Информзащита
IZ:SOC

Синергия SOC и DFIR в обеспечении ИБ

Особенности построения процессов взаимодействия команд SOC и DFIR, позитивные и негативные стороны взаимодействия команд

02 Ключевые задачи SOC

Мониторинг

Threat hunting

Обнаружение угроз

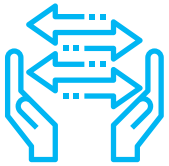
Vulnerability management

Реагирование на инциденты

03 Ключевые задачи DFIR

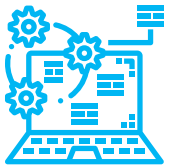
Расследование компьютерных преступлений

Восстановление потерянных/удалённых данных (карвинг)



Оперативное получение цифровых артефактов

Выработка рекомендаций по предотвращению инцидентов

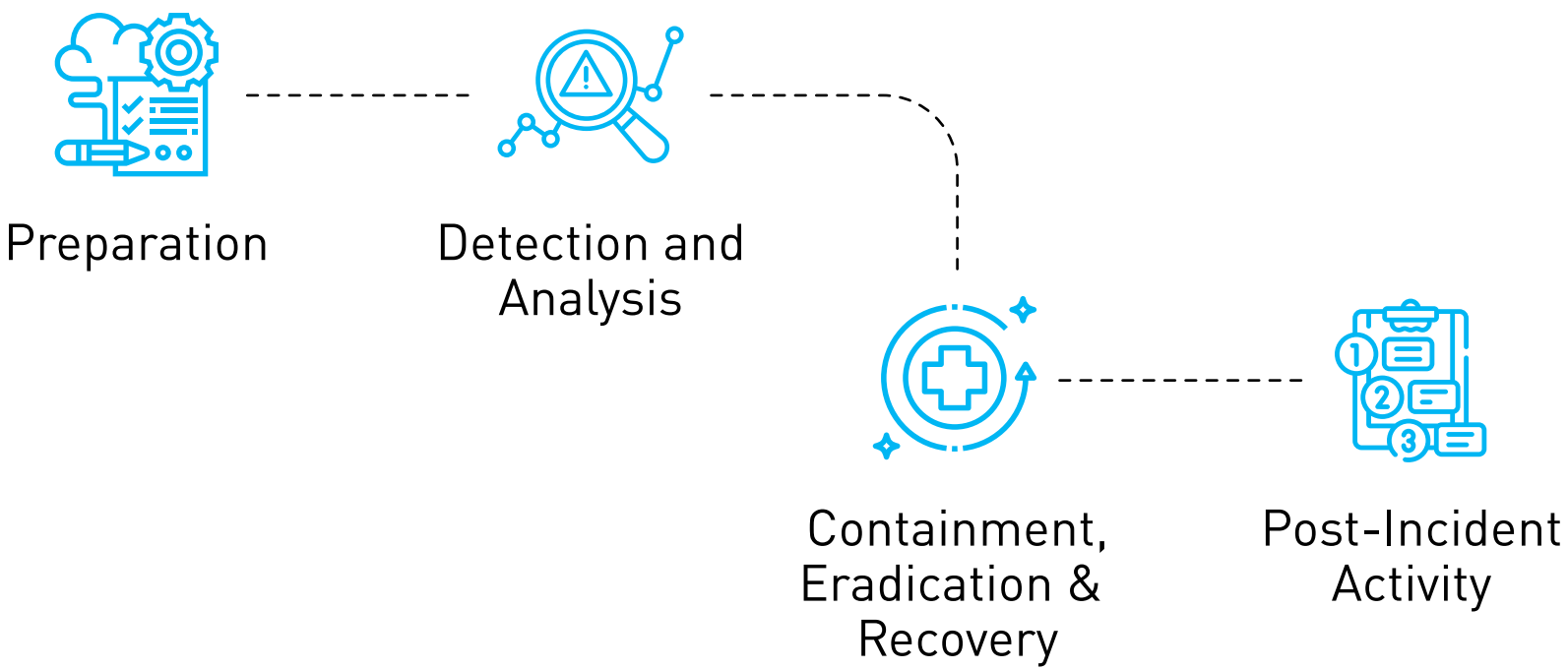


Обратная разработка вредоносного ПО (MA/RE)

