

ИСТОРИЯ ОДНОЙ НОЧИ В SOC

ИЛИ МОЙ ПЕРВЫЙ TRUE POSITIVE



МИЛЬКО ДМИТРИЙ

Ведущий инженер-аналитик в коммерческом SOC

Расследование инцидентов, фильтрация и автоматизация
рутинных задач через IRP, SOAR, SIEM

Преподаватель-исследователь в МИФИ/Скиллфэктори

Автор курса по информационно-аналитическим системам
защиты информации

dmitry.s.milko@gmail.com

@mityanya135



ЧТО ВЫ УЗНАЕТЕ

Как проходит обычная смена инженера SOC на линии

Как мне впервые удалось самому обнаружить True Positive сработку

Как устроен наш SOC и как попасть к нам на работу

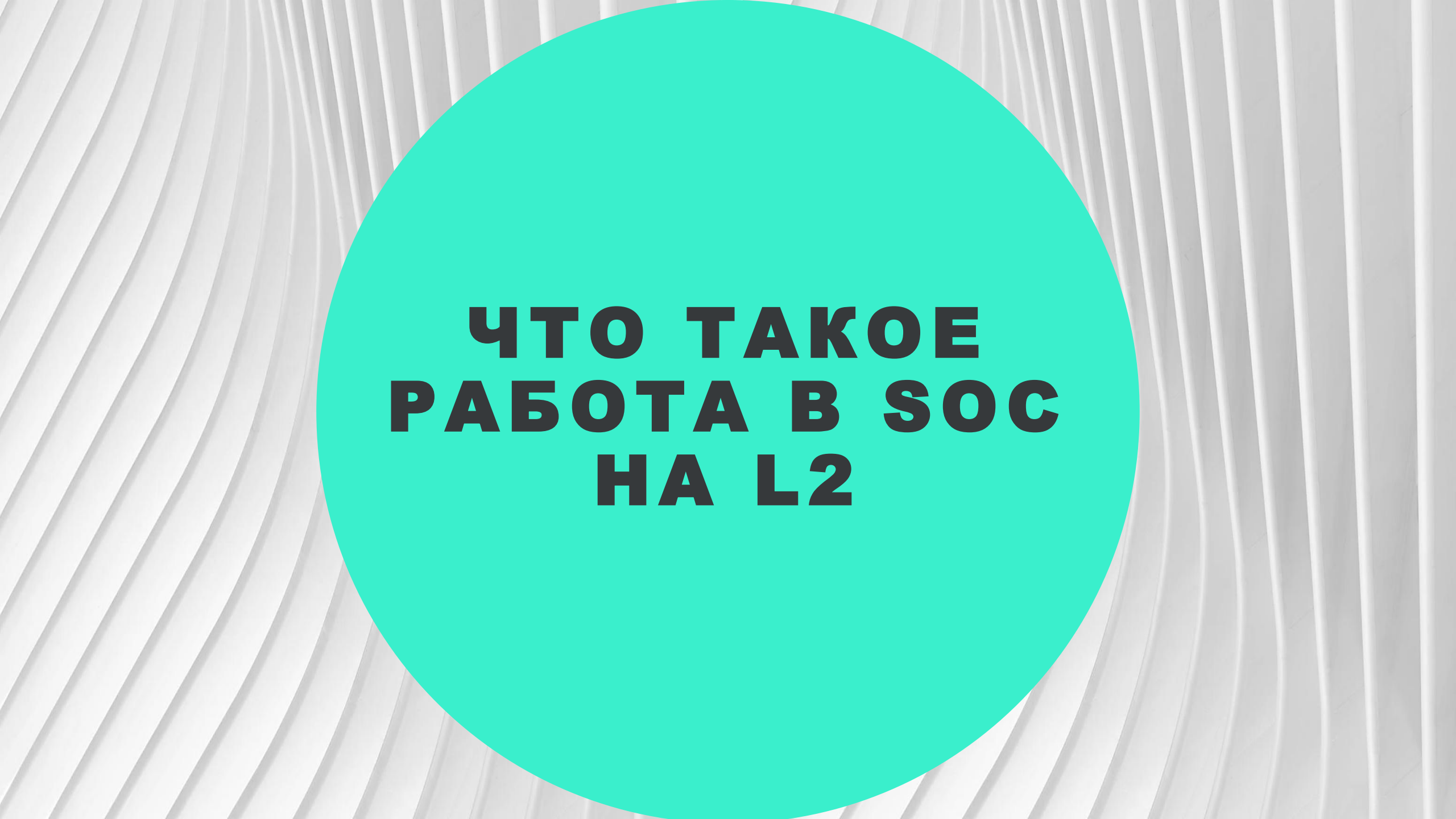


НЕМНОГО СТАТИСТИКИ

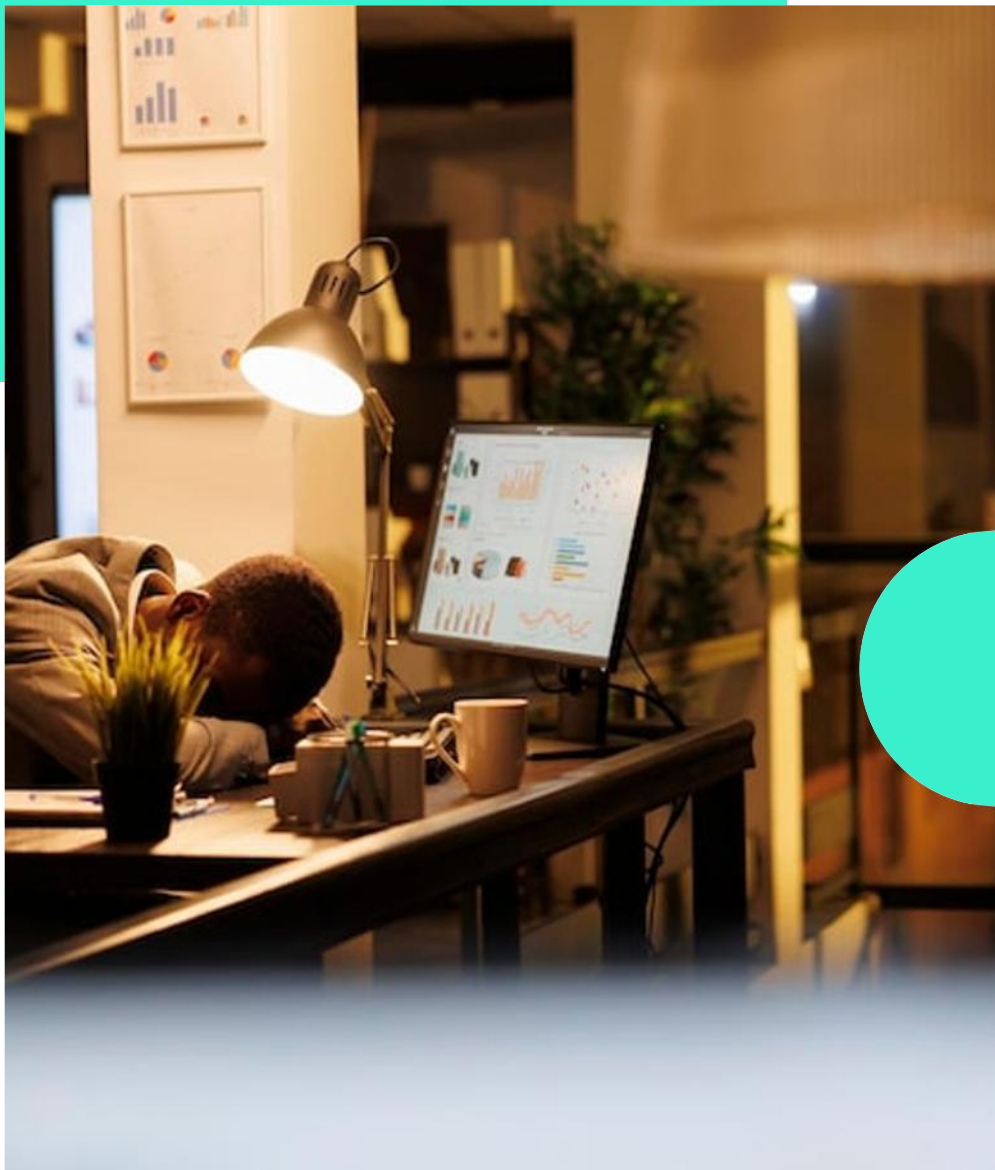
Каждые 39 секунд в мире происходит кибератака

