

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

КАК МЫ СТАЛИ ЖЕРТВОЙ
НАПРАВЛЕННОЙ АТАКИ

И ПОТЕРЯЛИ КОНТРОЛЬ
НАД ИНФРАСТРУКТУРОЙ

ЗА 97 МИНУТ

ГК «БАЗОВЫЕ РЕШЕНИЯ»

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

450+ человек

Центральный офис в Москве, филиалы, гибридный режим работы

Требования регуляторов

Полный комплекс работ по защите персональных данных

Platformix

Системный интегратор

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

СИЛА

Вендор

Производство корпоративного ИТ-оборудования, разработка ПО

Зрелая система ИБ

Защита от типовых и распространённых атак, усиленная безопасность ключевых систем

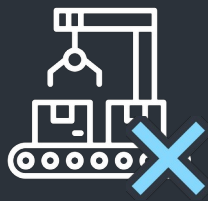
Процессы ИБ

Сертификация ISO 27001

Нас не будут целенаправленно атаковать



КИИ



Производство



Деньги



Данные



Государство



Защита



Осведомленность



Автономность



Бэкапы

Нам сложно причинить существенный ущерб

KILLCHAIN

ПРОНИКНОВЕНИЕ

ПРОДВИЖЕНИЕ

ЦЕЛЬ



РЕАГИРОВАНИЕ НА ИНЦИДЕНТ

SOC
FORUM
2023

ОБНАРУЖЕНИЕ

РЕАГИРОВАНИЕ

ПОСТ-АНАЛИЗ

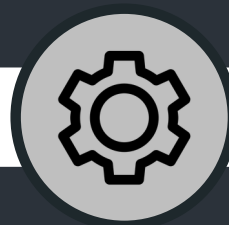
Обнаружение
Detection



Сдерживание
Containment



Устранение
последствий
Eradication
and Recovery



Подтверждение
Confirmation

Анализ
Analysis

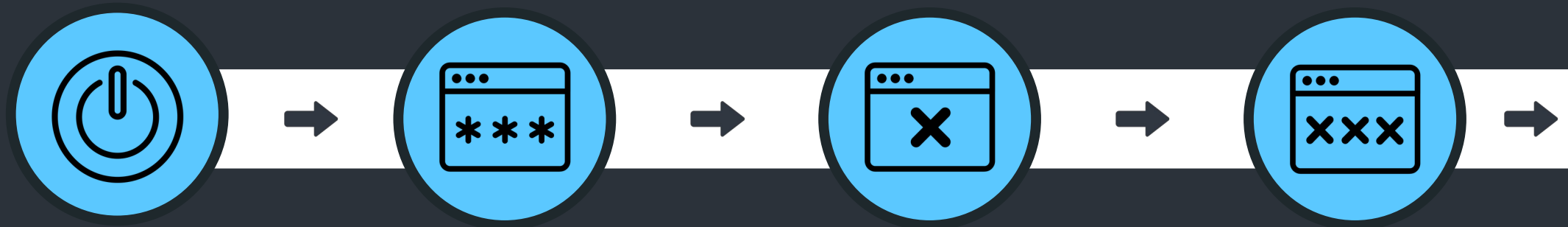
Расследование
причин
Investigation

Выводы