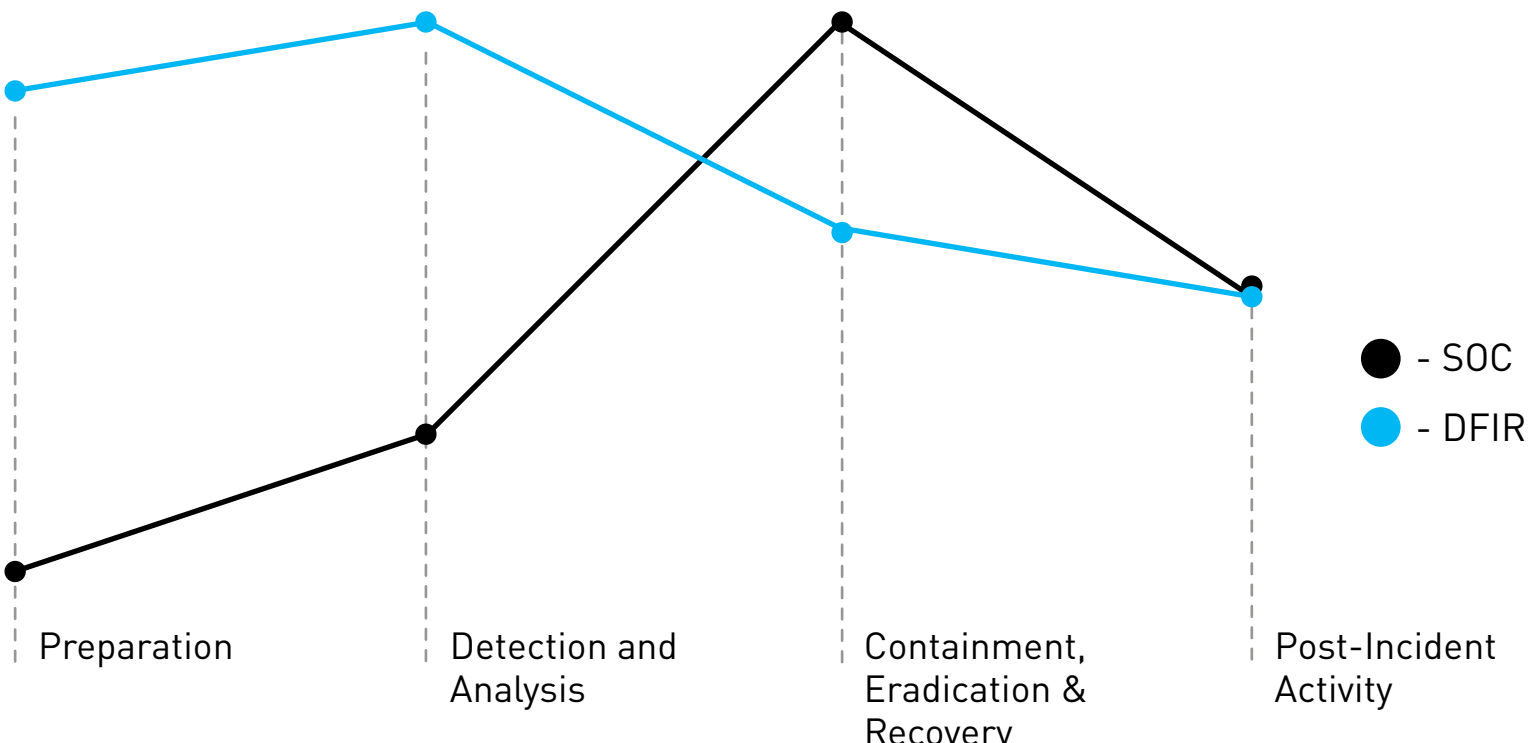
Анализ дампов оперативной памяти

DFIR

04 Жизненный цикл инцидента



05 Вовлечение в процессах реагирования на инциденты



06 Preparation

SOC Team

- Инвентаризация активов
- Харденинг инфраструктуры
- Подключение источников к непрерывному мониторингу
- Изучение информации о новых угрозах
- Профилирование детектирующих правил под конкретную инфраструктуру и бизнес-процессы
- Построение каналов коммуникации с ключевыми лицами
- Разработка playbook-ов
- EPS-оцид!!!

DFIR Team

- Подготовка машинных носителей для копирования цифровых свидетельств/артефактов
- Подготовка стендов для анализа цифровых артефактов
- Подготовка инфраструктуры для оперативного получения цифровых артефактов

SOC DFIR

07 Detection and Analysis

SOC Team

- Непрерывный мониторинг
- Анализ алертов от систем безопасности
- Профилирование сетей и систем
- Приоритезация инцидентов
- Threat Hunting
- Оповещение ключевых лиц при возникновении инцидентов

DFIR Team

- Анализ цифровых артефактов
- Подтверждение/опровержение угроз
- Оперативное получение цифровых артефактов

SOC DFIR

08 Containment, Eradication & Recovery (CER)

SOC Team

- Определение скоупа инцидента
- Получение цифровых свидетельств/артефактов
- Взаимодействие с администраторами/владельцами бизнес-процессов

DFIR Team

- Определение стратегии сдерживания
- Сохранение цифровых свидетельств/артефактов для их передачи в сдубные инстанции/правоохранительные органы
- Атрибуция атакующего
- Восстановление хронологии инцидента

