SOC
FORUM
2023

Platformix

Кибератака на инфраструктуру Platformix

Публичный разбор инцидента информационной безопасности
и механизмов реагирования ИТ-компании со зрелым подходом к ИБ

SOC
FORUM
2023

Виталий Масютин

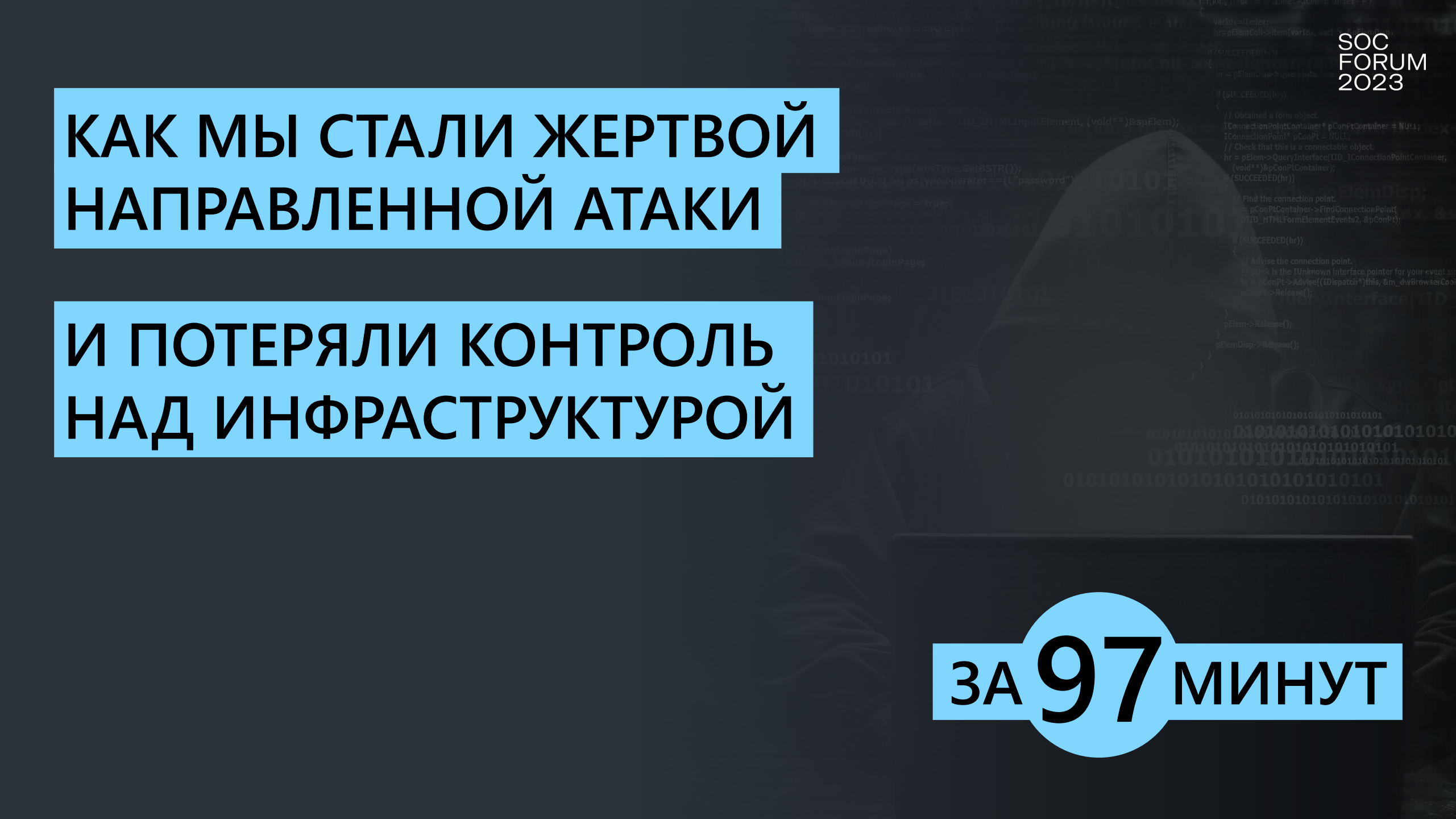
Заместитель директора департамента информационной безопасности

Platformix

SOC FORUM 2023

КАК МЫ СТАЛИ ЖЕРТВОЙ НАПРАВЛЕННОЙ АТАКИ

И ПОТЕРЯЛИ КОНТРОЛЬ НАД ИНФРАСТРУКТУРОЙ



ЗА 97 МИНУТ

МЫ, КАК ОБЪЕКТ АТАКИ

SOC FORUM 2023

ГК «БАЗОВЫЕ РЕШЕНИЯ»

