КІБЕРБЕЗПЕКА ХМАРНИХ ІНФРАСТРУКТУР: ПРАКТИКИ ESET З РОЗСЛІДУВАННЯ ІНЦИДЕНТІВ У ХМАРІ

Digital Security
Progress. Protected.

Нікіта Веселков

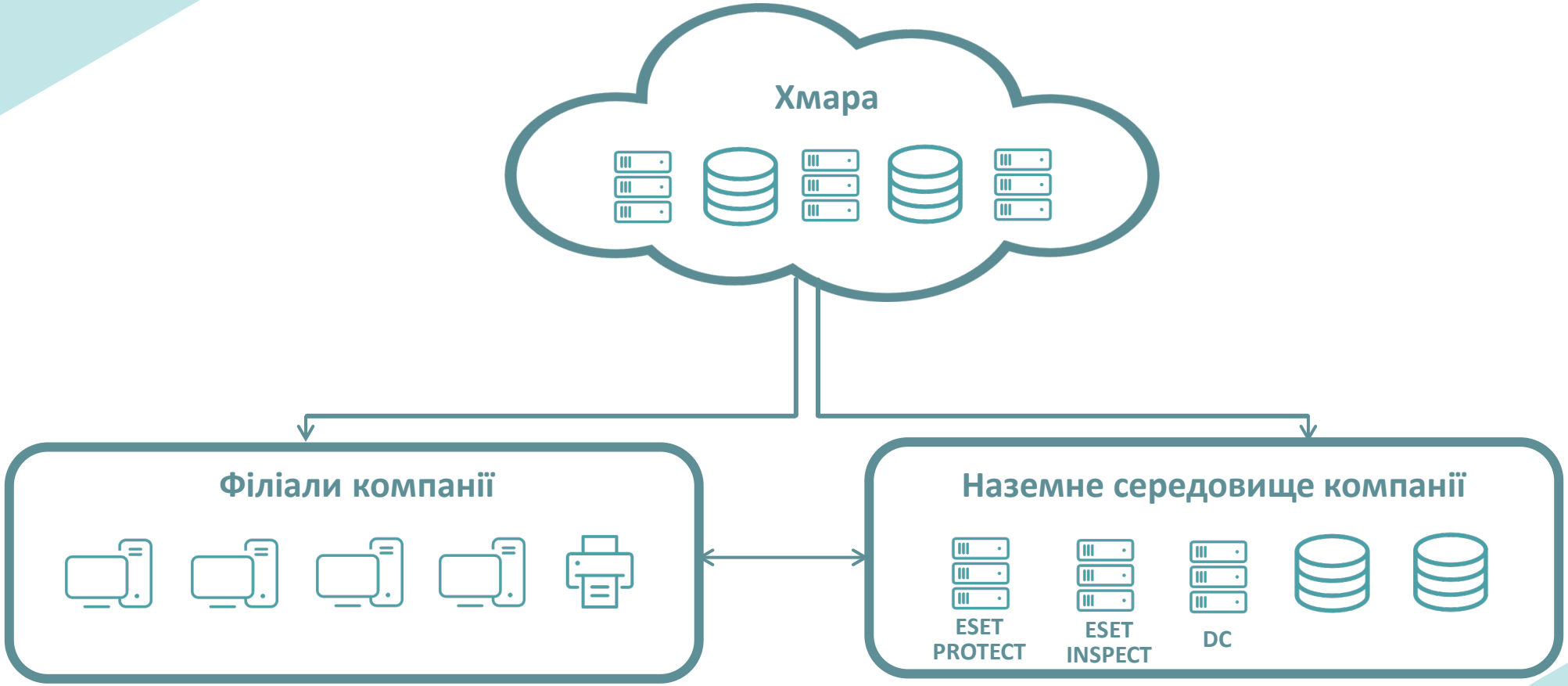
Провідний технічний спеціаліст

nikita.v@eset.ua

User Case

Розслідування атаки у хмарі

ОПИС ІНФРАСТРУКТУРИ КОМПАНІЇ



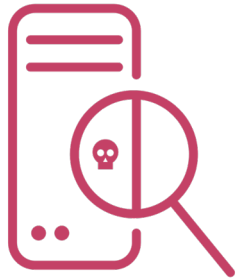
ІНФОРМАЦІЯ СТАНОМ НА ПОЧАТОК РОЗСЛІДУВАННЯ