SOC DFIR

09 Post-Incident Activity

SOC Team

- Доработка детектирующих правил корреляции
- Разработка новых правил корреляции
- Оптимизация процессов реагирования и обнаружения инцидентов

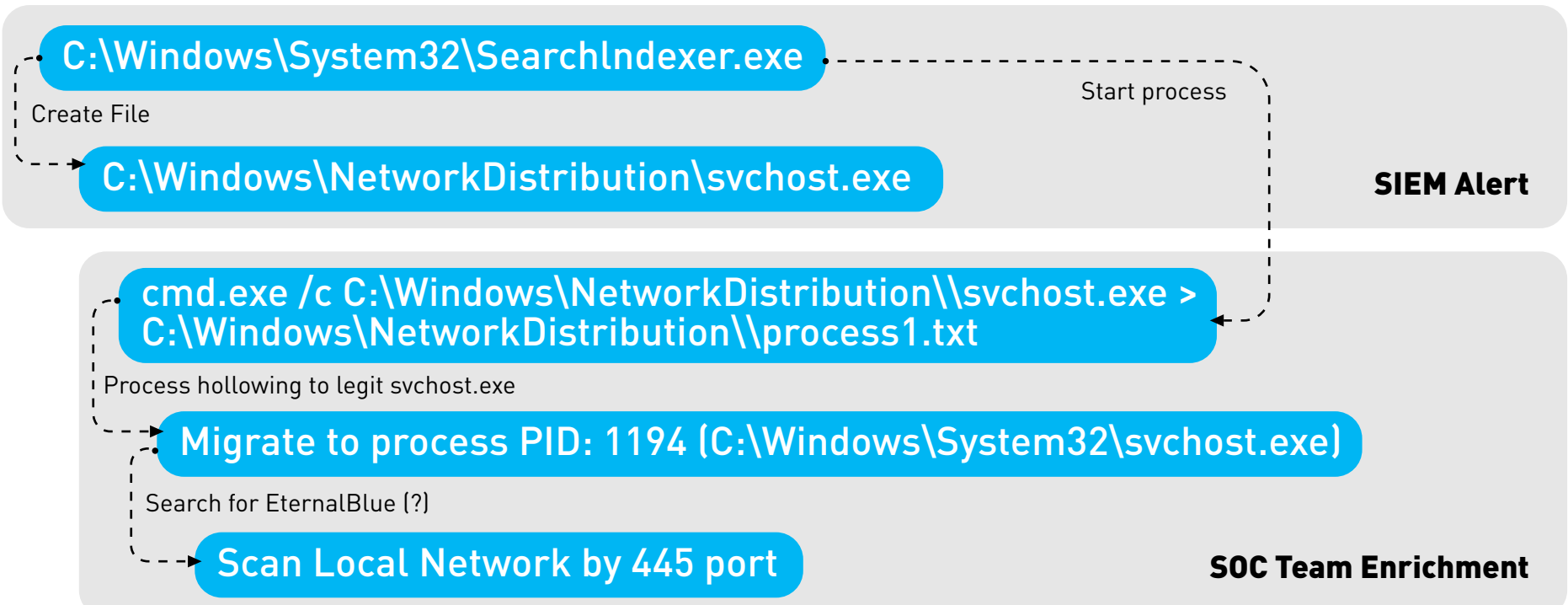
DFIR Team

- Наполнение TI-базы об угрозах
- Восстановление утерянных данных (при возможности)
- Написание отчёта по инциденту
- Выявление слабых мест в инфраструктуре, которые были использованы атакующими