Предлагает полный спектр решений и услуг в области построения надежных санкционно-устойчивых корпоративных ИТ-инфраструктур

Platformix

Системный интегратор
Создание, защита и развитие ИТ-инфраструктур заказчиков с 1992 года

СИЛА

Вендор
Производство корпоративного ИТ-оборудования, разработка ПО

450+ человек

Центральный офис в Москве, филиалы, гибридный режим работы

Зрелая система ИБ

Защита от типовых и распространённых атак, усиленная безопасность ключевых систем

Требования регуляторов

Полный комплекс работ по защите персональных данных

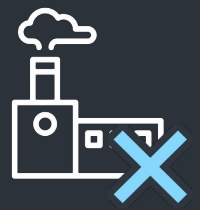
Процессы ИБ

Сертификация ISO 27001

МЫ, КАК ЦЕЛЬ АТАКИ

SOC FORUM 2023

Нас не будут целенаправленно атаковать



КИИ

Производство

Деньги

Данные

Государство

Защита

Осведомленность

Автономность

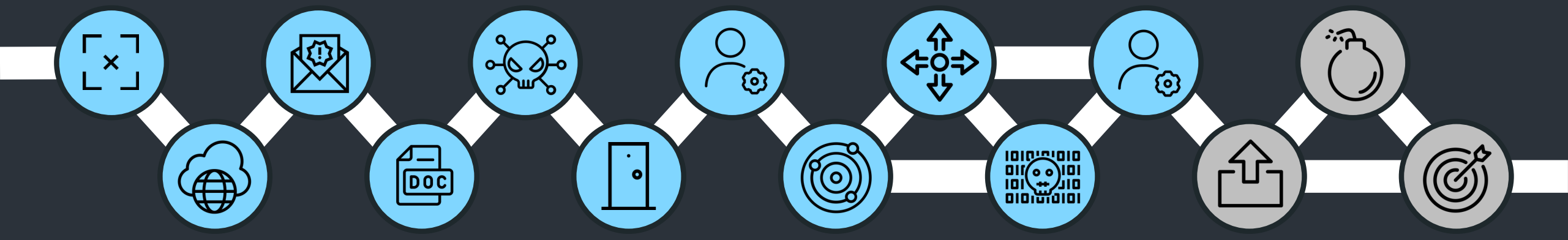