- Локальні сервери зашифровані
- Хмарні сервери зашифровані
- Філії частково зашифровані

ПОЧАТКОВІ РЕЗУЛЬТАТИ РОЗСЛІДУВАННЯ

Довготривала присутність зловмисників в мережі

Компрометація доменного запису адміністратора



Компрометація ОС сервера ESET PROTECT

ПОЧАТКОВІ РЕЗУЛЬТАТИ РОЗСЛІДУВАННЯ

03.06.2022 15:28	ESET Inspect	Исправление		Succ
03.06.2022 15:28	ESET Inspect	Выход	Пользователь ' вышел	Выполнено
03.06.2022 15:27	Обновление модулей	Обновить	Модули успешно обновлены.	Выполнено
03.06.2022 15:25	Основной пользователь	Изменить	Изменение основного пользователя 'Administrator'.	Выполнено
03.06.2022 15:25	Основной пользователь	Изменить	Изменение пароля для основного пользователя 'Administrator'.	Выполнено
03.06.2022 15:25	Маркер единого входа	Выдача маркера ед	Маркер сеанса единого входа '********' выдан для основного пользователя	Выполнено

Рис. 1. Частина журналу з сервера постраждалої компанії

ПОЧАТКОВІ РЕЗУЛЬТАТИ РОЗСЛІДУВАННЯ

05.06.2022 22:38	Группа домена	Попытаться войти	Проверка подлинности пользователя домена	Сбой
05.06.2022 22:38	Основной пользователь	Попытаться войти	Проверка подлинности основного пользователя	Доступ запрещен
05.06.2022 22:38	Основной пользователь	Попытаться войти	Проверка подлинности основного пользователя	Доступ запрещен
05.06.2022 22:37	Основной пользователь	Попытаться войти	Проверка подлинности основного пользователя	Доступ запрещен
05.06.2022 22:36	Основной пользователь	Попытаться войти	Проверка подлинности основного пользователя 'admin'.	Доступ запрещен
05.06.2022 22:36	Основной пользователь	Попытаться войти	Проверка подлинности основного пользователя 'admin'.	Доступ запрещен
05.06.2022 22:36	Основной пользователь	Попытаться войти	Проверка подлинности основного пользователя 'admin'.	Доступ запрещен
05.06.2022 22:15	Серверная задача	Запуск	Запуск серверной задачи 'Automatic renaming of synchronized computers to FQDN format' типа 'Переименовани	Выполнено