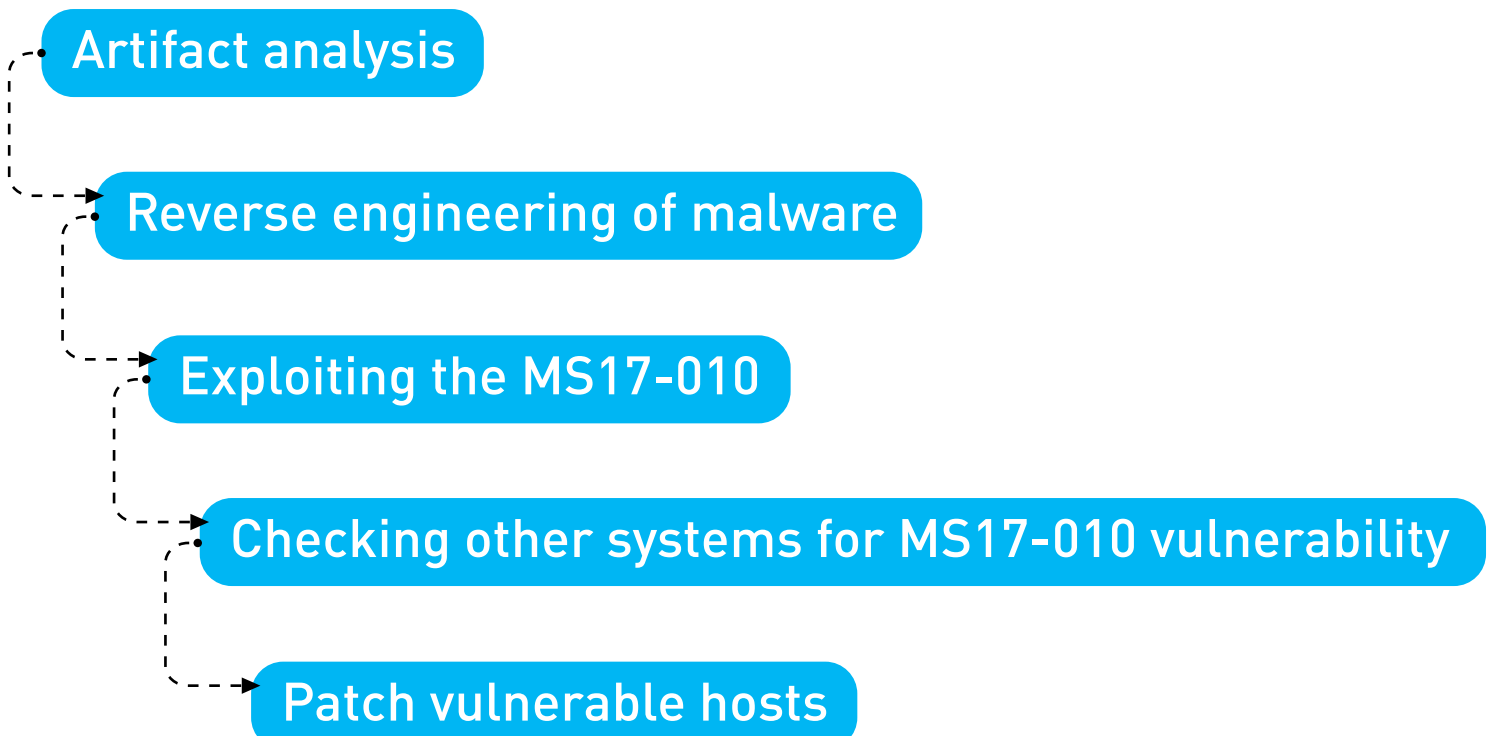
SOC DFIR

10 Обработка алертов от SIEM

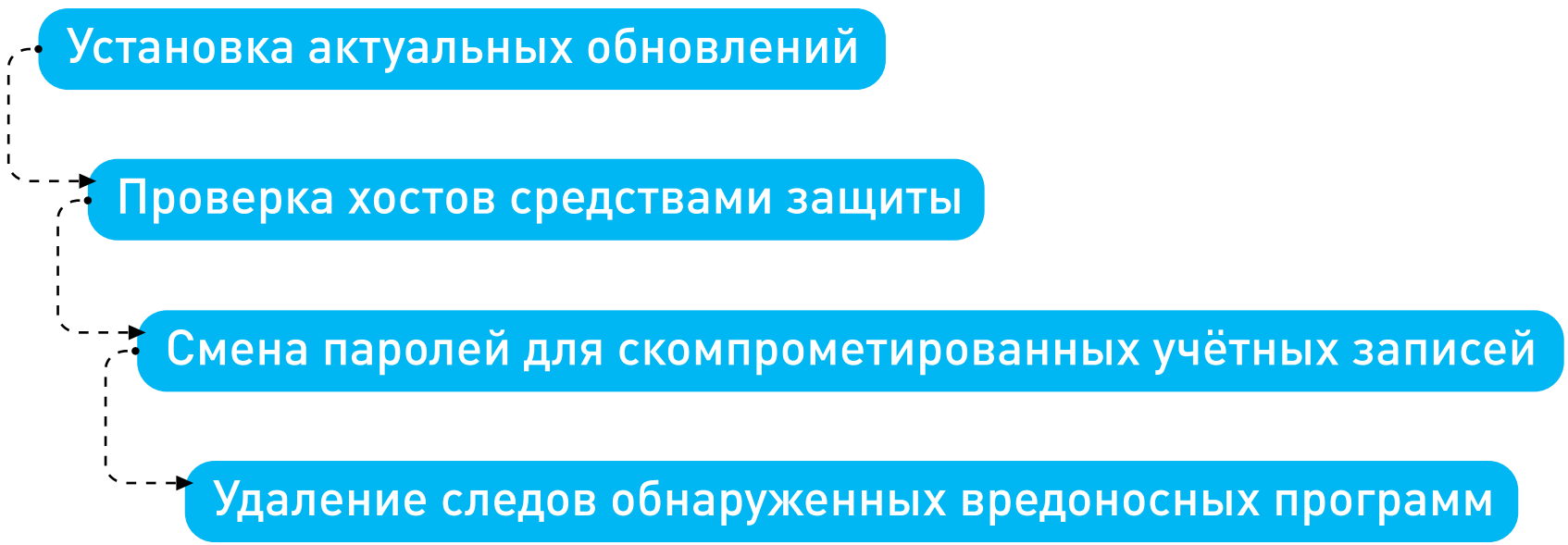
11 Case №1


C:\Windows\System32\SearchIndexer.exe
Create File
Start process
C:\Windows\NetworkDistribution\svchost.exe
SIEM Alert
cmd.exe /c C:\Windows\NetworkDistribution\\svchost.exe > C:\Windows\NetworkDistribution\\process1.txt