Бэкапы

Нам сложно причинить существенный ущерб

KILLCHAIN

SOC FORUM 2023

ПРОНИКНОВЕНИЕ | **ПРОДВИЖЕНИЕ** | **ЦЕЛЬ**



Разведка
Reconnaissance

Подготовка инфраструктуры
Resource Development
+
Вооружение
Weaponization

Социальная инженерия
Social Engineering
+
Доставка
Delivery

Эксплуатация
Exploitation
+
Выполнение кода
Execution

Закрепление
Persistence

Управление и контроль
Command and Control
+
Туннелирование
Pivoting

Эскалация привилегий
Privilege Escalation
+
Кража УЗ
Credential Access

Обнаружение
Discovery

Горизонтальное продвижение
Literal Movement

Эксплуатация
Exploitation
+
Выполнение кода
Execution

Эскалация привилегий
Privilege Escalation
+
Кража УЗ
Credential Access

Сбор данных
Collection
+
Эксфильтрация данных
Exfiltration

Нанесение ущерба
Impact

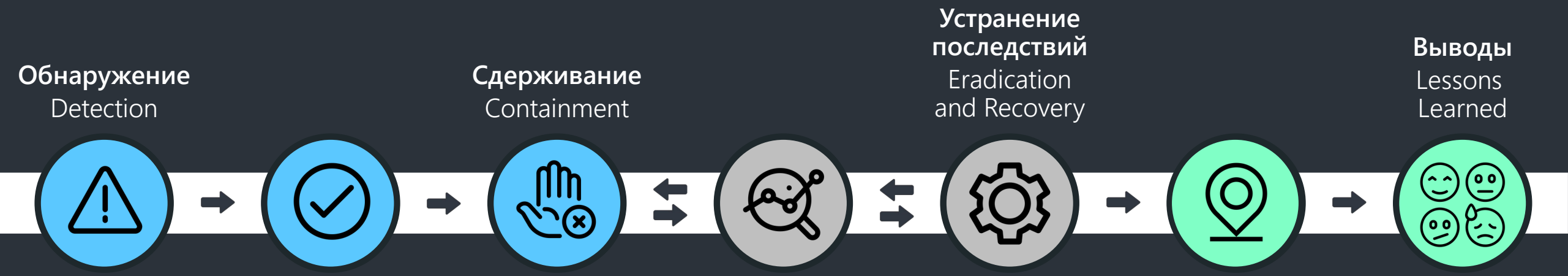
Достижение целей атаки
Objectives

Обход средств защиты | Defence Evasion

РЕАГИРОВАНИЕ НА ИНЦИДЕНТ

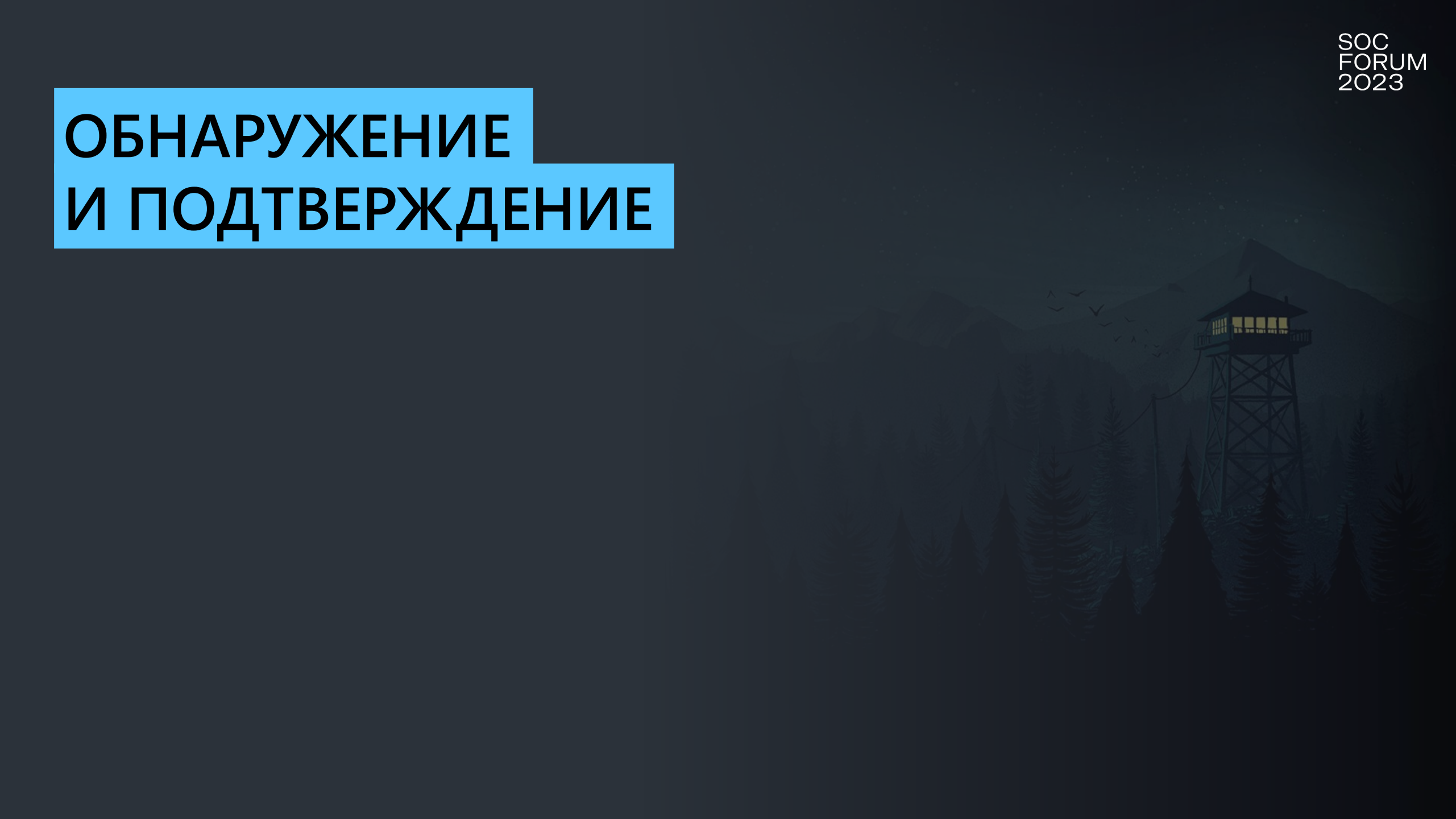
SOC FORUM 2023

ОБНАРУЖЕНИЕ | **РЕАГИРОВАНИЕ** | **ПОСТ-АНАЛИЗ**



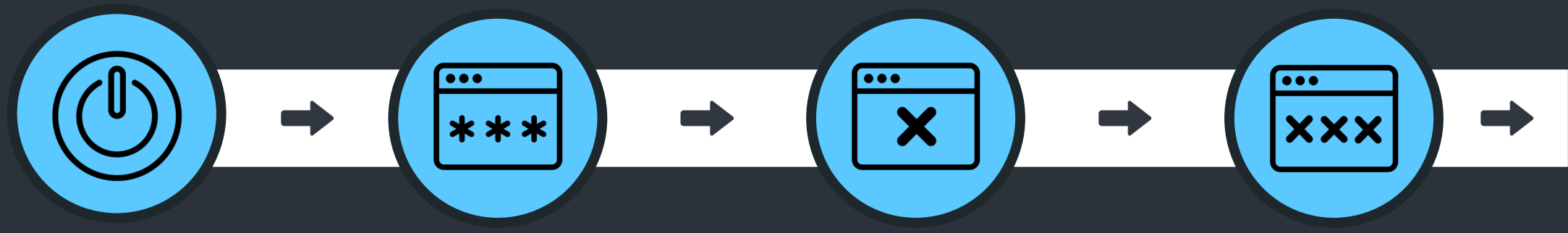
SOC
FORUM
2023

ОБНАРУЖЕНИЕ И ПОДТВЕРЖДЕНИЕ



ОБНАРУЖЕНИЕ И ПОДТВЕРЖДЕНИЕ

SOC FORUM 2023

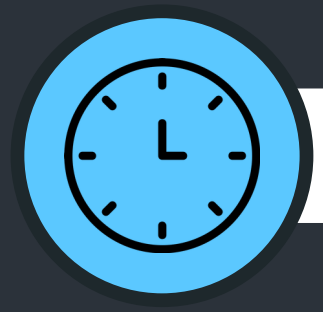


Антивирус начал отключаться на серверах

Администратор пытается подключиться к серверу

Пароль администратора не подходит

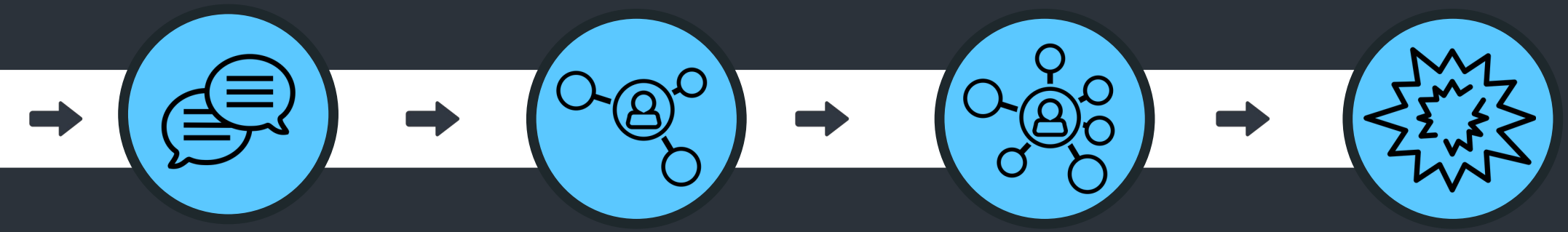
Пароль другого администратора тоже не подходит



СУББОТА, НОЧЬ

ОБНАРУЖЕНИЕ И ПОДТВЕРЖДЕНИЕ

SOC FORUM 2023



Обзвон и уведомление администраторов

Проверка учетных записей администраторов

Проверка учетных записей пользователей

ИНЦИДЕНТ!