Рис. 2. Частина журналу з сервера постраждалої компанії

ПОЧАТКОВІ РЕЗУЛЬТАТИ РОЗСЛІДУВАННЯ

06.06.2022 0:18	Серверная задача	Запуск	Запуск серверной задачи 'Automatic renaming of synchronized computers to FQDN format' типа 'Переименовани	Выполнено	Administrator
06.06.2022 0:17	Политика	Создать	Создание политики 'New Policy'.	Выполнено	Administrator
06.06.2022 0:06	Лицензия	Отключить	Деактивация всех активных рабочих мест для лицензии на компьютере	Выполнено	Administrator
06.06.2022 0:06	Лицензия	Отключить	Деактивация всех активных рабочих мест для лицензии на компьютере	Выполнено	Administrator
06.06.2022 0:05	Маркер единого входа	Выдача маркера ед	Маркер сеанса единого входа '********' выдан для основного пользователя 'administrator'.	Выполнено	
06.06.2022 0:05	Основной пользователь	Попытаться войти	Проверка подлинности основного пользователя 'administrator'.	Выполнено	
05.06.2022 23:56	Основной пользователь	Выход	Выполнение выхода основного пользователя 'Administrator'.	Выполнено	Administrator
05.06.2022 23:42	Маркер единого входа	Выдача маркера ед	Маркер сеанса единого входа '********' выдан для основного пользователя 'EEI'.	Выполнено	
05.06.2022 23:42	Основной пользователь	Попытаться войти	Проверка подлинности основного пользователя 'EEI'.	Выполнено	
05.06.2022 23:42	Маркер единого входа	Выдача маркера ед	Маркер сеанса единого входа '********' выдан для основного пользователя 'administrator'.	Выполнено	
05.06.2022 23:42	Основной пользователь	Попытаться войти	Проверка подлинности основного пользователя 'administrator'.	Выполнено	
05.06.2022 23:42	Группа домена	Попытаться войти	Проверка подлинности пользователя домена 'administrator'.	Сбой	
05.06.2022 23:41	Сервер	Запуск	Запуск сервера.	Выполнено	
05.06.2022 23:15	Серверная задача	Запуск	Запуск серверной задачи 'Automatic renaming of synchronized computers to FQDN format' типа 'Переименовани	Выполнено	Administrator
05.06.2022 23:09	Основной пользователь	Попытаться войти	Проверка подлинности основного пользовател	Доступ запрещен	