Process hollowing to legit svchost.exe
Migrate to process PID: 1194 (C:\Windows\System32\svchost.exe)
Search for EternalBlue (?)
Scan Local Network by 445 port
SOC Team Enrichment

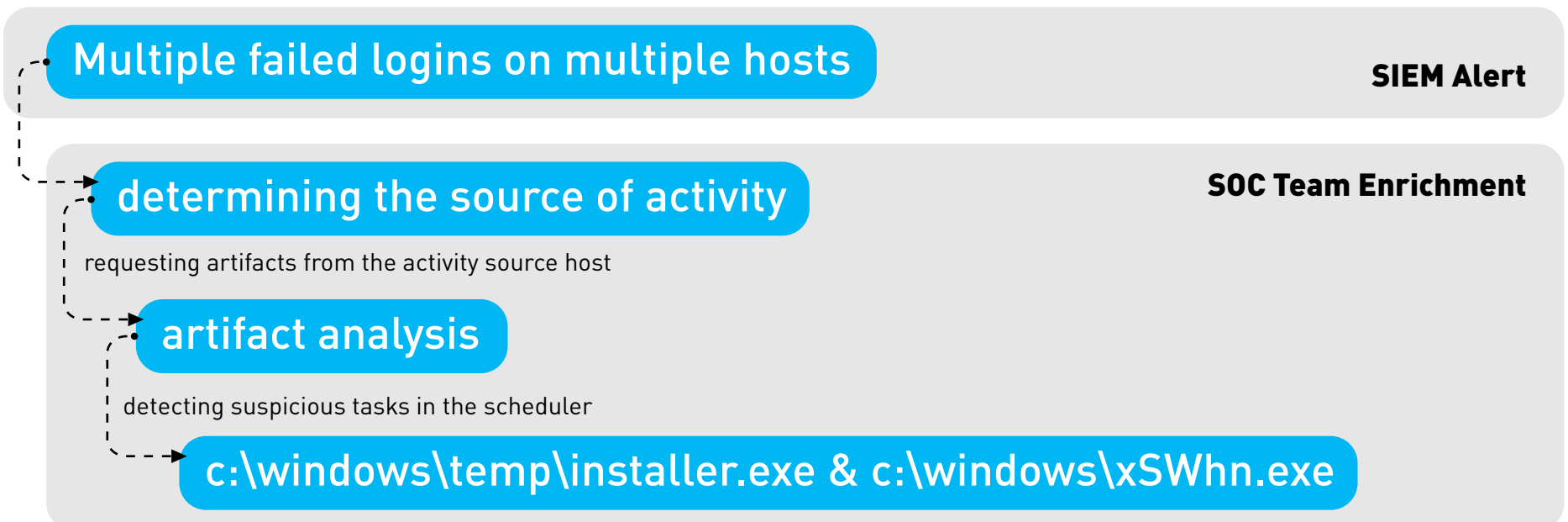
12 Case №1


Artifact analysis
Reverse engineering of malware
Exploiting the MS17-010
Checking other systems for MS17-010 vulnerability
Patch vulnerable hosts

