



НАСОЛОДЖУЙСЯ БЕЗПЕКОЮ

Новое поколение решений ESET для противодействия современным киберугрозам

Александр Иллюша

Руководитель службы технической
поддержки ESET в Украине

+38044 545 77 26

alex@eset.ua





EDTD – облачная песочница





ESET

Обнаружение

Выявление
подозрительной
или аномальной
активности в ОС



Enterprise Inspector

Просмотр

Какой процесс
задействован?
Когда это случилось?
Как это случилось?



Реагирование

Блокировка
угрозы
Удаление
угрозы



Программы-вымогатели (Ransomware)



Целенаправленные атаки (APT) и взлом



Слабозащищенные инфраструктуры



Недостаток информации для анализа
инцидентов информационной безопасности



Неправомерные действия сотрудников



Отсутствие квалифицированных кадров

Современные киберугрозы



ESET Dynamic Threat Defense

Останавливает
ransomware на
входе



Ransomware Shield

Поведенческий
анализ
контролирует
изменения в
системе и контент



ESET Enterprise Inspector

Выявление
процессов с
поведением
похожим на
ransomware
(что было изменено,
когда, как и кем/чем)

Ransomware



Целевые атаки и взлом

Блокировка
эксплойтов,

Расширенный
сканер памяти

предупреждение

- YARA-правила
- DATA-feed

& ESMS

Возможность
найти иголку
в стоге сена



Решения для защиты всех узлов инфраструктуры (Linux/Unix, Mac OS, Android, iOS)



Двухфакторная аутентификация при доступе к корпоративным ресурсам

Слабозащищенные инфраструктуры



Решения для шифрования систем и конфиденциальных данных



Решения для резервного копирования и восстановления информации



ESMC – централизованный мониторинг, оповещение и отчетность

Недостаток информации для анализа инцидентов информационной безопасности



EDTD – проверка в облачной песочнице, корпоративная база данных



EI – инструмент для выявления и реагирования на инциденты безопасности

GREYCORTEX
MENDEL

NTA – решение для мониторинга и глубокого анализа сетевого трафика



Веб-контроль, блокировка с учетом времени



Контроль устройств, блокировка с учетом времени

Неправомерные действия сотрудников



Отчетность и оповещения в ESMS



Enterprise Inspector – EDR система

Возможность выявить любую подозрительную активность



Safetica – DLP система

анализ действий сотрудников *(что они реально делают)*



Отсутствие квалифицированных кадров

решений

Мы поможем
развернуть

инцидентов

Мы поможем
расследовать
инцидент
безопасности

состояния

Мы поможем
обеспечить
защиту сетевой
инфраструктуры

**Новые
продукты
для Linux**

**ESMC
Cloud**

**ESMC
и MSP**

**Сканер
уязвимостей**

**ESET Endpoint
Encryption
в ESMC**

**EEI для
mac OS**

**Новые
продукты
для Linux**



Спасибо за внимание!