Lessons
Learned

ОБНАРУЖЕНИЕ И ПОДТВЕРЖДЕНИЕ



ОБНАРУЖЕНИЕ И ПОДТВЕРЖДЕНИЕ



Антивирус начал отключаться на серверах

Администратор пытается подключиться к серверу

Пароль администратора не подходит

Пароль другого администратора тоже не подходит

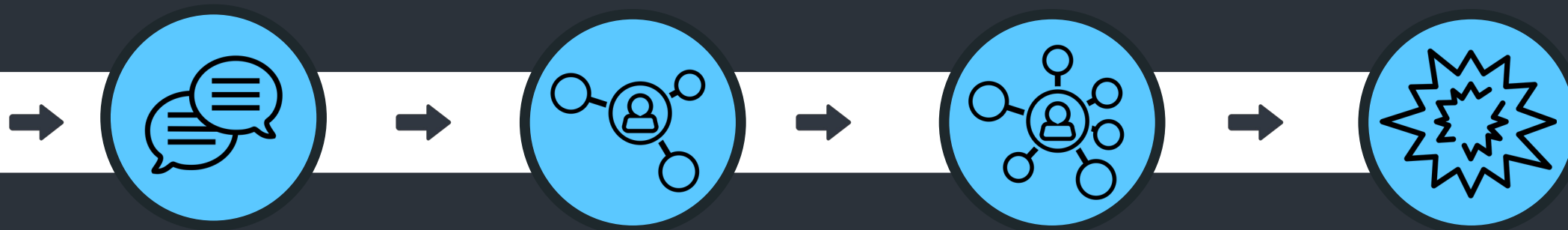


СУББОТА, НОЧЬ

ОБНАРУЖЕНИЕ И ПОДТВЕРЖДЕНИЕ



SOC
FORUM
2023



Обзвон
и уведомление
администраторов

Проверка
учетных записей
администраторов

Проверка
учетных записей
пользователей

ИНЦИДЕНТ!



СУББОТА, НОЧЬ

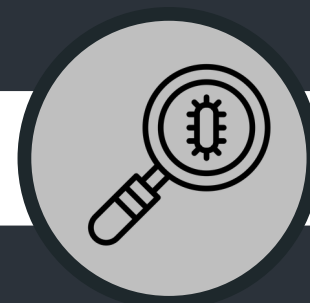
РЕАГИРОВАНИЕ СВОИМИ СИЛАМИ



СДЕРЖИВАНИЕ И АНАЛИЗ

★★★★★
SOC
FORUM
2023

ИТ



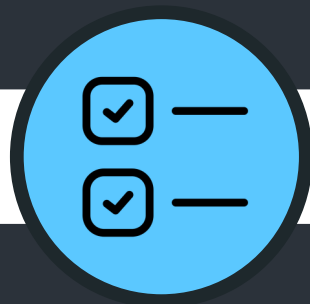
Сброс паролей
администраторов

Проверка состояния
резервных копий

Ограничение
удаленного доступа

Проверка устройств
администраторов

ИБ

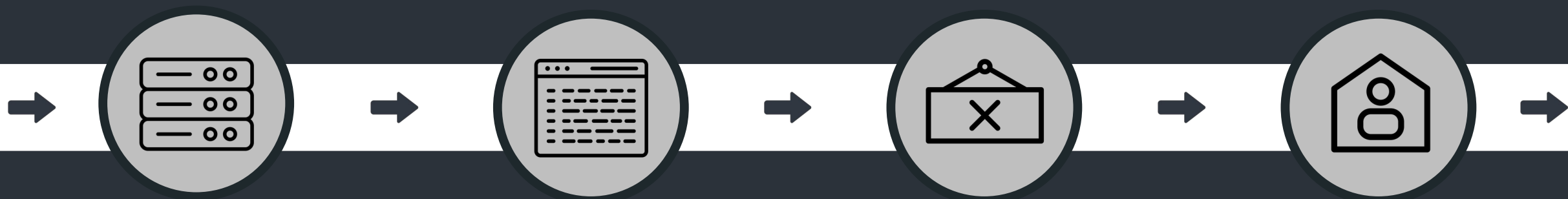


Определение
активов
для анализа

Первичный анализ
журналов
событий

Мониторинг
в реальном
времени

СДЕРЖИВАНИЕ И АНАЛИЗ



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

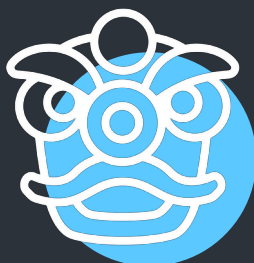
Анализ
взаимодействий
с сетью Интернет

ПРОМЕЖУТОЧНЫЕ РЕЗУЛЬТАТЫ

★★★★
SOC
FORUM
2023



Скомпрометированы
учетные записи
администраторов
и пользователей



Скомпрометированы
инфраструктурные
серверы компании,
включая сервер
антивирусной защиты



