та кібератак

- Атаки проводяться у декілька етапів, які розтягнуті за часом
- На попередніх етапах використовується соціальна інженерія
- Постійні спроби проникнення через багато різних векторів
- Первинні модулі мають цифровий підпис і не містять зловмисного коду
- Перехоплення облікових записів та підвищення привілеїв
- Приховане розповсюдження в середині зламаної інфраструктури
- Побудова захищених каналів зв’язку із серверами управління (C&C)
- Активна фаза атаки – без використання файлів та збереження даних

Емуляція багатоетапної кібератаки з використанням Ransomware


ESET
INTERNET
BAD GUY
MAIL SERVER
ADMIN

Слабка ефективність класичних систем захисту

Слабка ефективність класичних систем захисту

- Сучасні кіберзловмисники діють в обхід існуючих систем захисту
- APT-угрупування постійно винаходять нові техніки і тактики
- Регулярно виявляються нові уразливості в ПЗ та ОС
- Використовуються застарілі підходи до захисту інфраструктури
- Дуже велика кількість щоденних заблокованих файлів та IP-адрес
- Багато часу витрачається на відпрацювання некритичних інцидентів
- Найслабшою ланкою в захищеній інфраструктурі залишається людина

ЕКОСИСТЕМА

КІБЕРВІЙНА

КЕРОВАНИЙ THREAT HUNTING

ЦІЛЕСПРЯМОВАНІ АТАКИ

COMPLIANCE

ІНТЕРНЕТ РЕЧЕЙ (IoT)

МАШИННЕ НАВЧАННЯ

ПРОГРАМИ-ВИМАГАЧІ

ПЕРЕДБАЧЕННЯ АТАКИ ТА РЕАГУВАННЯ

БЕЗФАЙЛОВІ АТАКИ

UEFI

ТЕХНОЛОГІЇ

ТЕХНОЛОГІЇ

1995

Вбудована пісочниця

1998

Евристичний аналіз

Вбудована у сканер нейронна мережа

2002

Розширена евристика

2005

Родові виявлення

2010

Виявлення на основі машинного навчання (у LiveGrid®)

Хмарні сервіси LiveGrid®

2012

Репутація та кеш

Контроль пристроїв

Захист від мережевих атак

Захист від експлойтів

2013

Розширений сканер пам’яті

2014

Захист від ботнетів

2017

Сканер UEFI

2018

Розширене машинне навчання (у LiveGrid®)

Сканер скриптів (AMSI)

Розширене машинне навчання (вбудоване)

2019

Захист від програм-вимагачів

Глибокий поведінковий аналіз

2020

Захищений браузер

Сканування реєстру та WMI

2021

Захист від підбору паролів

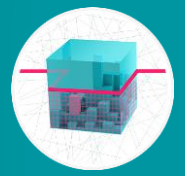
ЯДРО ВИЯВЛЕННЯ

ПЕРЕД ВИКОНАННЯМ

ВИКОНАННЯ

ПІСЛЯ ВИКОНАННЯ

Репутація та кеш



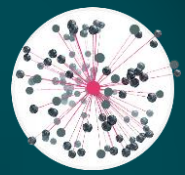
Сканер UEFI

Родові виявлення

Контроль пристроїв

Захист від програм-вимагачів

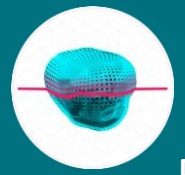
Хмарні сервіси LiveGrid®



Захист від ботнетів

Захищений браузер

Сканер скриптів (AMSI)