Ежедневно жертвами хакеров становятся более 200 организаций

Примерные оценки 2025 года, источник - <https://www.demandsage.com/cybersecurity-statistics/>



ЧТО ТАКОЕ РАБОТА В SOC НА L2

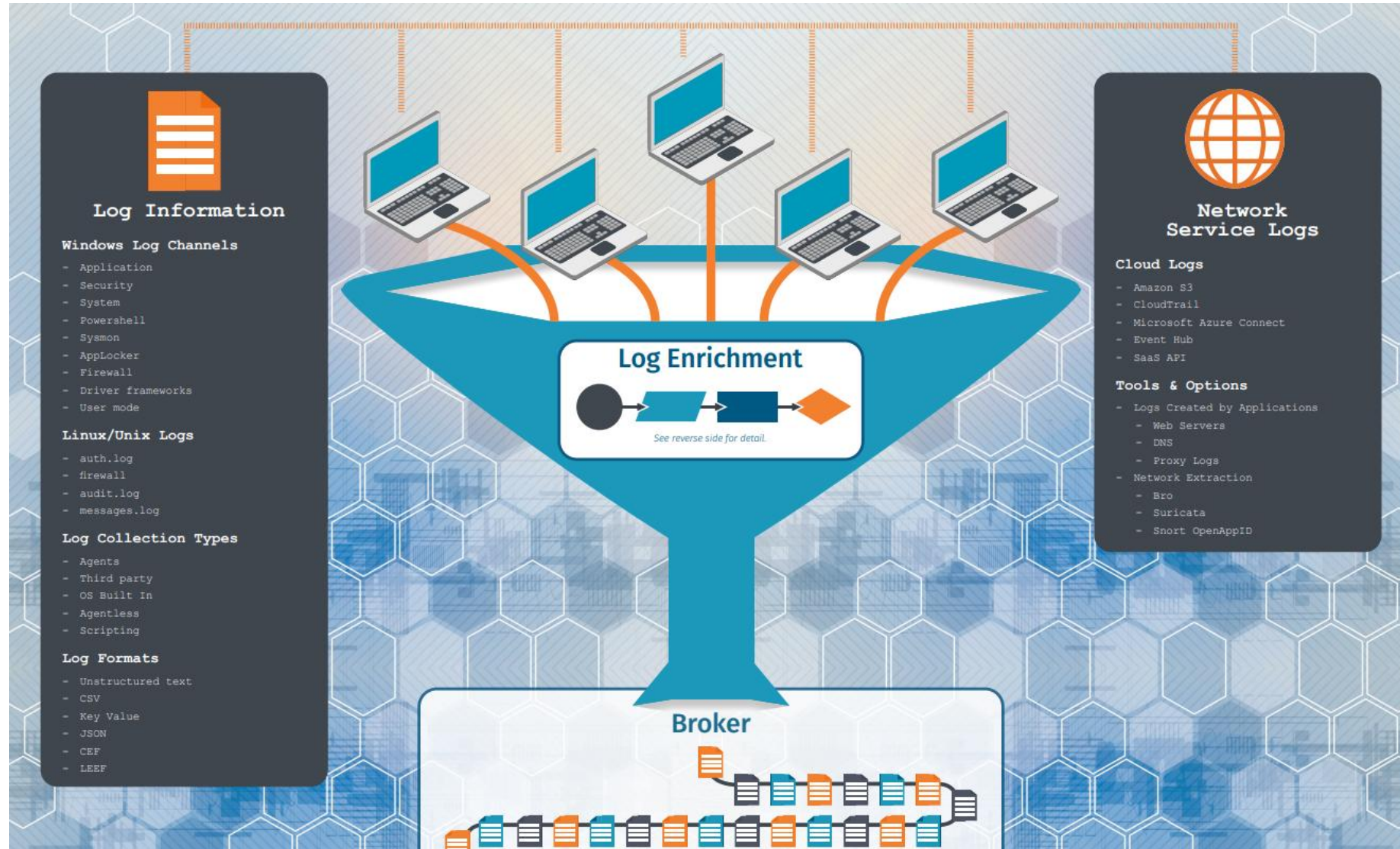


ОБЫЧНАЯ СИТУАЦИЯ

Начало смены инженера с 06:00 ИРК
(01:00 МСК)

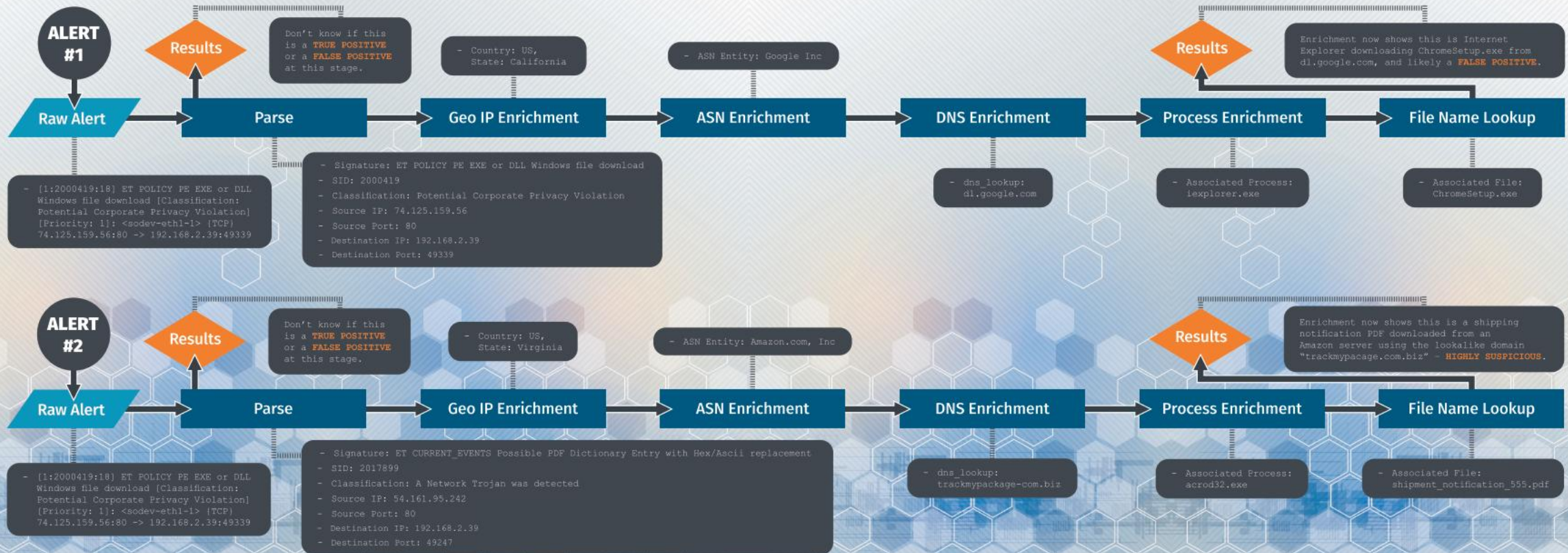
Проснулся, включил ноутбук, ввел
пароли для SIEM и IRP