СУББОТА, НОЧЬ

SOC
FORUM
2023

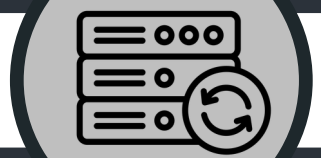
РЕАГИРОВАНИЕ СВОИМИ СИЛАМИ

СДЕРЖИВАНИЕ И АНАЛИЗ

SOC FORUM 2023

ИТ

Сброс паролей администраторов



Проверка состояния резервных копий

Ограничение удаленного доступа

Проверка устройств администраторов

ИБ

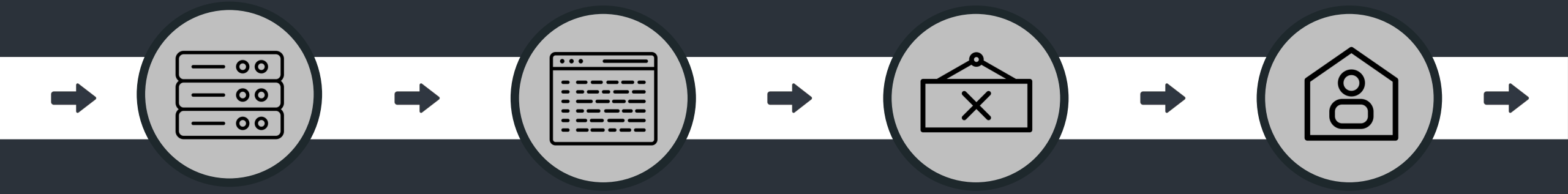
Определение активов для анализа

Первичный анализ журналов событий

Мониторинг в реальном времени

СДЕРЖИВАНИЕ И АНАЛИЗ

SOC FORUM 2023



Проверка состояния ключевых систем

Проверка состояния чувствительных данных

Изоляция и восстановление скомпрометированных устройств

Изоляция и сброс пароля скомпрометированных учетных записей

Анализ удаленных подключений

Анализ изменений устройств

Анализ действий с учетными записями

Анализ взаимодействий с сетью Интернет

ПРОМЕЖУТОЧНЫЕ РЕЗУЛЬТАТЫ

SOC FORUM 2023

Скомпрометированы учетные записи администраторов и пользователей

Скомпрометированы инфраструктурные серверы компании, включая сервер антивирусной защиты

Обнаружен подозрительный драйвер, который применялся ранее при реализации Ransomware-атак

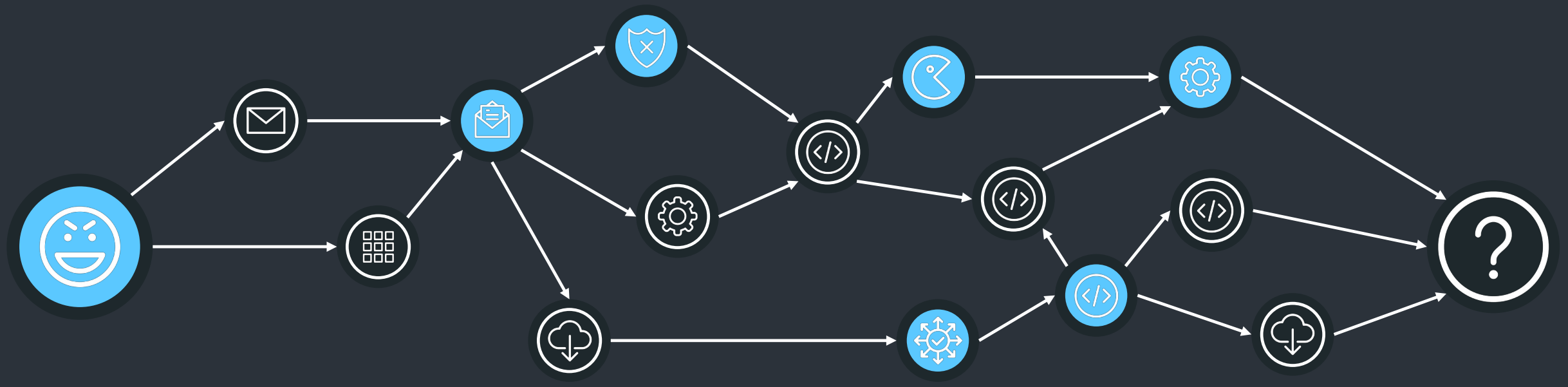
- 5 администраторов и 2 пользователя
- 8 серверов и 7 станций
- 1 драйвер и 2 утилиты
- 1 подозрительный сайт

CUBA RANSOMWARE?

КИТАЙЦЫ?

ПРОМЕЖУТОЧНЫЕ РЕЗУЛЬТАТЫ

SOC FORUM 2023



ЧТО МЫ ЕЩЕ НЕ НАШЛИ?

ЗЛОУМЫШЛЕННИКИ ВСЕ ЕЩЕ ТУТ?