Рис. 3. Частина журналу з сервера постраждалої компанії

ПОЧАТКОВІ РЕЗУЛЬТАТИ РОЗСЛІДУВАННЯ

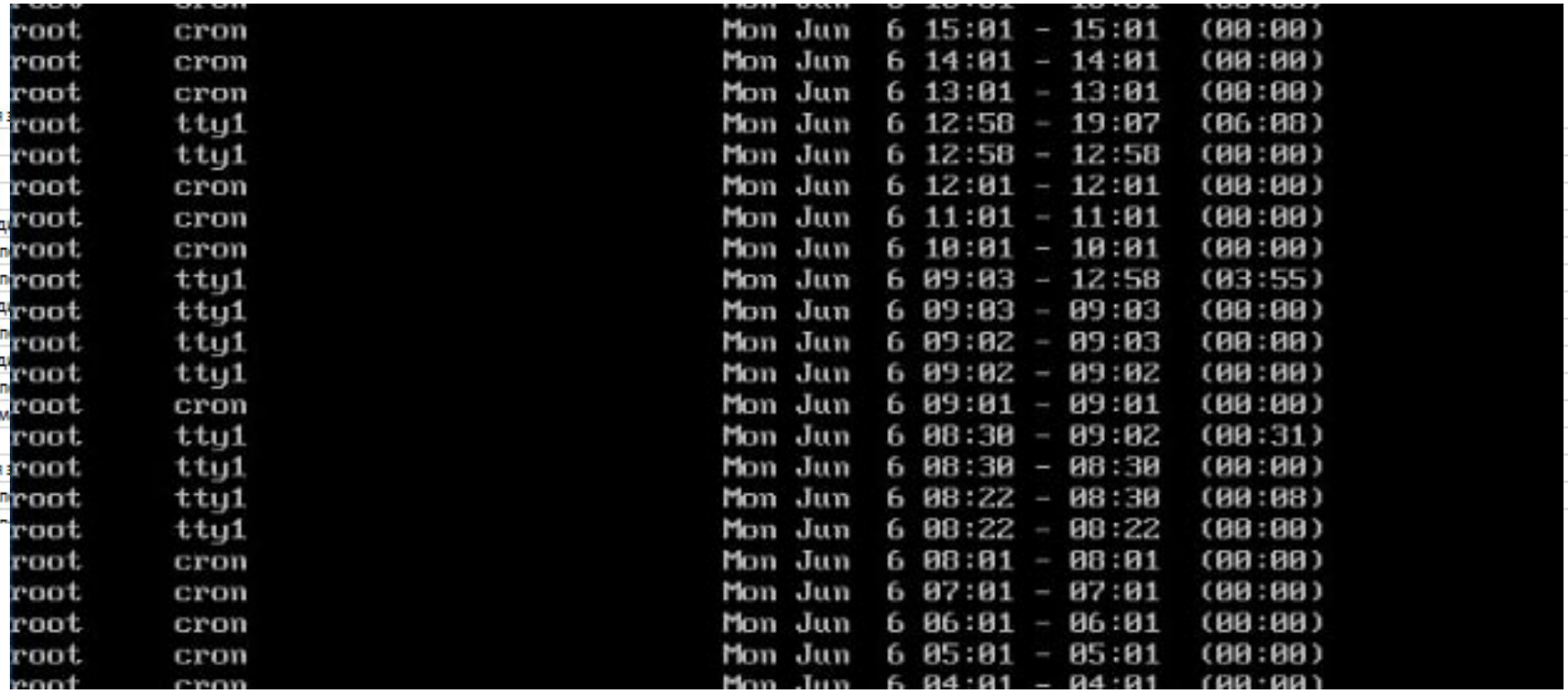


Рис. 4. Частина журналу з сервера постраждалої компанії

РОЗСЛІДУВАННЯ ЗА ДОПОМОГОЮ XDR-СИСТЕМИ

ESET INSPECT

- Сліди сканування інфраструктури зловмисниками
- Модифіковані локальні записи адміністраторів
- Шифрування через планувальник задач
- Видалення всіх тіньових копій файлів після шифрування

ОСОБЛИВОСТІ РОЗСЛІДУВАННЯ КІБЕРІНЦИДЕНТУ

Гібридність і розгалуженість інфраструктури ускладнює розслідування атаки

Відсутність досвіду та достатньої компетенції у співробітників атакованої компанії щодо розслідування кіберінцидентів

Швидкий доступ до будь-яких ресурсів компанії

Додаткові технології захисту та журнали від хмарного провайдера

Зручний процес відновлення систем з резервних копій

ВИСНОВКИ ЗА РЕЗУЛЬТАТАМИ РОЗСЛІДУВАННЯ

- Розслідування кіберінциденту в гібридній інфраструктурі є більш комплексним та розгалуженим процесом порівняно з розслідуванням в локальному середовищі.
- Використання локальних консолей управління для продуктів з безпеки та інструментів адміністрування в гібридній інфраструктурі є не найкращою практикою.
- Хмарні середовища, хоч і є більш надійними і безпечними порівняно з локальними, все одно потребують комплексних підходів до безпеки.
- Людський ресурс є однією з основних складових ефективного захисту.

РЕКОМЕНДАЦІЇ

Захист всіх облікових записів організації за допомогою використання багатофакторної автентифікації

Використання XDR-рішення для виявлення підозрілої та аномальної активностей, а також реагування на них

Постійне підвищення кваліфікації спеціалістів з кібербезпеки

Перехід на хмарні консолі управління продуктами з безпеки

Створення та тестування сценаріїв аварійного відновлення (Disaster Recovery Plan)

ДОДАТКОВІ РІВНІ ЗАХИСТУ

Багатофакторна автентифікація	ESET SECURE AUTHENTICATION
XDR-рішення	ESET INSPECT
Кваліфіковані спеціалісти	ESET СЕРВІСИ
Хмарна консоль управління	ESET PROTECT CLOUD
Аварійне відновлення	ESET РІШЕННЯ ТА СЕРВІСИ

Digital Security
Progress. Protected.