SECURITY INFORMATION AND EVENT MANAGEMENT - SIEM



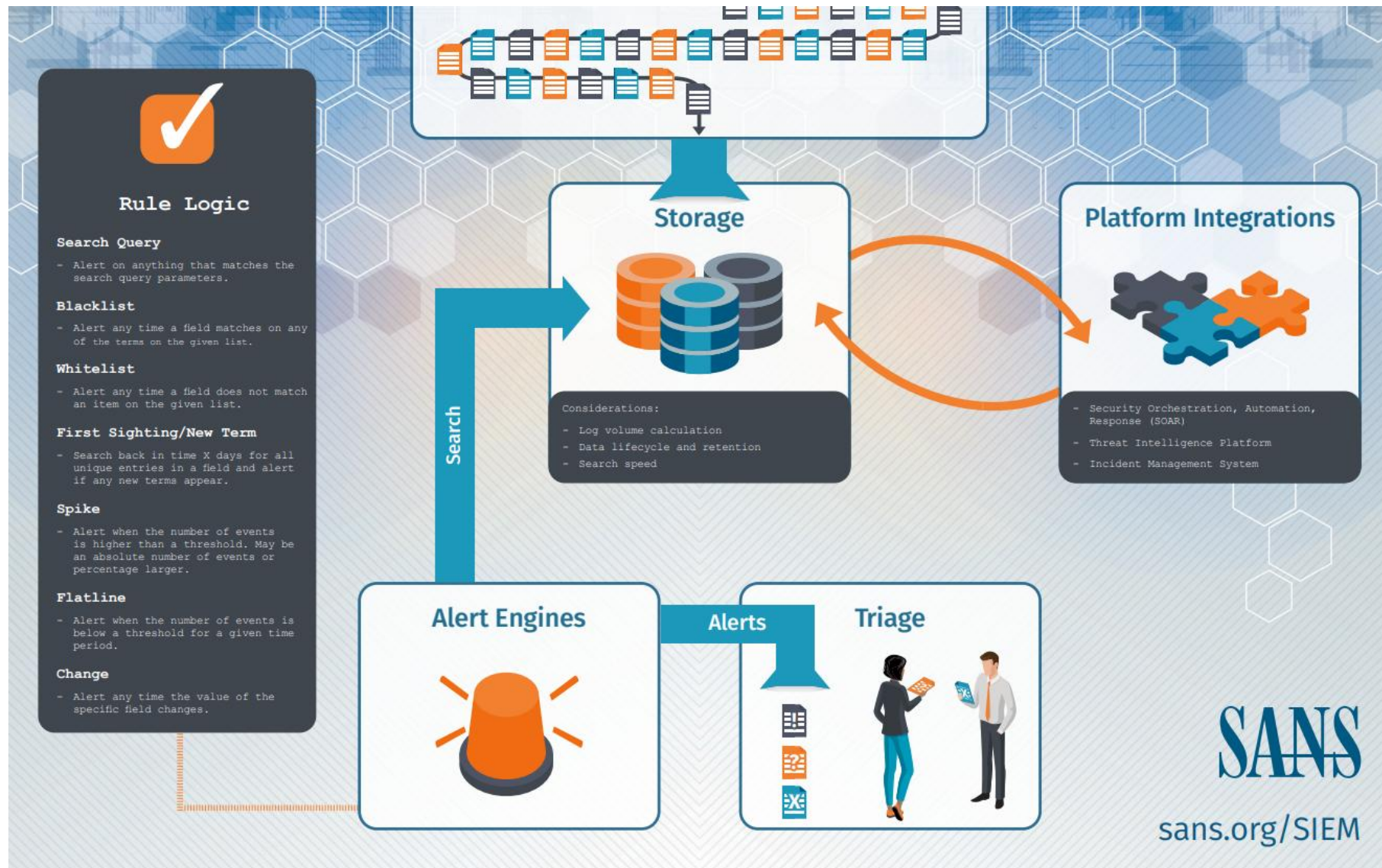
SECURITY INFORMATION AND EVENT MANAGEMENT - SIEM

Log Enrichment



«Собери все события, чтобы определить инцидент»

SECURITY INFORMATION AND EVENT MANAGEMENT - SIEM



INC-1
Разведка

Статус

Опасность ■ Средняя
Статус ● Новый
Ответственный
Автор SIEM
Источник инцидента Ручной ввод
Обнаружен 05 августа, 17:28
Создан 10 сентября, 12:11
Последнее изменение **Изменено: задача**
10 сентября, 14:23

Параметры

Категория Атака
Тип Сканирование сети
Влияние Потенциальное воздействие на не критически важный актив
Список сканируемых портов 22, 135
Методы сканирования TCP-запросы
Расположение

Задачи События Активы и сети Атакующие активы Комментарии

Время	Событие	
05 августа 15:30	Обнаружена попытка просканировать 22 порт на 100 узлах с узла 192.168.1.35	
05 августа 15:30	Обнаружена попытка просканировать 135 порт на 100 узлах с узла 192.168.1.35	
05 августа 15:30	Обнаружена попытка просканировать 22 порт на 108 узлах с узла 192.168.1.35	
05 августа 15:30	Обнаружена попытка просканировать 135 порт на 108 узлах с узла 192.168.1.35	

Открыть страницу События

pt

MaxPatrol 10

Активы

События

Инциденты

Стандарты

Сбор данных

Система

События

за последние 7 дней

Все события

Группы

Все события

Непривязанные

По всем активам

192.168.1.0/24

All

Unix

Windows

Desktop

Servers

192.168.3.0/24

All

Unix

Windows

Фильтры

Все события

Стандартные фильтры

Методы сбора данных

Оконечные узлы

Все события

Файловые операции

Сетевая активность

Процессы

Работа с реестром

Сессии пользовате...

Журналы событий

Аутентификация, а...