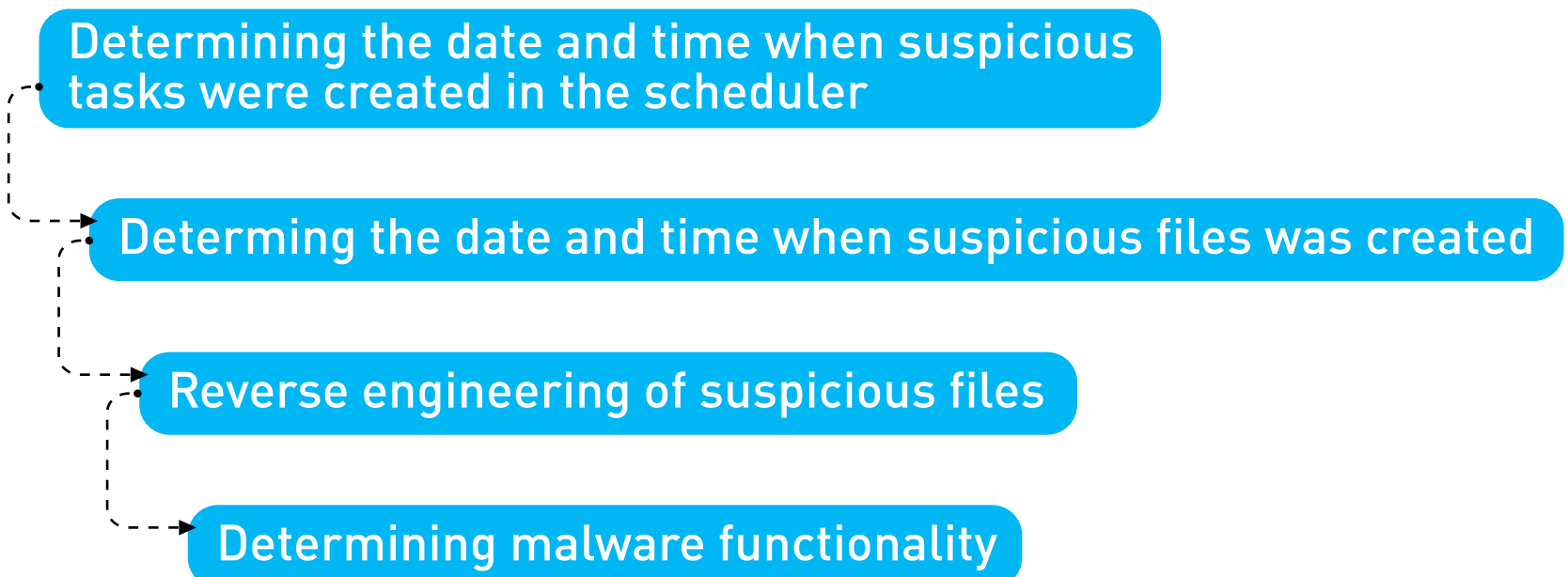
13 Case №1


Установка актуальных обновлений
Проверка хостов средствами защиты
Смена паролей для скомпрометированных учётных записей
Удаление следов обнаруженных вредоносных программ