SOC
FORUM
2023

РЕАГИРОВАНИЕ
ПОМОЩЬ СО СТОРОНЫ

СДЕРЖИВАНИЕ И АНАЛИЗ

SOC FORUM 2023

СДЕРЖИВАНИЕ И АНАЛИЗ

SOC FORUM 2023

УСТРАНЕНИЕ ПОСЛЕДСТВИЙ

SOC FORUM 2023

ИТ

Переустановка скомпрометированных активов

Перевыпуск тикетов Kerberos

Массовый сброс паролей учётных записей

Корректировка политик безопасности инфраструктуры

Мониторинг в реальном времени

+

Повышение осведомленности пользователей

ОПЕРАТИВНЫЕ МЕРЫ ПО ИБ

ОЦЕНКА УЩЕРБА

SOC FORUM 2023

21	14	-	-	-
Сервер и рабочая станция	Учетных записей пользо-вателей и администраторов	Кража или потеря информации	Репутационный ущерб	Финансовый ущерб

ВРЕМЯ РАБОТНИКОВ

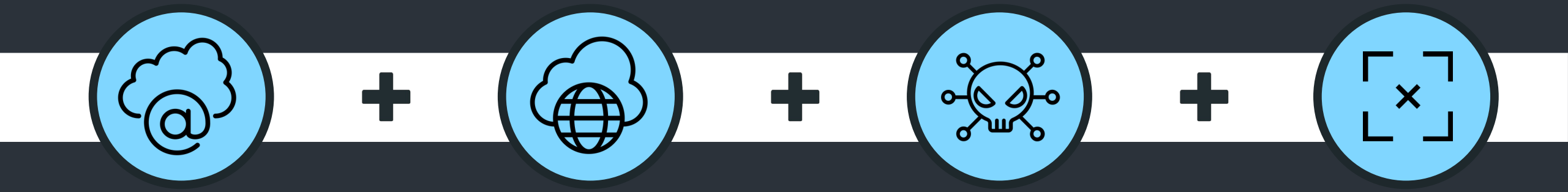
СТОИМОСТЬ ПРИВЛЕЧЕНИЯ СТОРОННЫЕ ОРГАНИЗАЦИИ

SOC
FORUM
2023

РАССЛЕДОВАНИЕ

ПОДГОТОВКА

SOC FORUM 2023



Получен доступ к почте сторонней организации

Создана инфраструктура для реализации атаки

Подобрано редкое вредоносное программное обеспечение

Определены жертвы среди работников Platformix

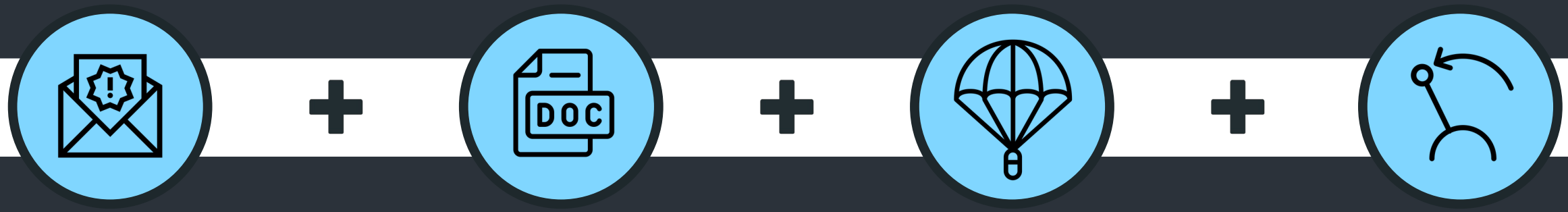
Подписанный драйвер для принудительного отключения антивируса (защищенный VMProtect)

Инструмент для повышения привилегий (UAC Bypass), Утилита для извлечения паролей из памяти

Инструмент для отключения антивируса из ядра ОС

ПРОНИКНОВЕНИЕ

SOC FORUM 2023



28 работников получают фишинговое письмо

1 работник открывает вложенный файл

На машине работника активируется вредоносное ПО

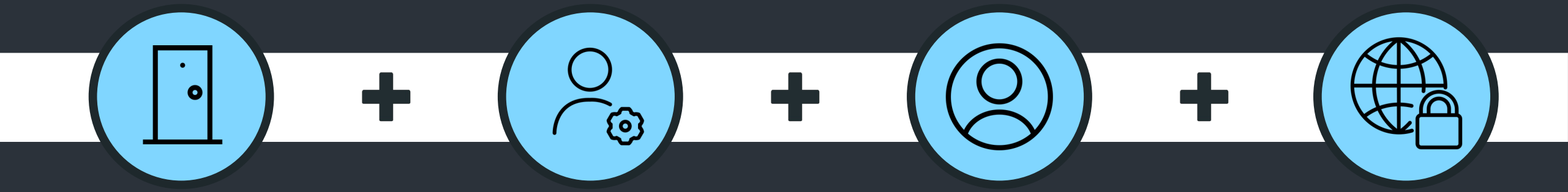
Вредоносное ПО отключает Symantec и Defender

Вложенный файл содержал Trojan.MSOffice.SAgent

Цепочка действий: Malicious Template → VB Script → PS Script → C&C Connection → Malware Execution