СУБД

Создать инцидент

Связать с инцидентом

Экспорт

Показать на топологии

Фильтр: Все события

time, event_src.host, text

time (свежее сверху)

Выполнить

time	event_src.host	text
02.12.2024 14:37:31	UGOS	Соединение по протоколу tcp с узла 185.7.214.20:55063 на узел 93.158.193.76:24418 запре
02.12.2024 14:37:30	UGOS	Соединение по протоколу tcp с узла 51.75.210.207:59140 на узел 93.158.193.76:30341 запре
02.12.2024 14:37:25	UGOS	Соединение по протоколу udp с узла 192.168.1.10:53 на узел 192.168.1.1:2377 запрещено пр
02.12.2024 14:37:25	UGOS	Соединение по протоколу tcp с узла 194.180.49.141:47493 на узел 93.158.193.76:7720 запре
02.12.2024 14:37:25	UGOS	Соединение по протоколу tcp с узла 154.213.184.18:49266 на узел 93.158.193.76:8080 запре
02.12.2024 14:37:23	UGOS	Соединение по протоколу udp с узла 172.30.250.2:61732 на узел 64.233.161.95:443 разреше
02.12.2024 14:37:23	UGOS	Создана udp-трансляция с узла 172.30.250.2:61732 на узел 93.158.193.76:61732 на узле utm
02.12.2024 14:37:18	UGOS	Соединение по протоколу udp с узла 192.168.2.69:49235 на узел 255.255.255.255:1947 запр
02.12.2024 14:37:15	UGOS	Соединение по протоколу tcp с узла 193.163.125.198:37098 на узел 93.158.193.76:9608 запр
02.12.2024 14:37:14	UGOS	Запрос пользователя к ресурсу 213.180.204.232:443 разрешен узлом utmcore@fthecaersnth
02.12.2024 14:37:14	UGOS	Соединение по протоколу tcp с узла 192.168.1.10:64473 на узел 213.180.204.232:443 разре
02.12.2024 14:37:14	UGOS	Создана tcp-трансляция с узла 192.168.1.10:64473 на узел 93.158.193.76:64473 на узле utm
02.12.2024 14:37:14	UGOS	Соединение по протоколу tcp с узла 192.168.1.10:64471 на узел 77.88.8.8:53 разрешено пра
02.12.2024 14:37:14	UGOS	Создана tcp-трансляция с узла 192.168.1.10:64471 на узел 93.158.193.76:64471 на узле utm
02.12.2024 14:37:14	UGOS	Соединение по протоколу tcp с узла 192.168.1.10:64472 на узел 77.88.8.8:53 разрешено пра
02.12.2024 14:37:14	UGOS	Создана tcp-трансляция с узла 192.168.1.10:64472 на узел 93.158.193.76:64472 на узле utm

Всего 730 892 события, выбрано 1

02.12.2024 14:37:31

Соединение по протоколу tcp с узла 185.7.214.20:55063 на узел 93.158.193.76:24418 запрещено правилом "Default Block Input"

Субъект

Default Block Input

subject rule

Действие

deny

Статус

success

Отправитель

185.7.214.20 0

Получатель

93.158.193.76 0

Источник

entensys usergate_utm

Категория

Connection / Network Interaction Management / Control

Адресаты

Отправитель

src.host 185.7.214.20

src.ip 185.7.214.20

src.port 55063

src.geo.country RU

Получатель

dst.host 93.158.193.76

dst.ip 93.158.193.76

dst.port 24418

dst.geo.country RU

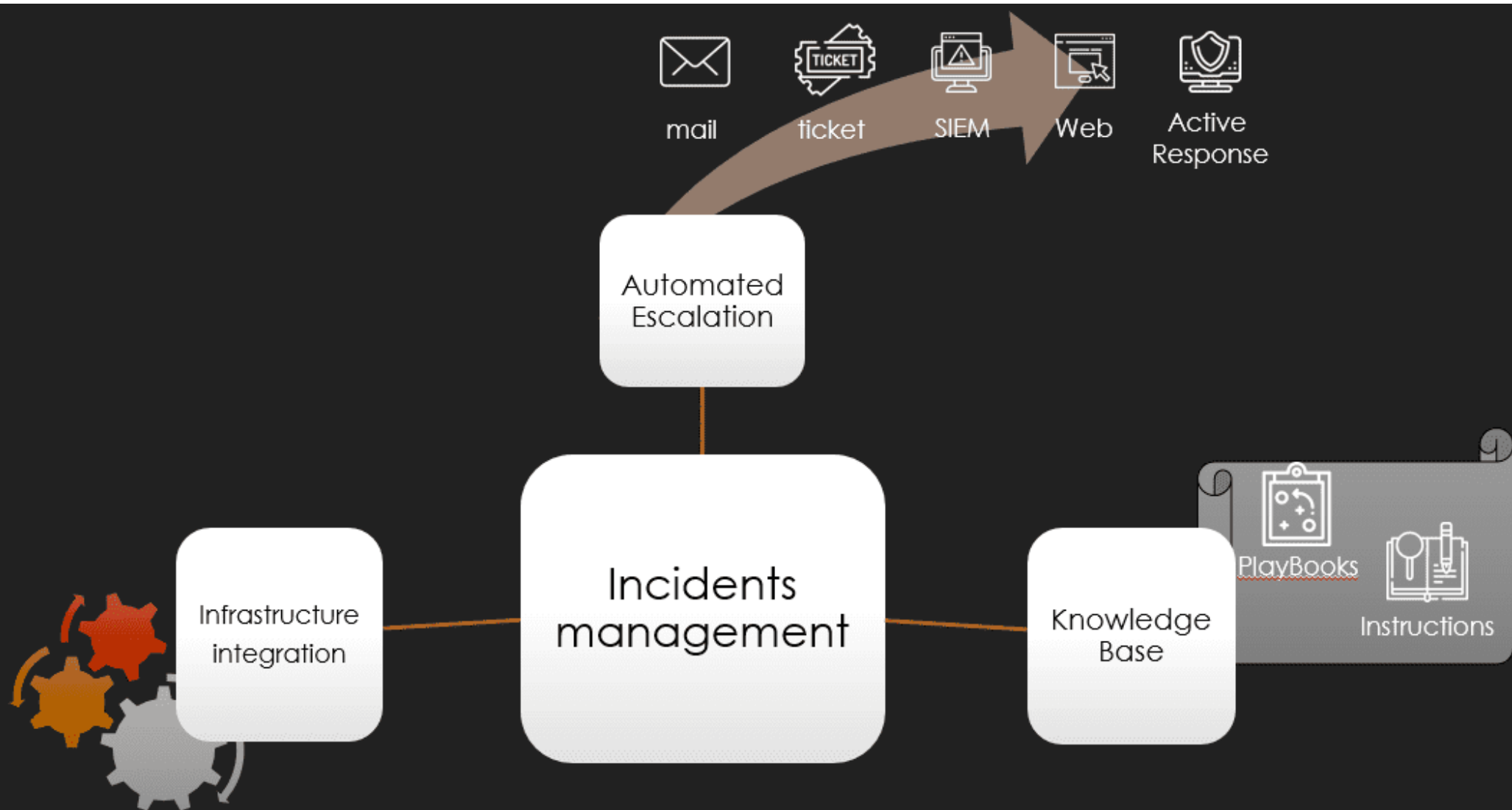
Роли во взаимодействии

Субъект

subject rule

INCIDENT RESPONSE PLATFORM - IRP

<https://www.anti-malware.ru/practice/solutions/free-IRP-on-your-own>



INCIDENT RESPONSE PLATFORM - IRP

<https://www.anti-malware.ru/practice/solutions/free-IRP-on-your-own>

На основе алерта
из SIEM
создается
инцидент,
который далее
сопровождается
уже внутри IRP



INCIDENT RESPONSE PLATFORM - IRP

<https://www.anti-malware.ru/practice/solutions/free-IRP-on-your-own>

Инженер работает
с интерфейсом IRP
на уровне
инцидентов (Case)
и задач (Task)

