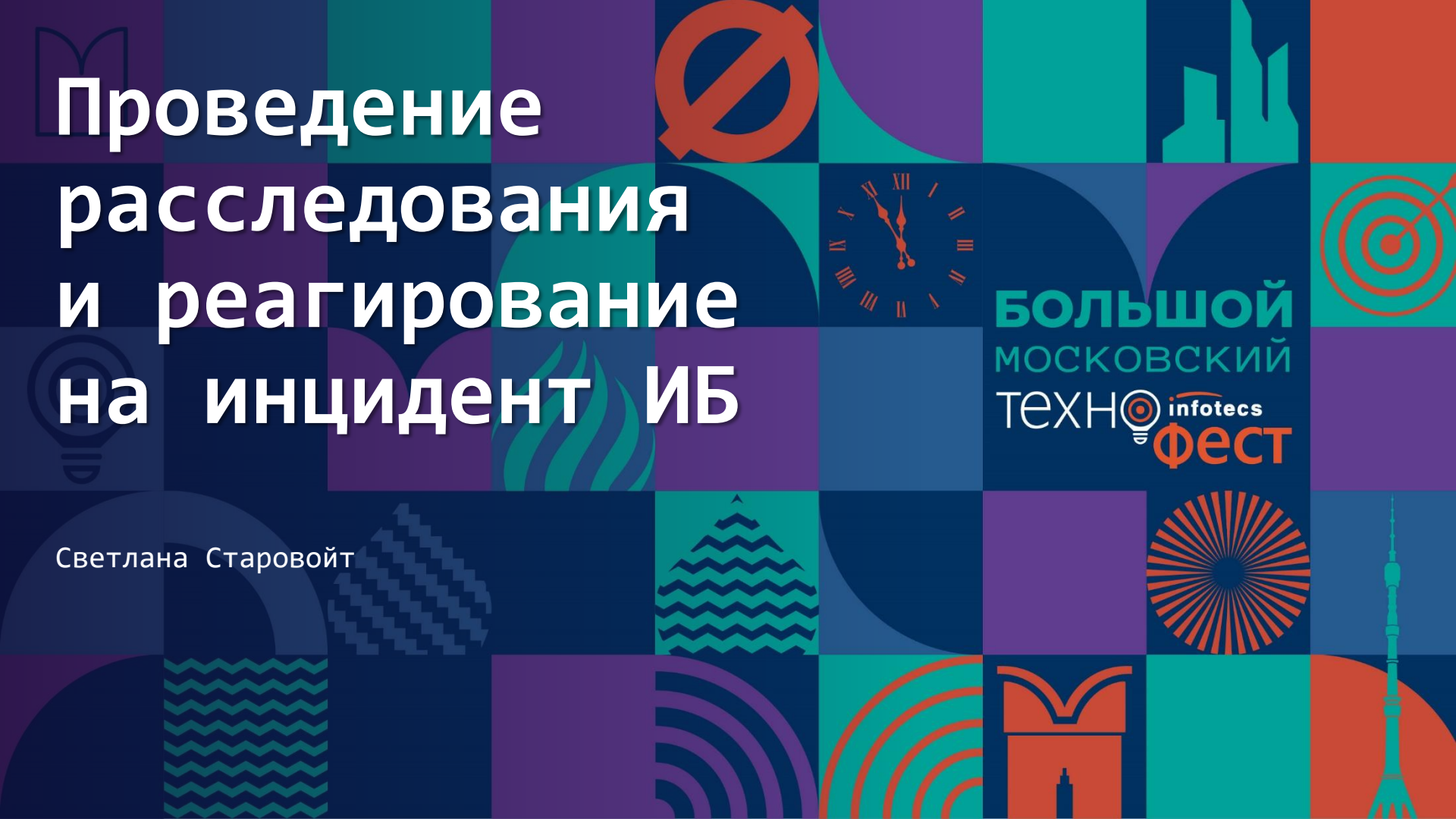
Проведение расследования и реагирование на инцидент ИБ