ЗАКРЕПЛЕНИЕ

SOC FORUM 2023



Получение интерактивного удаленного доступа

Получение прав локального администратора

Компрометация доменных учетных записей на устройстве

Получение доступа через VPN-шлюз

Использование нескольких вариантов скриптов

Создание локальных учетных записей на скомпрометированных устройствах

Использование дополнительных C&C серверов и IP-адресов

ПРОДВИЖЕНИЕ

SOC FORUM 2023

Использование стандартных утилит для удаленного администрирования и доступа

Создание дополнительных точек закрепления по мере развития атаки

События ИТ-мониторинга привлекли внимание административно

Администраторы быстро сориентировались в обстановке и отреагировали

ВЫВОДЫ

SOC FORUM 2023

НАША СИСТЕМА ЗАЩИТЫ НУЖДАЕТСЯ В УСИЛЕНИИ

SOC FORUM 2023

Email Gateway

Точечная рассылка почты с легитимного адреса сторонней организации, который не был ранее замечен в рассылке спама и фишинговых писем

Web Gateway

Домены/адреса прошли репутационную проверку, модуль Antivirus не выявил ничего опасного или подозрительного

Firewall

Исходящий трафик попал под разрешающие правила, модули безопасности не выявили признаков атаки

Anti-Virus

Антивирус не обнаружил вредоносное ПО, которое отключило антивирус

+

Sandbox

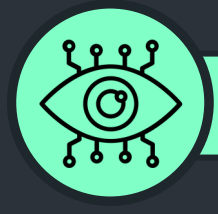
Интеграция со средствами защиты периметра, анализ поведения файлов и объектов в контролируемой среде

EDR

Контроль состояния, активности и изменений на конечных устройствах для защиты от неизвестных угроз