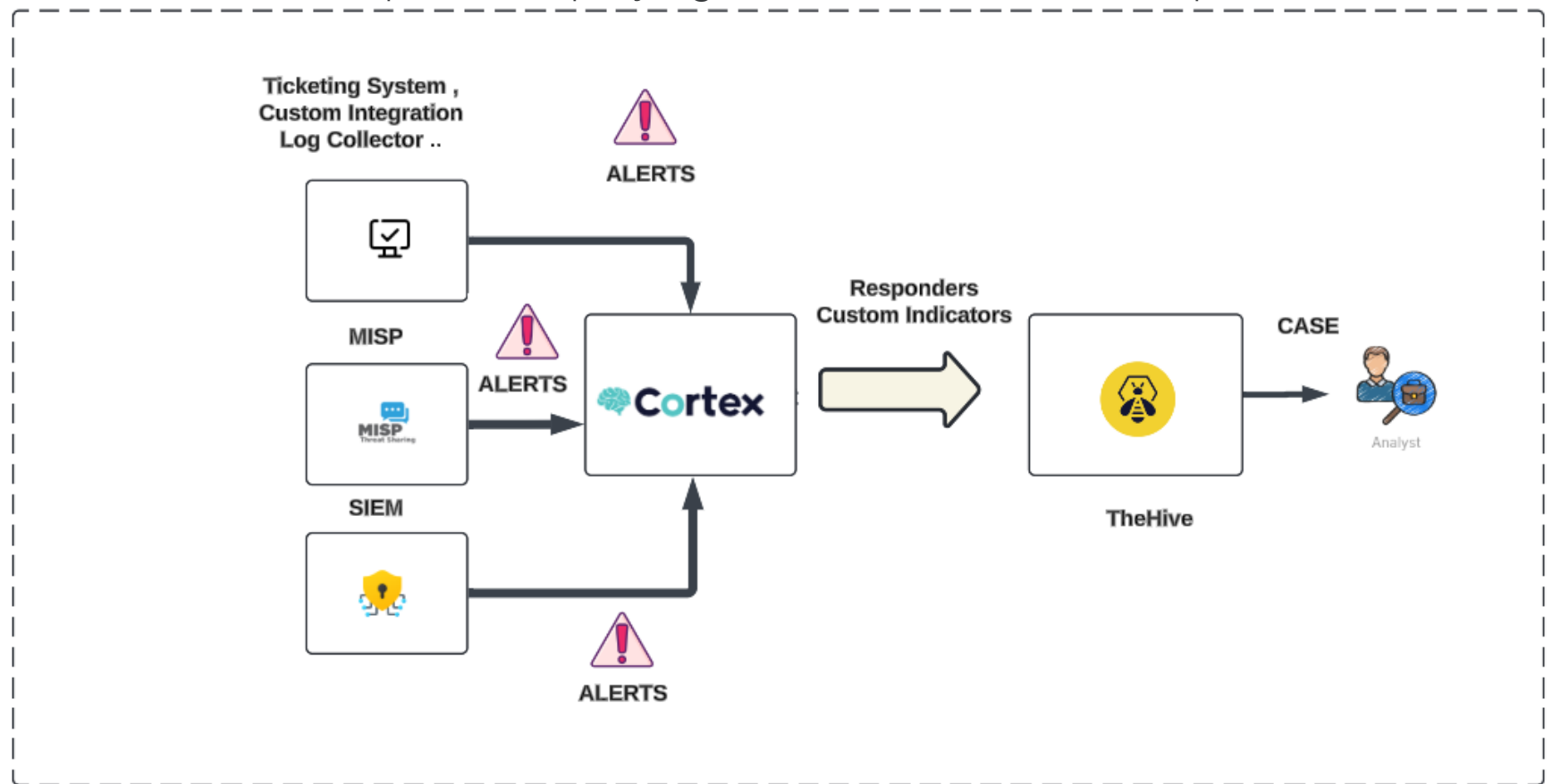
Details Tasks 5 Observables 5					
+ Add Task		Show Groups		Filter	
Group	Task	Date	Assignee	Actions	
▼ ▶ group1	[Обнаружение] 1. Анализ. Проверка состоятельности. Наполнение карточки инцидента Started 7 minutes ago	Mon, Oct 29th, 2018 10:42 +03:00	Иван Важенин	🔒 Close	⚙️
▼ ▶ group1	[Обнаружение] 2. Запрос информации об узле и пользователе Started 6 minutes ago	Mon, Oct 29th, 2018 10:42 +03:00	Иван Важенин	🔒 Close	⚙️
▲ ▶ group2	[Реагирование] 3. Провести анализ полученного образца ВПО. Разработать меры по ликвидации ВПО Started 6 minutes ago	Mon, Oct 29th, 2018 10:42 +03:00	Антон Калинин	🔒 Close	⚙️
1. Провести анализ полученного образца ВПО, запустив все анализаторы. Выполнить поиск информации в базе знаний. - Информации о ВПО в базе знаний нет - наполнить базу знаний информацией о типе выявленного ВПО и индикаторах компрометации, связанных с ВПО. Разработать меры по ликвидации ВПО - Информация о ВПО в базе знаний есть - дополнить листы обнаружения и блокировки средств мониторинга обнаруженными индикаторами компрометации, провести исторический анализ с обывтий и поиск дополнительных скомпрометированных узлов. 2. Взять задачу №4. Направить собранную информацию и мероприятия по ликвидации ВПО					
▼ group2	[Реагирование] 4. Направить собранную информацию и мероприятия по ликвидации ВПО.		Антон Калинин	▶ Start	⚙️
▼ group1	[Предупреждение] 5. Заполнение результатов реагирования на инцидент ИБ		Иван Важенин	▶ Start	⚙️

INCIDENT RESPONSE PLATFORM - IRP

<https://tamirsuliman.medium.com/streamlining-cyber-incident-response-deploying-thehive-with-docker-simplified-35f545e4c082>

IRP также решает задачи L1:

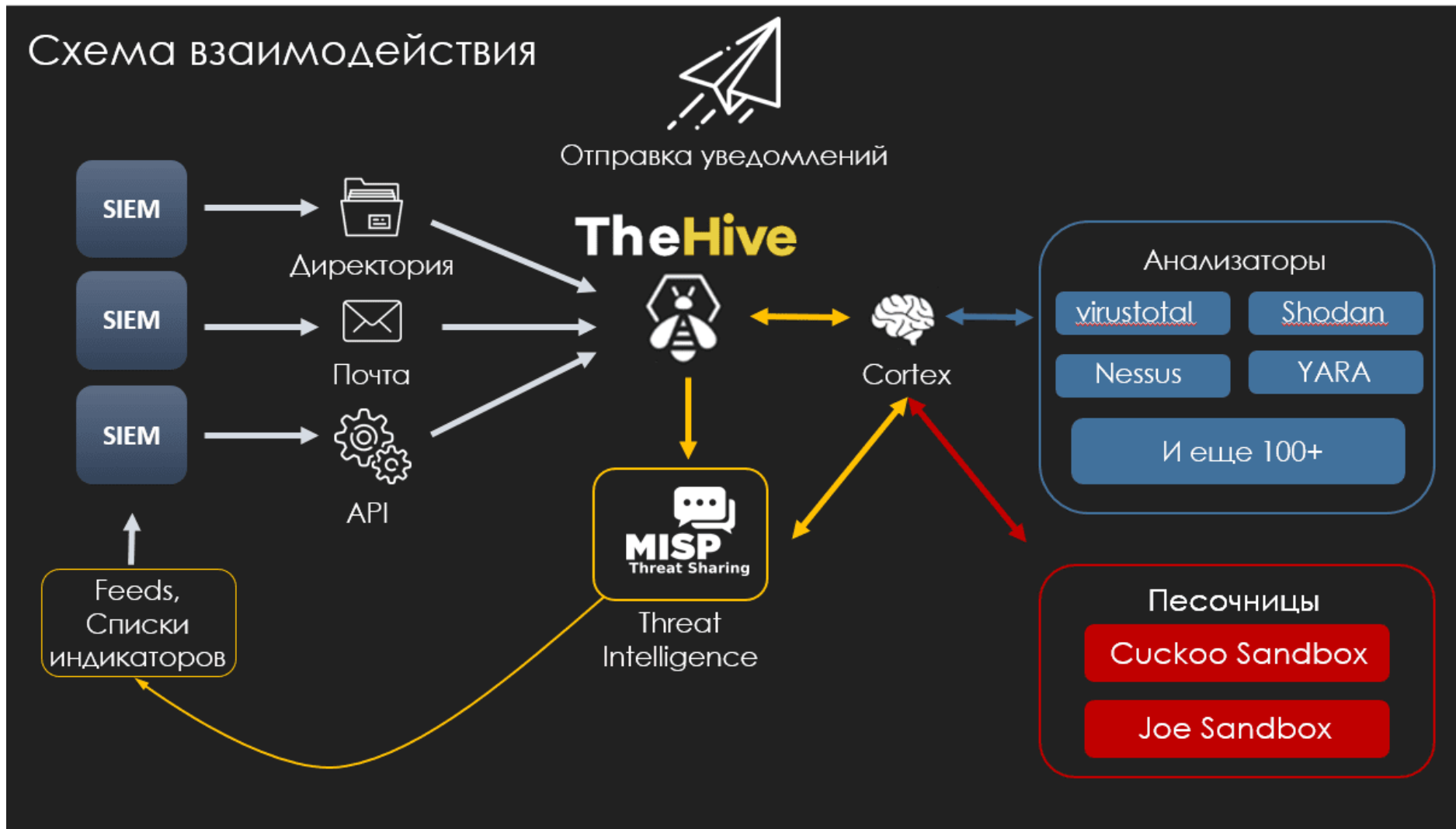
- находит аналогичные инциденты по кастомным IoC (по имени узла, IP-адресу, учетной записи)