Обнаружен подозри-
тельный драйвер,
который применялся
ранее
при реализации
Ransomware-атак



5 администраторов и 2 пользователя



8 серверов и 7 станций



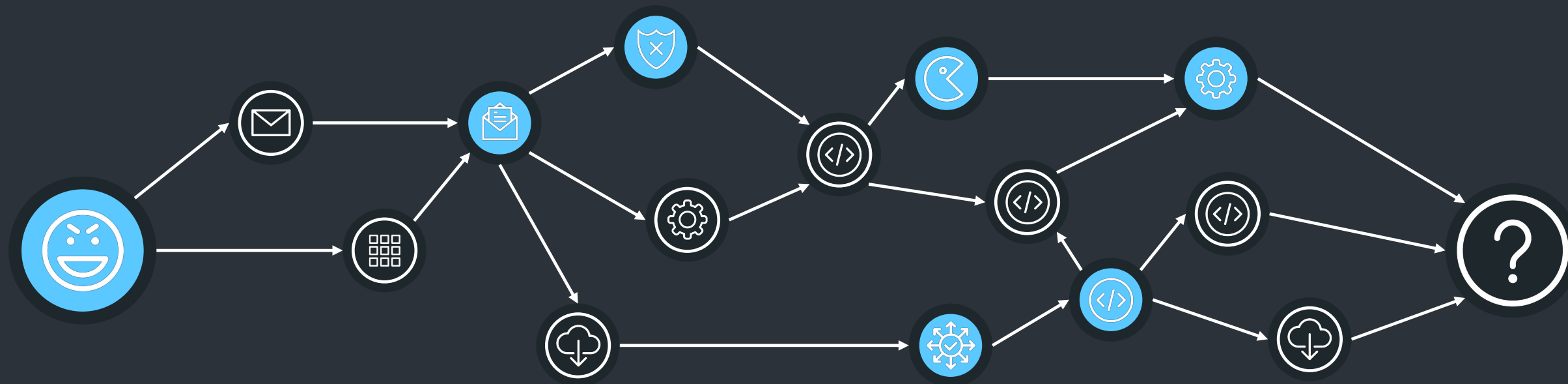
1 драйвер и 2 утилиты



1 подозрительный сайт

CUBA RANSOMWARE?

КИТАЙЦЫ?



ЧТО МЫ ЕЩЕ НЕ НАШЛИ?

ЗЛОУМЫШЛЕННИКИ ВСЕ ЕЩЕ ТУТ?

РЕАГИРОВАНИЕ ПОМОЩЬ СО СТОРОНЫ



СДЕРЖИВАНИЕ И АНАЛИЗ



SOC
FORUM
2023



СДЕРЖИВАНИЕ И АНАЛИЗ

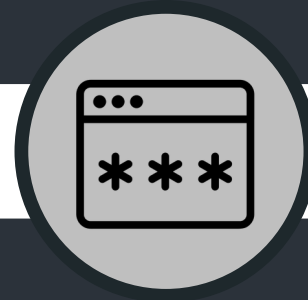
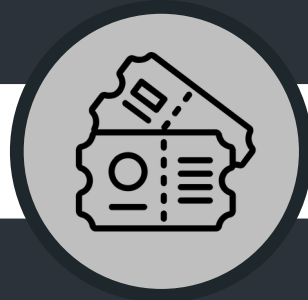
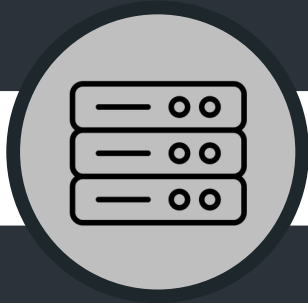