СЕРВІСИ ДЛЯ КОРПОРАТИВНИХ КОРИСТУВАЧІВ

ПРЕМІУМ-ПІДТРИМКА

		ESET PREMIUM SUPPORT ESSENTIAL	ESET PREMIUM SUPPORT ADVANCED	ESET DEPLOYMENT & UPGRADE	ESET HEALTHCHECK
Час реагування на критичні питання	Звичайний	2 години	2 години		
Час реагування на питання середнього рівня	Звичайний	4 години	4 години		
Час реагування на загальні питання	Звичайний	1 робочий день	1 робочий день		
Доступність служби технічної підтримки	365/24/7	365/24/7	365/24/7		
Кількість звернень	Необмежена	Необмежена	Необмежена		
Пріоритет в черзі викликів	✗	Так	Так		
Кількість запитів преміум-класу	✗	Необмежена	Необмежена		
Виділений спеціаліст	✗	✗	Так		
Пріоритетний розгляд запитів розробником	✗	✗	Так		
Проактивне інформування	✗	✗	Так		
Розгортання та модернізація продуктів ESET	✗	✗	1 раз	Так	
Перевірка стану систем захисту	✗	✗	1 раз		Так
Термін дії послуги		1, 2, 3 роки	1, 2, 3 роки	Разова	Разова

СЕРВІСИ З БЕЗПЕКИ

КАТЕГОРІЇ АКТИВНОСТЕЙ	АКТИВНОСТІ		ESET DETECTION AND RESPONSE ESSENTIAL	ESET DETECTION AND RESPONSE ADVANCED	ESET DETECTION AND RESPONSE ULTIMATE
Час реагування		Звичайний	Гарантований час реагування	Гарантований час реагування	Гарантований час реагування
Підтримка з безпеки робочих станцій	Шкідливе програмне забезпечення: невиявлені об’єкти	Так	Так	Так	Так
	Шкідливе програмне забезпечення: проблема очищення	Так	Так	Так	Так
	Шкідливе програмне забезпечення: інфікування програмами-вимагачами	Так	Так	Так	Так
	Помилкові спрацювання	Так	Так	Так	Так
	Загальне: дослідження підозрілої поведінки	Так	Так	Так	Так
Розслідування інцидентів та реагування	Базовий аналіз файлів	✗	Так	Так	Так
	Детальний / Поглиблений аналіз файлів	✗	Так	Так	Так
	Аналіз та розслідування інцидентів	✗	Так	Так	Так
	Допомога у реагуванні на виявлені інциденти	✗	Так	Так	Так
Супроводження системи виявлення та реагування (для користувачів ESET Inspect)	Підтримка – створення або корегування правил	✗	✗	Так	Так
	Підтримка – створення або корегування виключень до правил	✗	✗	Так	Так
	Загальне: питання, пов'язані з ESET Inspect	✗	✗	Так	Так
	ESET Inspect: первинна оптимізація	✗	✗	Так	Так
	ESET Inspect: Threat Hunting (за запитом)	✗	✗	Так	Так
Сервіс з безпеки (для користувачів ESET Inspect)	ESET Inspect: Threat Monitoring	✗	✗	✗	Так
	ESET Inspect: Threat Hunting (проактивний)	✗	✗	✗	Так
Додаткові преміум-сервіси	Розгортання та модернізація рішень ESET	✗	✗	✗	Так

УСІ НЕОБХІДНІ РІВНІ ЗАХИСТУ В ОДНОМУ РІШЕННІ ESET!

ESET PROTECT – єдина платформа з підтримкою XDR

- Консоль управління
- Захист робочих станцій
- Захист серверів
- Розширений аналіз у хмарі
- Повнодискове шифрування
- Захист поштових серверів
- Захист хмарних додатків
- Управління уразливостями та виправленнями

Детальніше

- Консоль управління
- Захист робочих станцій
- Захист серверів
- Розширений аналіз у хмарі
- Повнодискове шифрування
- Захист поштових серверів
- Захист хмарних додатків
- Управління уразливостями та виправленнями
- Виявлення та реагування
- Двофакторна автентифікація

Детальніше

- Консоль управління
- Захист робочих станцій
- Захист серверів
- Розширений аналіз у хмарі
- Повнодискове шифрування
- Захист поштових серверів
- Захист хмарних додатків
- Управління уразливостями та виправленнями
- Виявлення та реагування
- Двофакторна автентифікація
- Сервіси

Детальніше

Digital Security
Progress. Protected.

TELEGRAM-КАНАЛ НОВИН

ОФІЦІЙНИЙ САЙТ