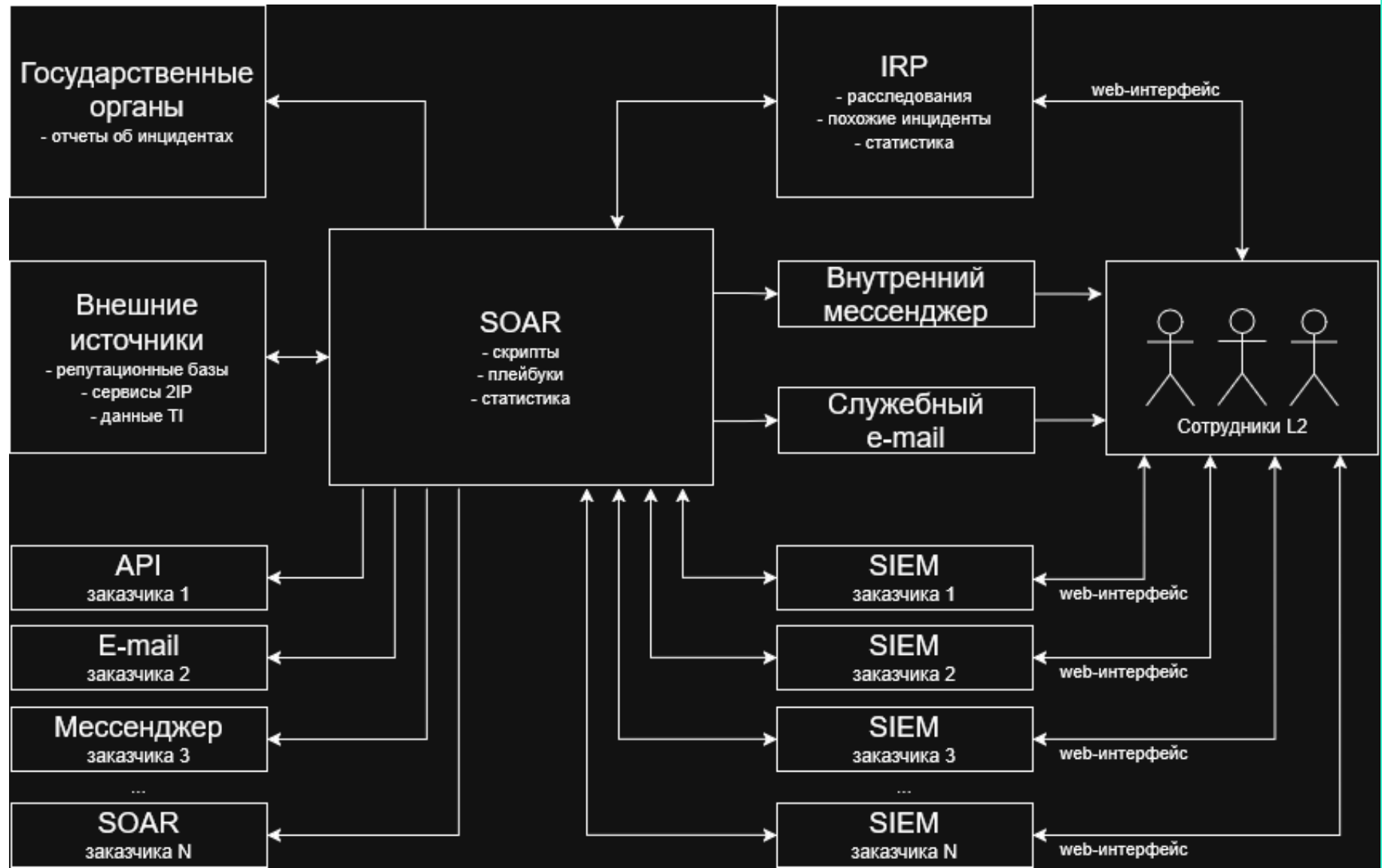
INCIDENT RESPONSE PLATFORM - IRP

<https://www.anti-malware.ru/practice/solutions/free-IRP-on-your-own>

Пример интеграции IRP-системы The Hive



SECURITY ORCHESTRATION, AUTOMATION AND RESPONSE - SOAR



SECURITY ORCHESTRATION, AUTOMATION AND RESPONSE - SOAR

SOAR решает задачи L1:

– собирает базовую
информацию о входах на
сетевом узле и показывает
её в IRP

logged_users	active_user
21.12.2025 17:37:29 UTC: nt authority\system (logon type: 5 - Service); 21.12.2025 17:37:46 UTC: nt authority\system (logon type: 3 - Network) from 127.0.0.1 (None); 21.12.2025 17:37:29 UTC: nt service\ksnproxy (logon type: 5 - Service); 21.12.2025 17:37:40 UTC: [REDACTED] (logon type: 11 - CachedInteractive); 21.12.2025 17:37:34 UTC: font driver host\umfd-1 (logon type: 2 - Interactive); 21.12.2025 17:37:34 UTC: window manager\dwm-1 (logon type: 2 - Interactive); 21.12.2025 17:37:34 UTC: nt authority\system (logon type: 0 - Unknown logon type); 21.12.2025 17:37:34 UTC: nt authority\local service (logon type: 5 - Service); 21.12.2025 17:37:34 UTC: font driver host\umfd-0 (logon type: 2 - Interactive); 21.12.2025 17:37:34 UTC: nt authority\network service (logon type: 5 - Service)	[REDACTED] (logon_type: 11)

SECURITY ORCHESTRATION, AUTOMATION AND RESPONSE - SOAR

SOAR решает задачи L1:
- показывает данные об учетной записи из контроллера домена