УСТРАНЕНИЕ ПОСЛЕДСТВИЙ



SOC
FORUM
2023

ИТ



Переустановка
скомпрометированных
активов

Перевыпуск
тикетов
Kerberos

Массовый
сброс паролей
учётных записей

Корректировка
политик безопасности
инфраструктуры



ОПЕРАТИВНЫЕ МЕРЫ ПО ИБ

Мониторинг
в реальном
времени

Повышение
осведомленности
пользователей

ОЦЕНКА УЩЕРБА

21

Сервер
и рабочая
станция

14

Учетных записей пользо-
вателей
и администраторов

-

Кража
или потеря
информации

-

Репутационный
ущерб

-

Финансовый
ущерб

ВРЕМЯ РАБОТНИКОВ

СТОИМОСТЬ ПРИВЛЕЧЕНИЯ СТОРОННИЕ ОРГАНИЗАЦИИ

РАССЛЕДОВАНИЕ

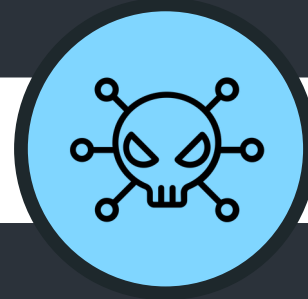




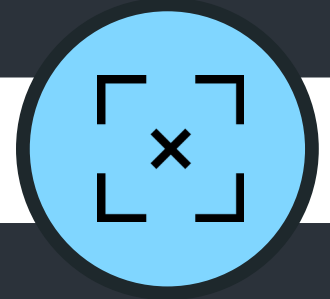
Получен доступ
к почте
сторонней
организации



Создана
инфраструктура
для реализации
атаки



Подобрано редкое
вредоносное
программное
обеспечение



Определены
жертвы среди ра-
ботников
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



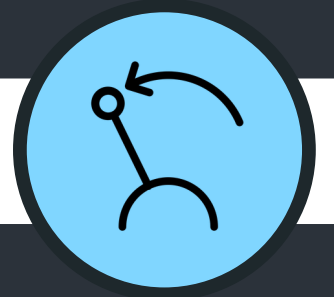
28 работников
получают
фишинговое
письмо



1 работник
открывает
вложенный
файл



На машине
работника
активируется
вредоносное ПО

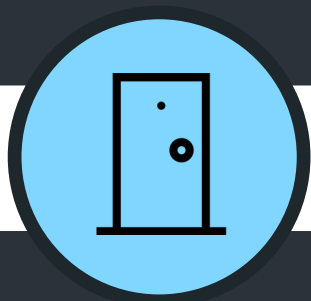


Вредоносное ПО
отключает
Symantec
и Defender

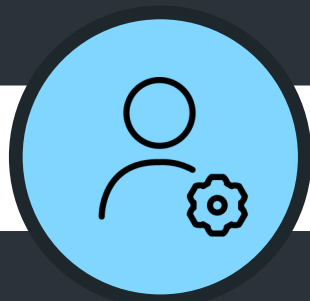
Вложенный файл содержал Trojan.MSOffice.SAgent