Светлана Старовойт



Новые сценарии IDS MC и IDS NS

Интеграция с Prime

Управление конфигурациями правил Coordinator HW5

Проверка наличия IoC в БРП IDS NS

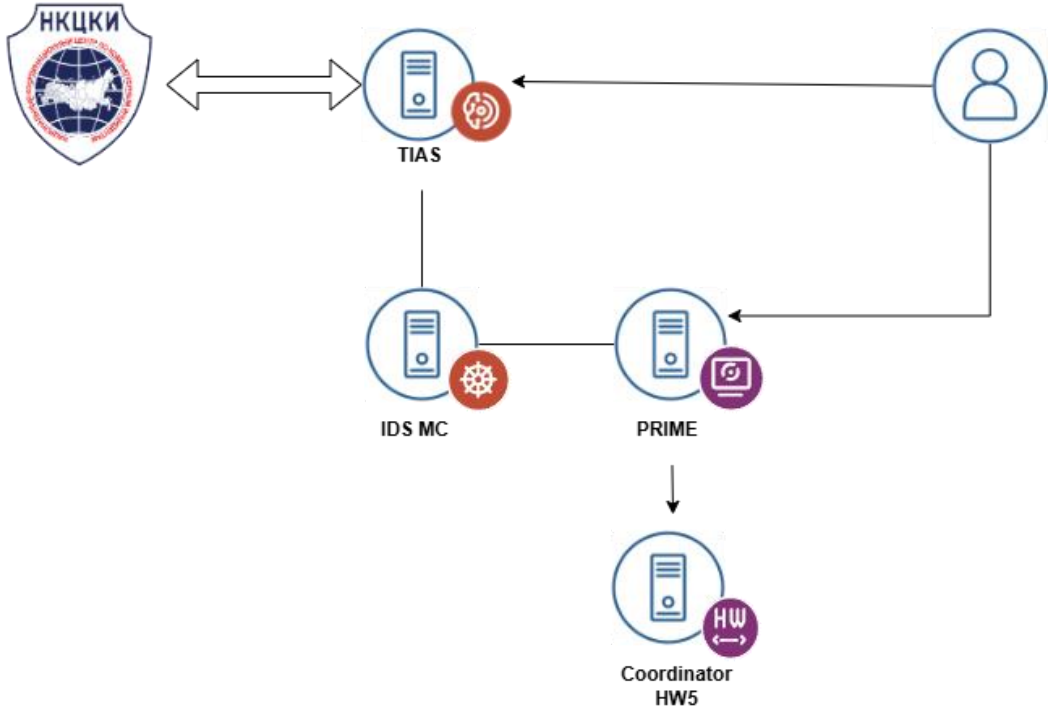
Новые сценарии в TIAS

Ретроспективный анализ событий

Взаимодействие с НКЦКИ через API

Фильтры для событий и инцидентов

Схема стенда



IDS MC зарегистрирован в Prime как модуль

Установлено взаимодействие с НКЦКИ

Coordinator HW5 - шлюз безопасности в Инфотекс Москва

Демо

Реагирование: блокировка трафика с задействованных узлов

Сигнатурные инциденты

Эксплуатация уязвимости CVE-2024-21412 (тип метаправила «Последовательность событий»)

Обращение к фишинговому доменному имени (тип метаправила «ML-событие»)

Эвристический инцидент

Классификатором обнаружена подозрительная активность (модель SID-Chain)

Отправка конфигурации правил из IDS MC на Coordinator HW5

Блокировка входящего и исходящего трафика от атакованных узлов `10.10.1.22` и `10.10.2.22`

Блокировка входящего трафика от атакующего узла `195.58.54.39`

Реагирование: уведомление НКЦКИ об инциденте

ТЕХНО infotecs ФЕСТ

Сигнатурные инциденты

Эксплуатация уязвимости CVE-2024-21412 (тип метаправила «Последовательность событий»)

Обращение к фишинговому доменному имени (тип метаправила «ML-событие»)

Эвристический инцидент

Классификатором обнаружена подозрительная активность (модель SID-Chain)

Ретроспективный инцидент

Классификатором обнаружена подозрительная активность (модель SID-Chain)

Отправка уведомления об инциденте из TIAS в НКЦКИ по API

Уведомление о компьютерном инциденте

Отработка бюллетеня с описанием угрозы

Проверка IoC

Реагирование: ложноположительный инцидент

Сигнатурный инцидент

Множественные попытки доступа по RDP к узлу контролируемой сети

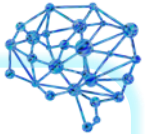
Создание правила фильтрации событий

Правило для фильтрации ложноположительного инцидента

Регистрация автообработанного инцидента

Инцидент со статусом «Обработан автоматически»

Помощь в расследовании



Эвристический инцидент

Цепочка событий из инцидента

AI Ассистент

Разбор событий с привязкой к тактикам и техникам Mitre

Интерпретация результатов

Описание действий злоумышленника

Основные техники

Релевантные документы

ТЕХНО infotecs ФЕСТ

Подписывайтесь
на наши соцсети,
там много интересного

CYBER MEDIA
NBJ НАЦИОНАЛЬНЫЙ БАНКОВСКИЙ ЖУРНАЛ
GLOBAL DIGITAL SPACE
CISOCLUB
РУТОКЕН
ПЕРСПЕКТИВНЫЙ МОНИТОРИНГ
АВАНГАРД
AR integ
АТБ ЭЛЕКТРОНИКА
infotecs {/-cademy}
merlion
УЧЕБНЫЙ ЦЕНТР ИНФОТЕКС