MFA

Многофакторная аутентификация для удаленного и административного доступа

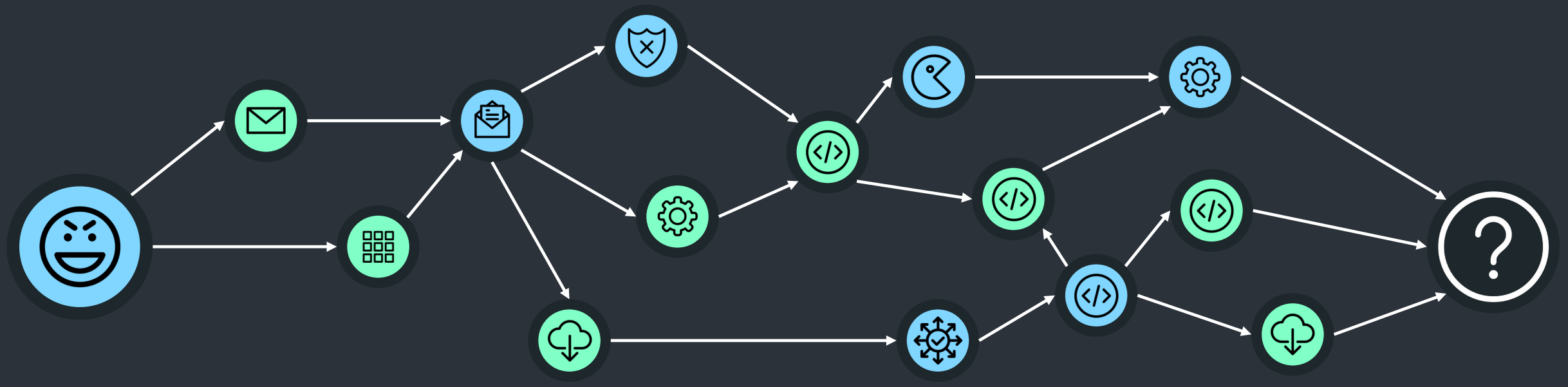


SIEM

Мониторинг и выявление инцидентов информационной безопасности

СИСТЕМА МОНИТОРИНГА

SOC FORUM 2023



Анализ трафика, файлов и событий

Слепых зон не остается

РЕАГИРОВАНИЕ НА ИНЦИДЕНТЫ

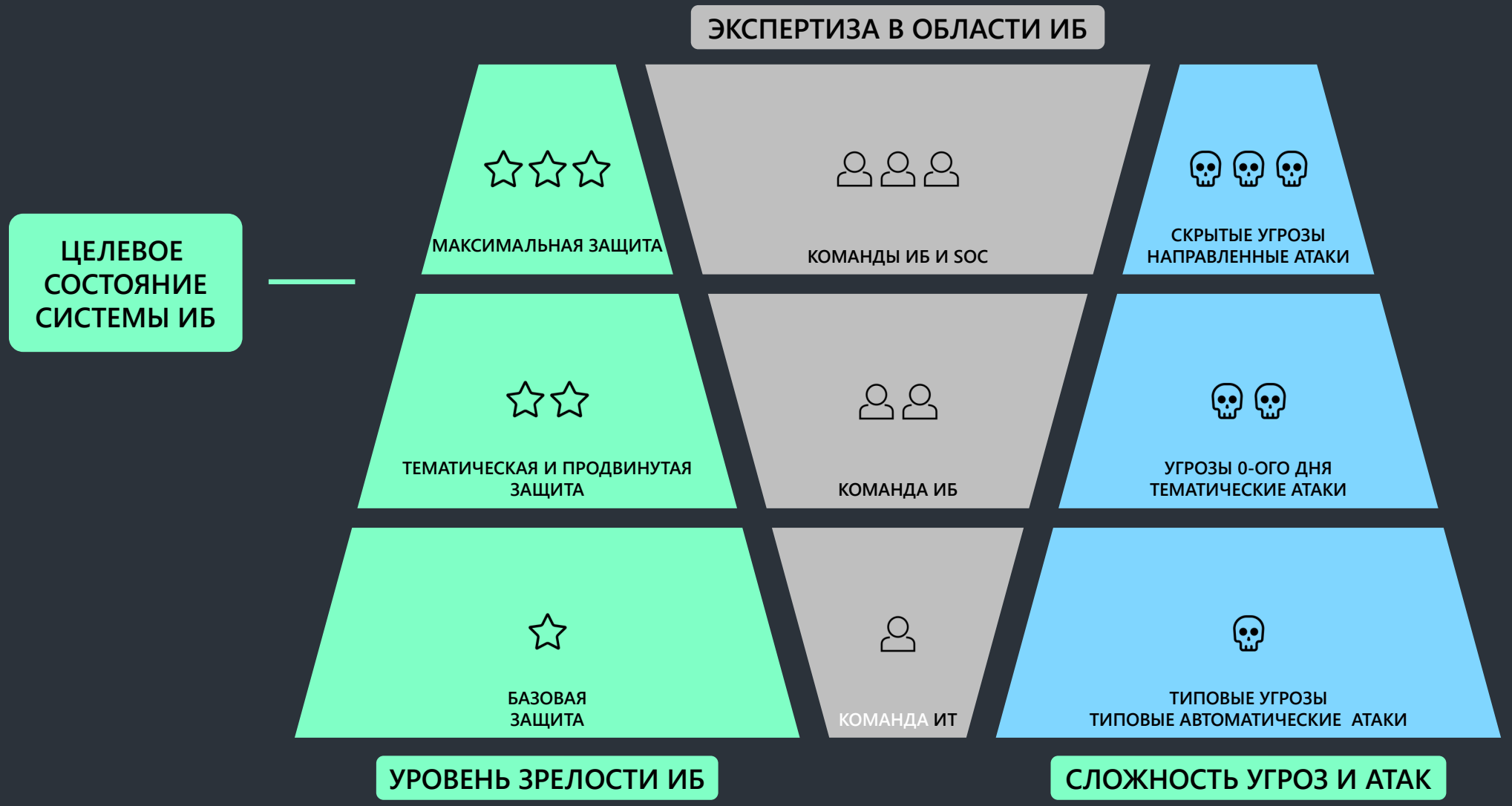
SOC FORUM 2023

Активная реакция на любое из этих событий

Например – изоляция устройства, блокировка учетной записи

НАМ НУЖНА ПОСТОЯННАЯ КОМАНДА ИБ

SOC FORUM 2023



ОБЩИЕ ВЫВОДЫ

SOC FORUM 2023

МЫ ТОЖЕ ПОПУЛЯРНЫ

Системные интеграторы, также как и любые другие подрядчики в цепочке поставок, стали целью для направленных атак

НАМ ПОВЕЗЛО

Стечение обстоятельств, наличие инструментов, людей и ресурсов позволили быстро реализовать сдерживание, расследование и устранение последствий инцидента

НАМ НУЖНО БОЛЬШЕ ИБ

«Стандартного» работа средств обеспечения ИБ недостаточно, для противодействия современным угрозам и атакам

СТАТИСТИКА НЕ РАБОТАЕТ

20 лет жизни без атак, не повод считать, что компания не будет атакована

SOC FORUM 2023

Platformix

+7 (495) 967-8050
info@platformix.ru

Москва
ул. Складочная д. 3, стр. 1