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

ЗАКРЕПЛЕНИЕ



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

Использование стандартных утилит для удаленного администрирования и доступа

Создание дополнительных точек закрепления по мере развития атаки

Разведка внутри локальной сети



Компрометация новых устройств



Компрометация новых учетных записей

События ИТ-мониторинга привлекли внимание административно

Администраторы быстро сориентировались в обстановке и отреагировали

ВЫВОДЫ

4549544087774966621777466610077343239251556974921076785048383198993995
87332616361660338962614103547183878947851189486371524883369381631607
0162187670854873506847065848932367178505995218634902334284
8675162143117211006104189692192986020010312367236296460828
109467396216397667955758273398422514894813686758395538602247
9300132027577559041790416046099960008143146533619911243338783
00689879685572760800242899342874153903820693981630235062776
61162366750473039703328722940643751725700746543109789064060211
6899503008172453568451051703905906142770071830898054142036546124981
78434643428447654191841846438606929752002870523808914481081493878306
10142738696235460855326303201202399738819381159114871838079164337711334
1122786939391989510541360853899533060078335544775354708232980766262745
157890078853136013526896716952517980635094049834959394559280180591217
913189708326092691723366602841459556179597644524530315508673597558817684
6096304428812359230152072217307225104967699462001196442243813211939800
336826825164257950902867626154764020964696479386247010376081385327807400
4889239033448271124040149847272238188331563878290307740028958681204592
2062511920709929593342315661272125249084868946281215568322409075628
594806520946837344313688836427565166379641939882927698829267666037605
453707724429833200703097524250499919774441190074457586188717718599044
094254655817933130716554080380854789835816406511488168192153770281914
60014452254418463361779882912088100708320908646902821056803007799783
66459537386816093269972397121528362769308638021244425154903137060
48735654785000966657024499134990453844053497461935106760049800435688060
4387015268440446307907628608111210314004498943630722774281684882212224024
557118111941356746170273618807013945323772001957686730923505858706757
121130951213312031198229373751838211569386086103028593873324825038447113
5278030603587065431845390946030027517712856409540847715409301661684282
084438361707793090186844673396676712212464488666869106381551703313
07636740759646397920814567217304728051095367052317464657771147020
01982610939907564989394763731278020440652241138368340524159505470623
0069260273538976088791126436671301715876493638173909103290373860665702
62107570793782247938072865849109202086180691680914454409265082819651
1457106552997409588082713580374944232032464622266273472990960685873575
00465678640056614785596324569293353433660879126381392068713516876
07018693054799433393774394067045006582460941700218637417480839436
46737827567556848381088673750095546462301014614912056260957784680
0733071108722108025731625289809948714698459384228875719725491227
009213278901437307243841847494876324561836508009064167572134072427
057185579990805094587569057117060370316678897687316805512096633458
07514489157936517054521144966453411643893217283930894551943174160
0396861527311856591125418746711460247411064609319643065050034413
05762117980777665204953462078872686606079695327345224565679799130
077368101830491299374023745158044158387580469111411786752046
0022810074612691324813027104091005584062889588943980390693020960

НАША СИСТЕМА ЗАЩИТЫ НУЖДАЕТСЯ В УСИЛЕНИИ



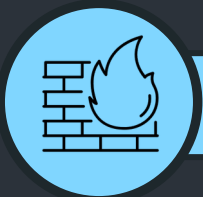
Email Gateway

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



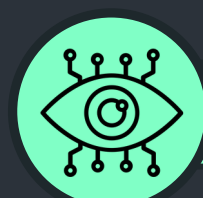
EDR

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



MFA

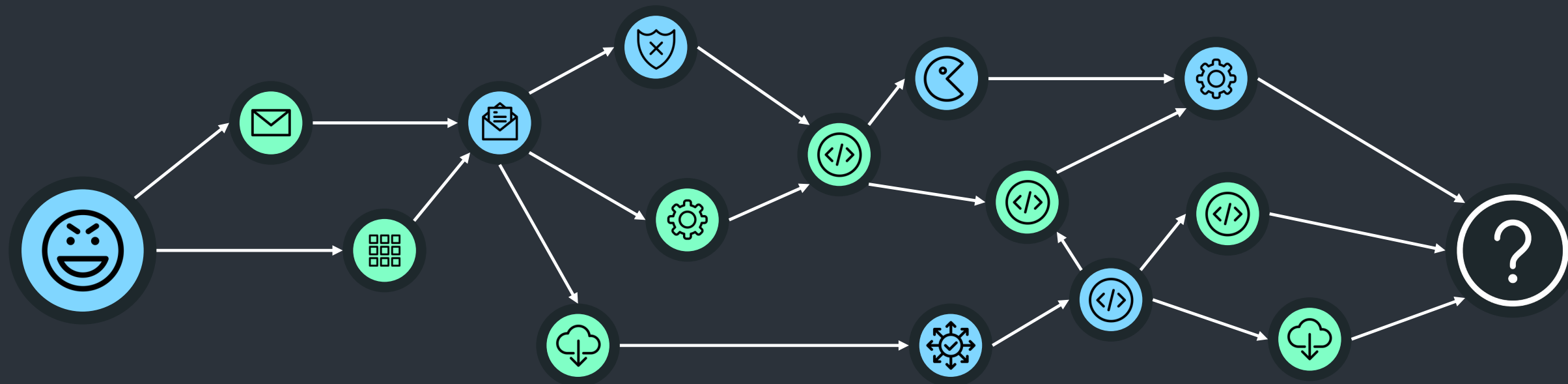
Многофакторная аутентификация для удаленного и административного доступа