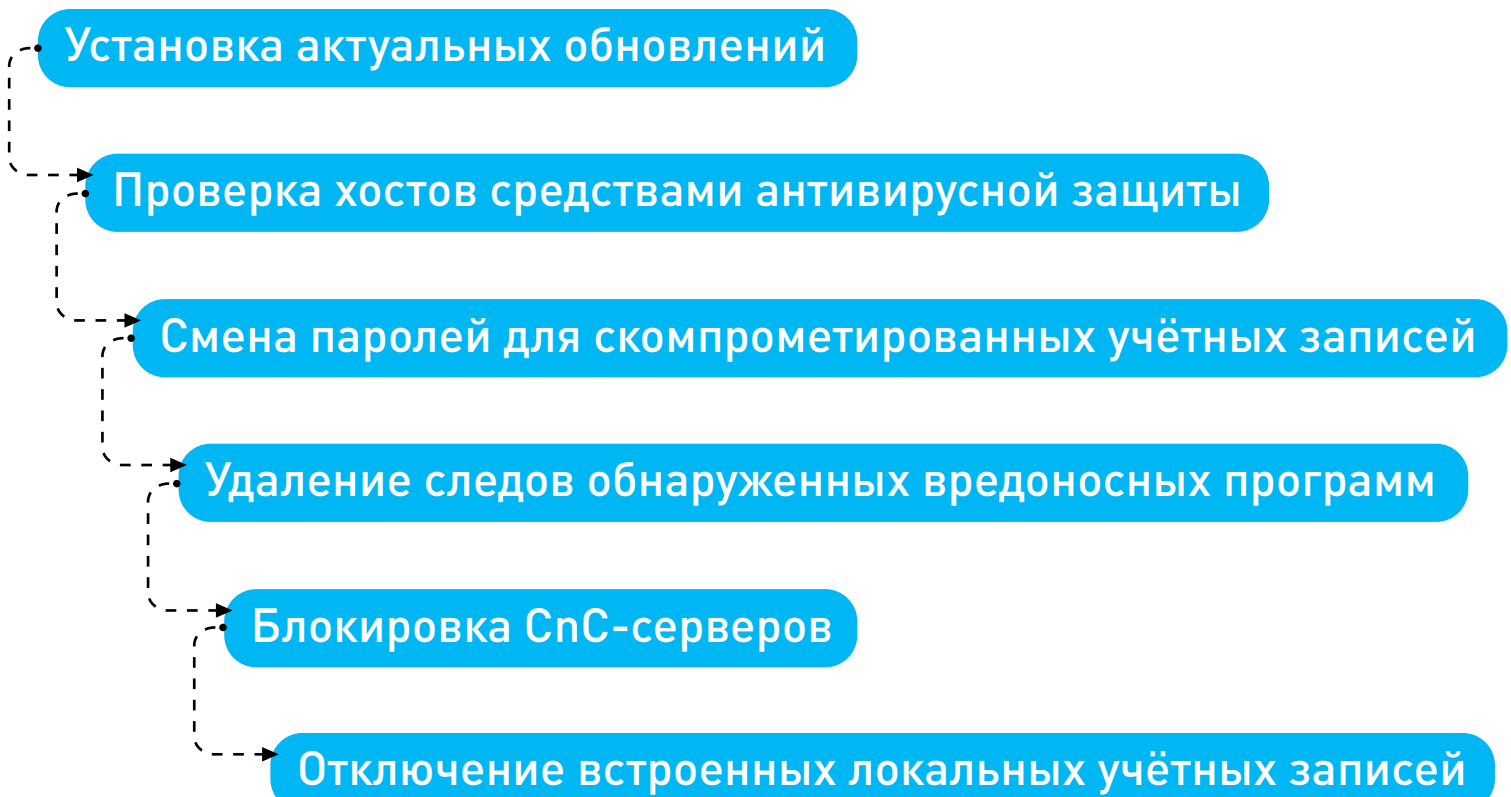
14 Case №2


Multiple failed logins on multiple hosts
SIEM Alert
determining the source of activity
SOC Team Enrichment
requesting artifacts from the activity source host
artifact analysis
detecting suspicious tasks in the scheduler
c:\windows\temp\installer.exe & c:\windows\xSWhn.exe

15 Case №2

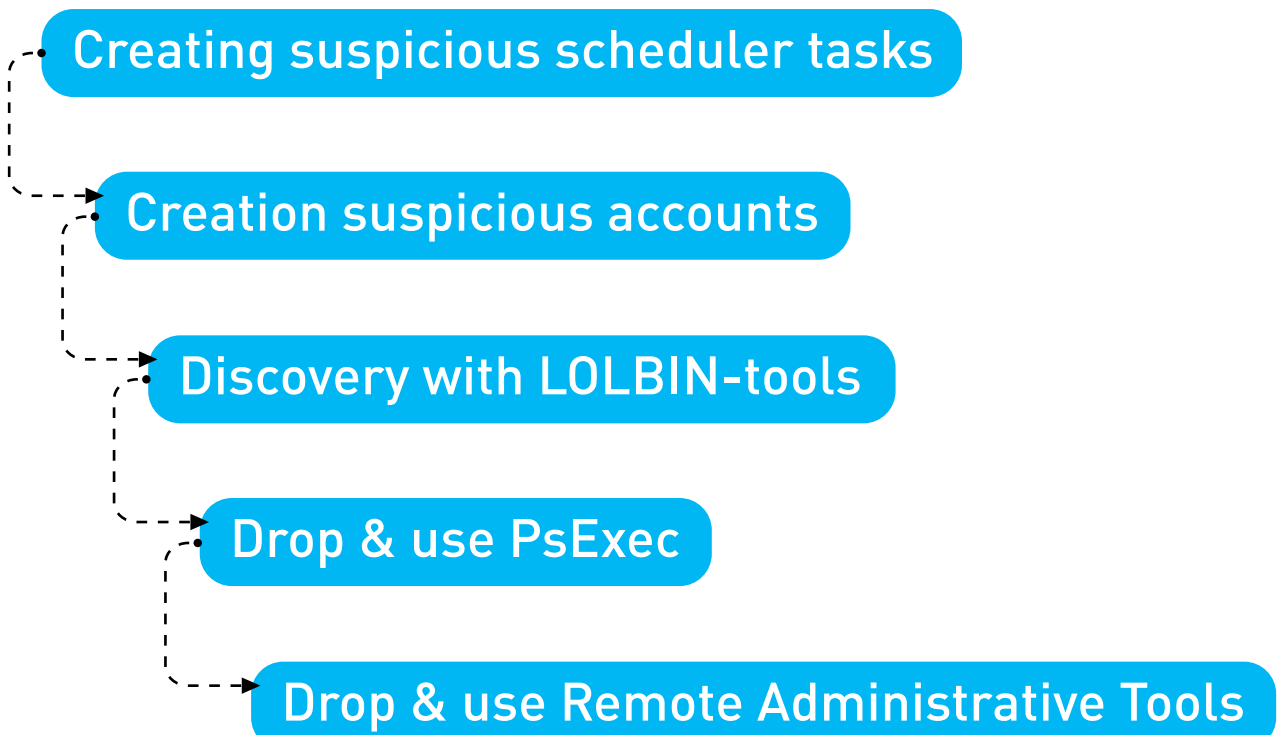

Determining the date and time when suspicious tasks were created in the scheduler
Determing the date and time when suspicious files was created
Reverse engineering of suspicious files
Determining malware functionality