ФИО пользователя	[REDACTED]	Группы пользователя	CN=[REDACTED],OU=[REDACTED],OU=[REDACTED] CN=[REDACTED] [REDACTED],OU=[REDACTED] [REDACTED],DC=[REDACTED],DC=ru	User Password Change	11/30/25 07:40
User Lastlogon	12/01/25 16:57	Отдел пользователя	[REDACTED]	Организация пользователя	[REDACTED] [REDACTED]
Должность пользователя	[REDACTED]	Описание целевого хоста	CN=[REDACTED] [REDACTED],OU=[REDACTED] [REDACTED],OU=[REDACTED] [REDACTED],DC=[REDACTED],DC=ru	Описание хоста инициатора	CN=WS-[REDACTED] [REDACTED],OU=[REDACTED],DC=[REDACTED]
УЗ хоста инициатора	ws-[REDACTED]	logged_users	04.12.2025 19:27:04 UTC: [REDACTED] \ws-[REDACTED] (logon type: 3 - Network) from 10.10.[REDACTED] (None);		

SECURITY ORCHESTRATION, AUTOMATION AND RESPONSE - SOAR

SOAR решает задачи L1:

- показывает данные об узле и его адресе из контроллера домена

Source FQDN	srv_ad	Логин пользователя	ivanov_ii	Домен пользователя	roga-i-kopyta.ru
Source IP	10.10.168.2	Destination FQDN	ws-12345.roga-i-kopyta.ru	Destination IP	10.10.168.99
MP SIEM event Id's	["8293f792-eeba-11f0-8748-005056bb46ca", "c8904340-eeba-11f0-9539-bf5056a6efcb"]	mpslem_corule	Bruteforce_password_spraying_internal	Ключевые поля инцидента	srv_ad 10.10.168.2 10.10.168.99
Значимые поля	Not Specified	Время создания алерта в SIEM	1768103847	scopelid	16521981-61asf-6546519801000041
ФИО пользователя	Иванов Иван Иванович	Группы пользователя	CN=Бухгалтерия, OU=Дирекция, DC=main_dc, DC=roga-i-kopyta CN=Пользователи удаленного рабочего стола	User Password Change	01/05/26 09:04
User Lastlogon	01/09/26 18:09	Отдел пользователя	Бухгалтерия основного подразделения	Организация пользователя	ООО "Рога и копыта"
Должность пользователя	Главный бухгалтер	Описание целевого хоста	CN=SRV_AD,OU=Domain Controllers,DC=main_dc,DC=roga-i-kopyta		

SECURITY ORCHESTRATION, AUTOMATION AND RESPONSE - SOAR

SOAR решает задачи L1:
- показывает данные об IP-адресах и доменах из репутационных баз

Reputation	213.209. [REDACTED] : -2 (VirusTotal IP)	Total Analysis Stats	213.209. [REDACTED] : malicious - 5, suspicious - 3, undetected - 31, harmless - 56, timeout - 0 (VirusTotal IP)	Whitelisted or Verdict	213.209. [REDACTED] : False (AbuseIPDB)
Usage Type	213.209. [REDACTED] : Fixed Line ISP (AbuseIPDB), Compromised Server (Proxycheck).	Tor Network	213.209. [REDACTED] : False (AbuseIPDB), False (AlienVault OTX)	Last Reported	213.20 [REDACTED] : 26.12.2025 (AbuseIPDB)
Domain	213.209. [REDACTED] : e [REDACTED] de (AbuseIPDB)	VPN	213.209. [REDACTED] : no (Proxycheck), False (AlienVault OTX)	Proxy	213.209. [REDACTED] : yes (Proxycheck), False (AlienVault OTX)
Risk	213.209. [REDACTED] : 99 (Very dangerous) (Proxycheck)	Attack history	213.209. [REDACTED] : Total - 1, Login Attempt - 1 (Proxycheck)	Pulses Uniq Names	213.209. [REDACTED] : DugganUSA Threat Intel 2025-12-26 #1, Oz Batch: 50 IOCs (avg BDE: 80) Honeypot Data – T-Pot - Sydney, Australia - December 2025, LCIA HoneyNet Data - December 2025 - H0neytr4p, Honeypot Data - Decemb... (AlienVault OTX)

SECURITY ORCHESTRATION, AUTOMATION AND RESPONSE - SOAR

SOAR решает задачи L1:

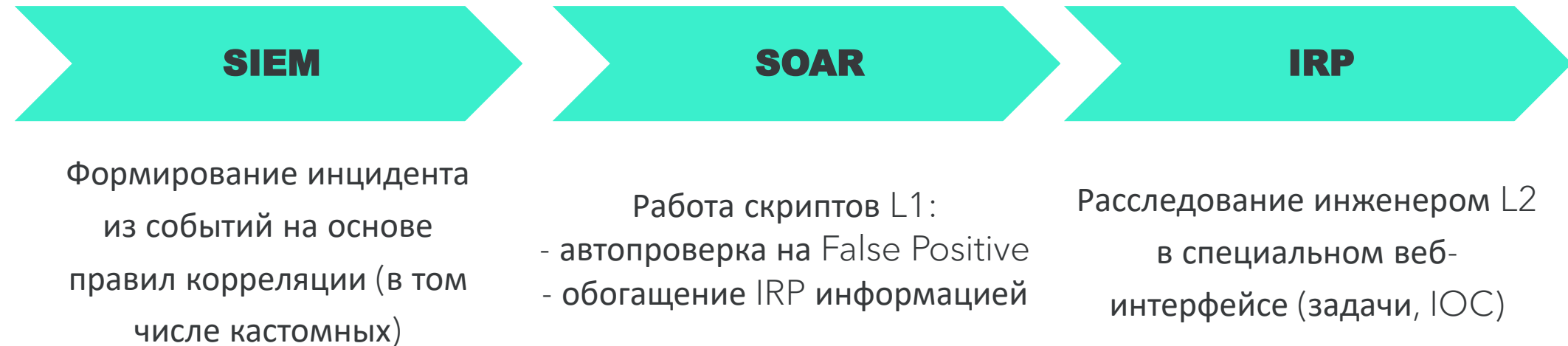
- показывает данные о хэш-суммах файлов из репутационных баз

File Type	A7691470E3...: Win32 EXE (VirusTotal Hash)	Total Detection	A7691470E3...: malicious - 0, suspicious - 0, undetected - 70, harmless - 0, timeout - 0, confirmed-timeout - 0, failure - 0, type-unsupported - 6 (VirusTotal Hash)	File Names	A7691470E3...: VirtualBox-7.1.12-169651-Win.exe, _cache_c9abc7bef5ff3929d1fd50cdcef1c5e894d47? (VirusTotal Hash)
File Signature	A7691470E3...: Product - Oracle VirtualBox, Copyright - Copyright (C) 2009-2025 Oracle Corporation, Description - VirtualBox Installer, File version - 7.1.12.169651 (VirusTotal Hash)				

ПУТЬ ИНЦИДЕНТА

В отличие от использования только базовых возможностей (SIEM) внедрение SOAR и IRP позволяет отказаться от рутинны на L1 и обогатить информацией на L2.

Таким образом существенно снижается количество False Positive сработок и время на реагирование (SLA) по True Positive сработкам.