SIEM

Мониторинг и выявление инцидентов информационной безопасности

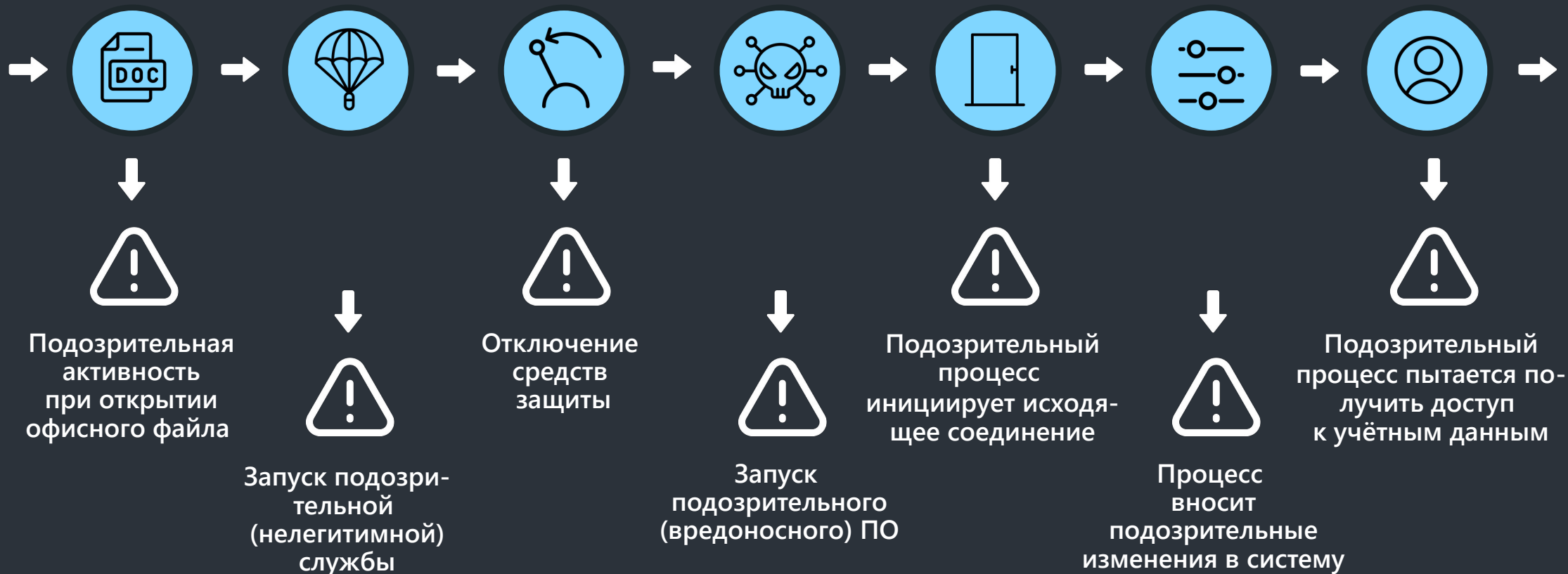




Анализ трафика, файлов и событий

Слепых зон не остается

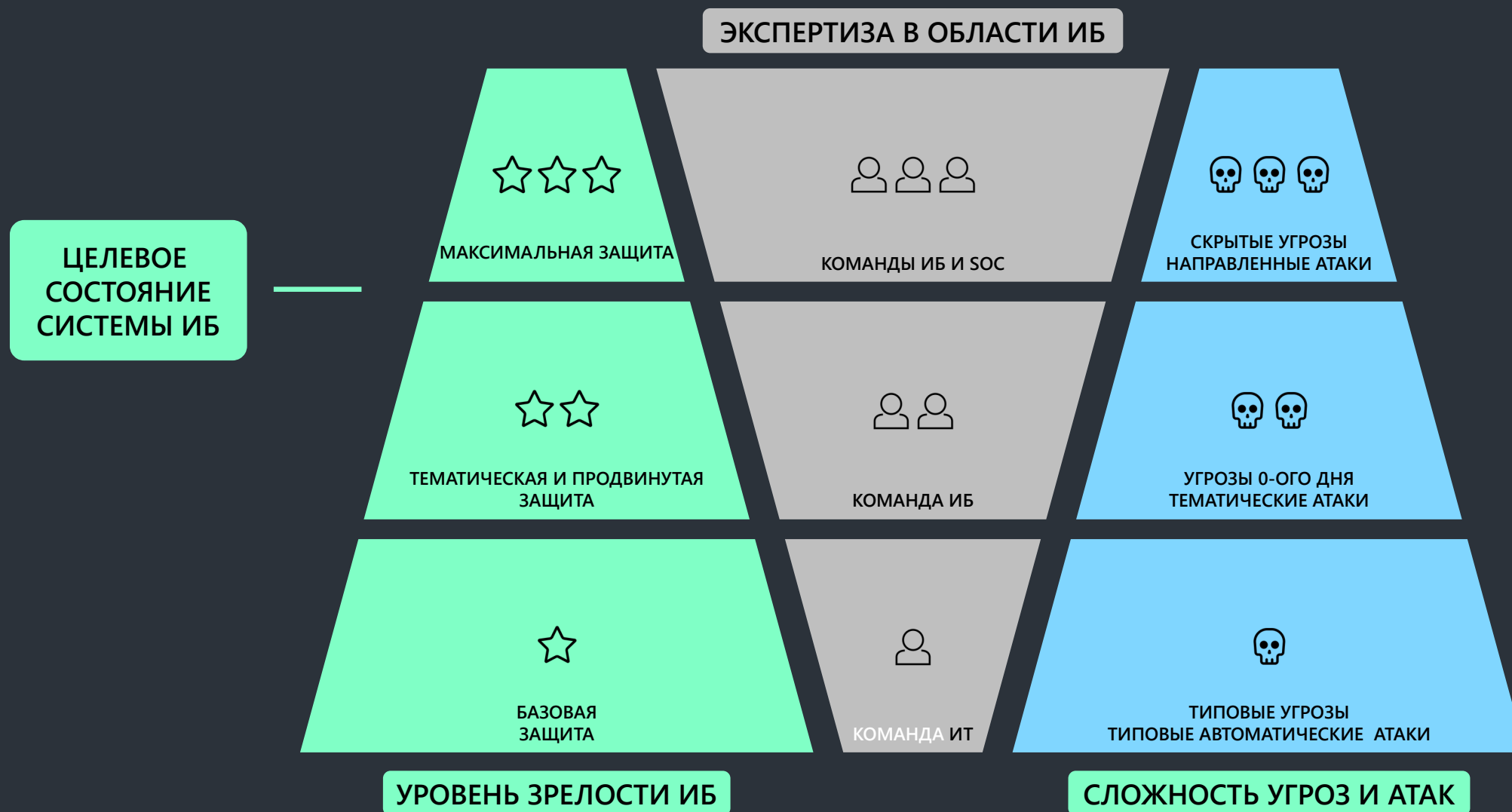
РЕАГИРОВАНИЕ НА ИНЦИДЕНТЫ



Активная реакция на любое из этих событий

Например – изоляция устройства, блокировка учетной записи

НАМ НУЖНА ПОСТОЯННАЯ КОМАНДА ИБ



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