Case №2

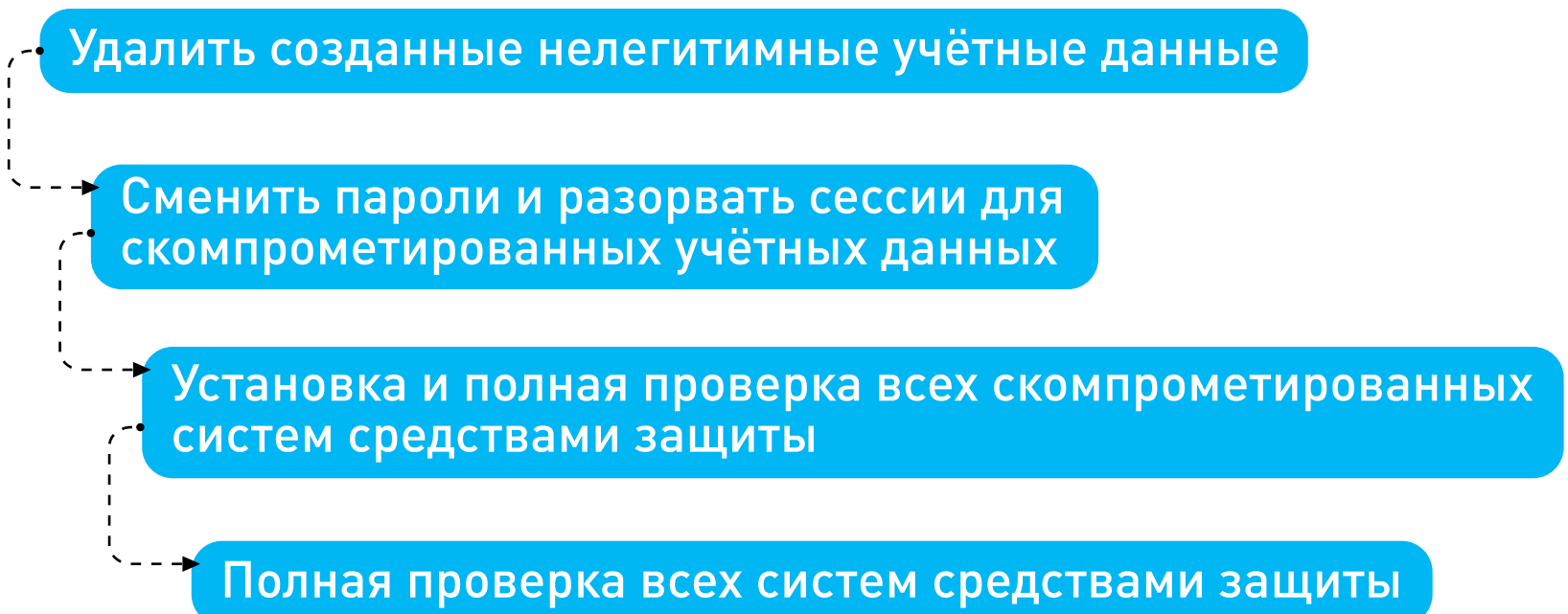

Установка актуальных обновлений
Проверка хостов средствами антивирусной защиты
Смена паролей для скомпрометированных учётных записей
Удаление следов обнаруженных вредоносных программ
Блокировка CnC-серверов
Отключение встроенных локальных учётных записей

17 Ретроспективный анализ

18 Case №3


Creating suspicious scheduler tasks
Creation suspicious accounts
Discovery with LOLBIN-tools
Drop & use PsExec
Drop & use Remote Administrative Tools

Case №3


Удалить созданные нелегитимные учётные данные
Сменить пароли и разорвать сессии для скомпрометированных учётных данных
Установка и полная проверка всех скомпрометированных систем средствами защиты
Полная проверка всех систем средствами защиты

20 Итоги 1

- Сопровождение инцидента на всех стадиях жизненного цикла инцидента
- Выявление и оперативное реагирование на инциденты
- Более полное определение поверхности атаки
- Анализ функциональных возможностей обнаруженного вредоносного ПО
- Больше подходит для коммерческих SOC

Информзащита
IZ:SOC

Информационная безопасность

24x7x365

Центр противодействия кибератакам IZ SOC

+7 495 980 23 45
izsoc@infosec.ru
www.izsoc.ru

Системный интегратор

+7 495 980 23 45
market@infosec.ru
www.infosec.ru

Центр противодействия мошенничеству

antifraud@infosec.ru

Сервисный центр

+7 495 981 92 22
support@itsoc.ru
www.itsoc.ru

Пресс-служба

pr@infosec.ru