Розширений сканер пам’яті

Захист від експлойтів

Глибокий поведінковий аналіз

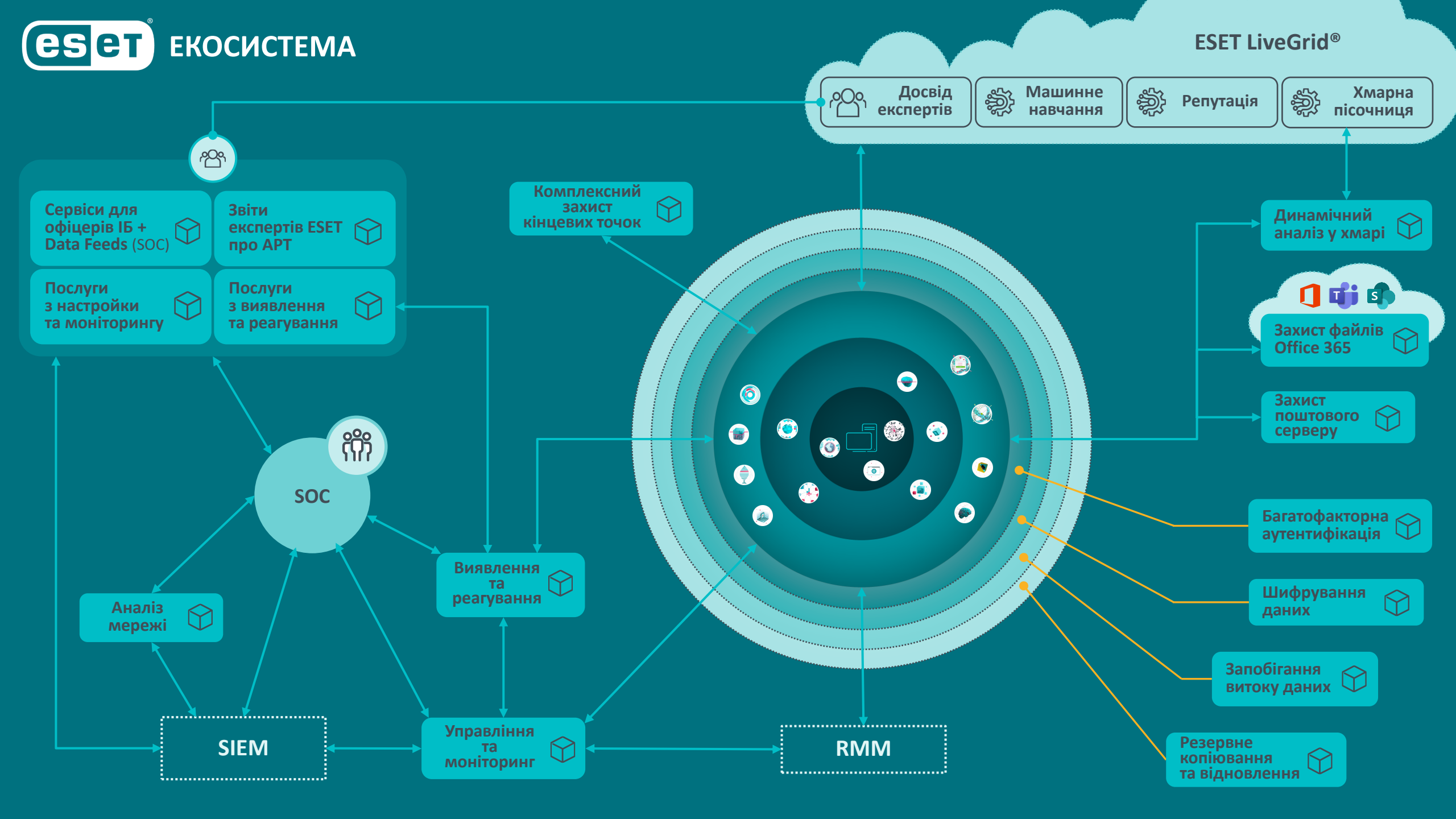
Розширене машинне навчання

Захист від підбору паролів

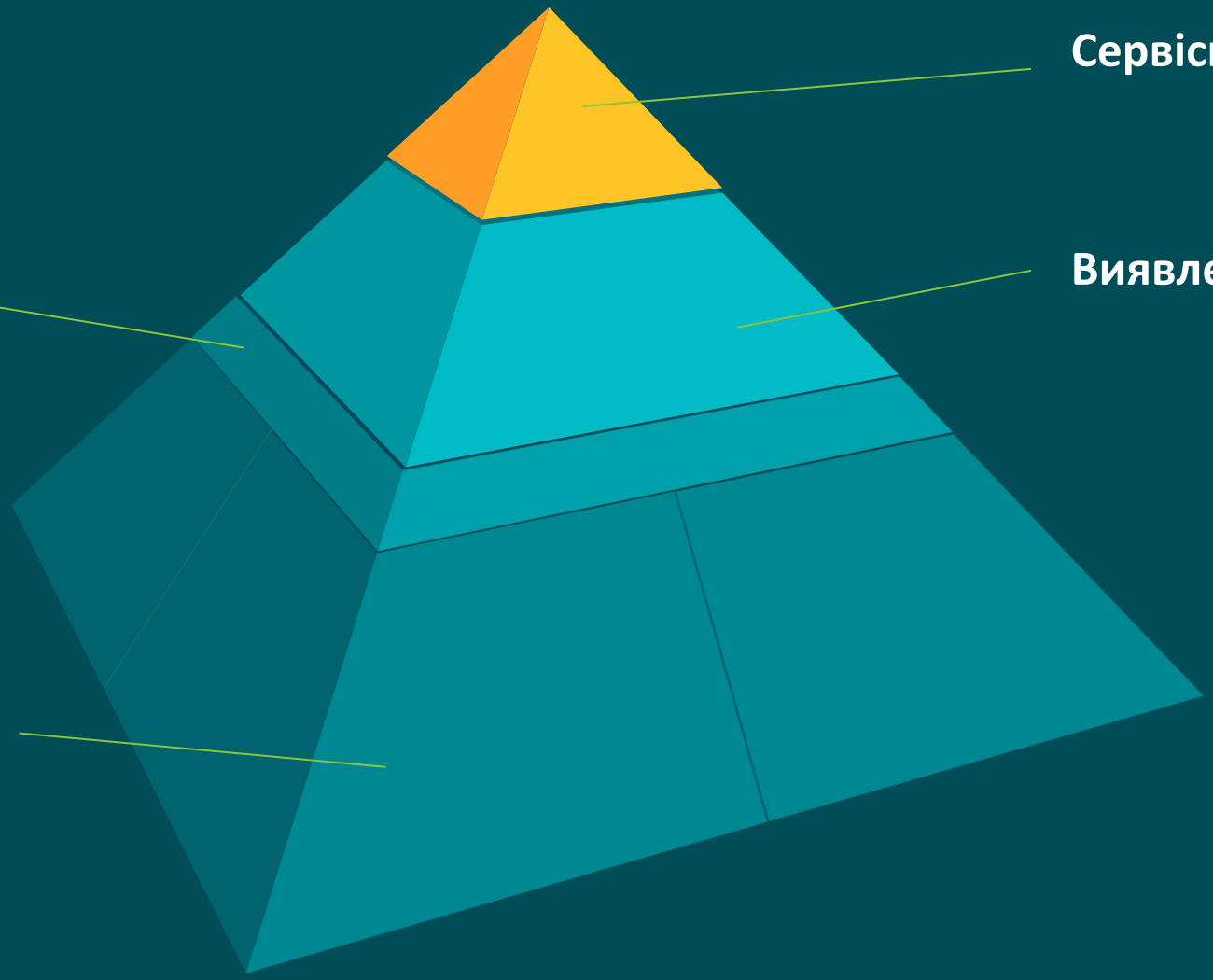
Захист від мережевих атак

Вбудована пісочниця

ESET ЕКОСИСТЕМА



БАГАТОРІВНЕВА БЕЗПЕКА



Сервіси з безпеки

Виявлення та реагування

Динамічний аналіз у хмарній пісочниці

Комплексний захист та запобігання

Практичний досвід залучення спеціалістів ESET до розслідування кіберінцидентів

Практичний досвід залучення спеціалістів ESET до розслідування кібер-інцидентів

- Багаторічний досвід у дослідженні кібератак та складних загроз
- Величезні база даних IoCs та база знань щодо діяльності APT-угрупувань
- Потужні системи телеметрії з мільярдами сенсорів у всьому світі
- Найшвидші автоматизовані аналітичні системи з елементами МН та ШІ
- Регулярні попередження українських компаній про активні кібератаки
- Вдалий досвід залучення до розслідування надскладних кібератак
- Допомога державним і приватним компаніям з аналізу кіберінцидентів

Кібератаки в Україні 2015 – 2021

Digital Security
Progress. Protected.

Оцінка поточного стану систем захисту з метою подальшої модернізації

Оцінка поточного стану систем захисту з метою подальшої модернізації

- Оцінка поточного рівня захищеності корпоративної інфраструктури
- Пошук слідів кібератак та оцінка ймовірності компрометації
- Аналіз безпеки всіх процесів в усіх операційних системах (***EDR***)
- Аналіз захищеності мережевої інфраструктури (***NTA***)
- Аналіз використання та переміщення корпоративних даних (***DLP***)
- Аналіз активності та ефективності співробітників компанії (***DLP***)

Дякуємо за увагу!

Офіційний Telegram-канал новин

ESET