ПРОЦЕСС РАССЛЕДОВАНИЯ НА L2



Сбор информации из различных источников и принятие решения (True Positive - TP или False Positive - FP)

Задачи расследования – найти ответ на все вопросы (5W):

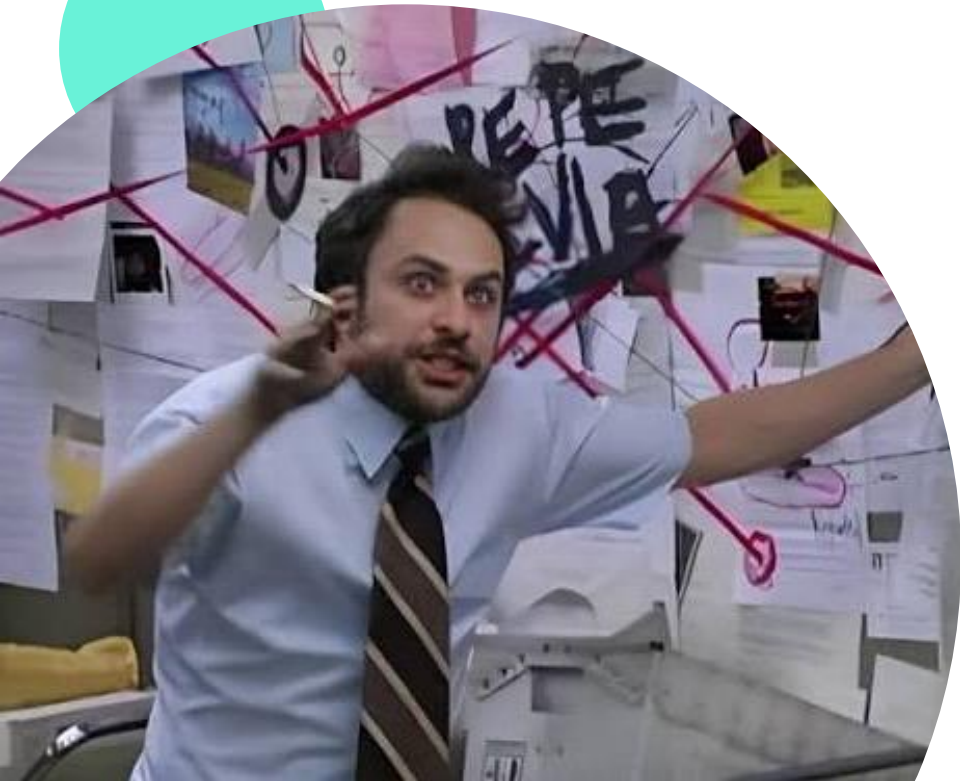
- когда случилось (when)
- что случилось (what)
- где/как случилось (where/how)
- кто виновник (who)
- зачем это нужно (why)

ПРОЦЕСС РАССЛЕДОВАНИЯ НА L2

Суть расследования –
подтверждение или
опровержение гипотез

ФАКТОРЫ, ВЛИЯЮЩИЕ НА РЕЗУЛЬТАТ РАССЛЕДОВАНИЯ:

- типична ли активность для данного заказчика
- подозрительно ли время активности
- вносилась ли похожая активность в профиль легитимной
- отвечал ли ранее заказчик по похожей активности
- чем сопровождается активность (смотрим сетевые подключения, создание УЗ, запуски процессов, ввод команд)



ПРОЦЕСС РАССЛЕДОВАНИЯ НА L2



Результат расследования:

- FP – закрываем и фильтруем во избежание будущих сработок
- TP – оповещаем заказчика об активности, при подтверждении легитимности – фильтруем, при атаке - реагирование

ФИЛЬТРАЦИЯ АКТИВНОСТИ

False Positive сработка должна быть внесена сотрудником L2 в профиль легитимной активности с целью фильтрации ложноположительных срабатываний.

Так работники SOC не будут отвлекаться на мешающий «фоновый шум» и смогут концентрироваться только на действительно важных алертах, требующих расследования.





ADVENTURE TIME

КОГДА СЛУЧИЛОСЬ? (WHERE)

Весна, субботняя ночь, 01:27 МСК, большой город уснул, на линию приходит алерт

Basic Information

Title	Обнаружение попыток изменить состав автозапуска ОС Windows (a [REDACTED] "c:\programdata\package cache\{7b91961e-93d9-46a5-ba4e-8b5f41b724b8}\dokansetup.exe" /burn.runonce) (2 Events)
--------------	---

Ночное время активности не характерно для активности администратора – 🚩 первый Red Flag 🚩

ПЕРВАЯ ГИПОТЕЗА



Администраторы пытаются установить что-то ночью.

Но! Мы не можем оставаться на одной гипотезе пока не ответили на все вопросы

КАК ВЫГЛЯДИТ РЕАЛЬНАЯ АТАКА?



ОЖИДАНИЕ:

Куча алертов о подозрительной активности, которые летят на линию

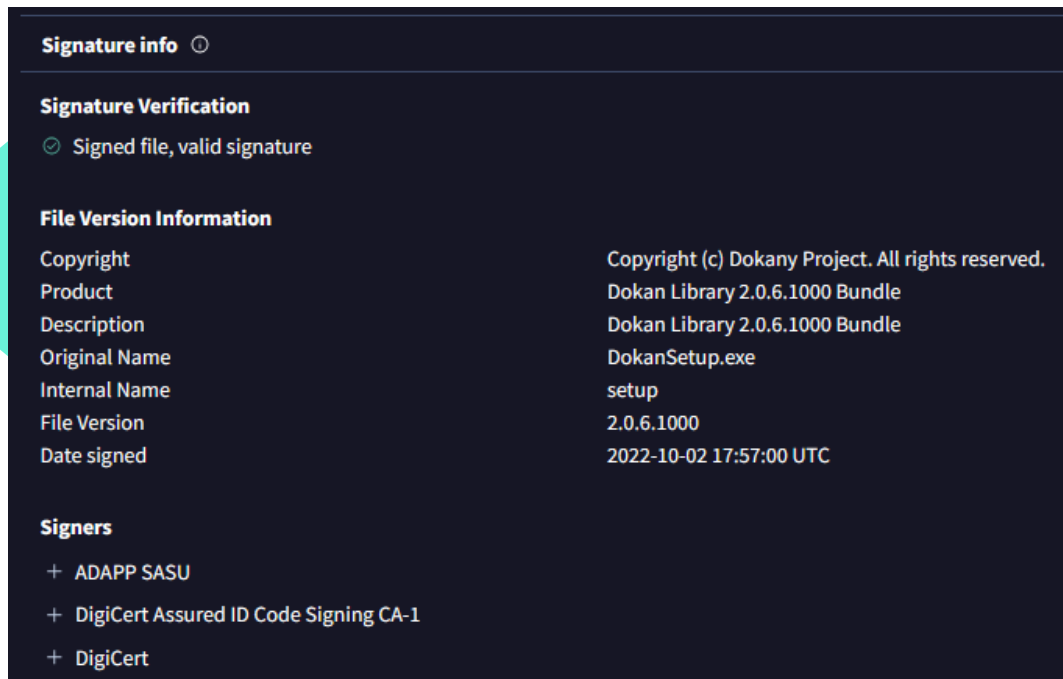
РЕАЛЬНОСТЬ:

Всего один алерт с любой критичностью, который можно случайно закрыть как FP

ВЫВОД:

К каждому инциденту нужно относиться как к «боевому» и присваивать FP только если нет никаких 🚩 Red Flag'ов 🚩 (есть уверенность в ответах на все 5W)

ЧТО СЛУЧИЛОСЬ? (WHAT)



Факты

- Файл в автозапуске – утилита Dokan (по хэш-сумме на VirusTotal)
- Ранее активность Dokan у заказчика ни разу не фиксировалась
- Dokan используют для создания виртуальных разделов ФС в Windows

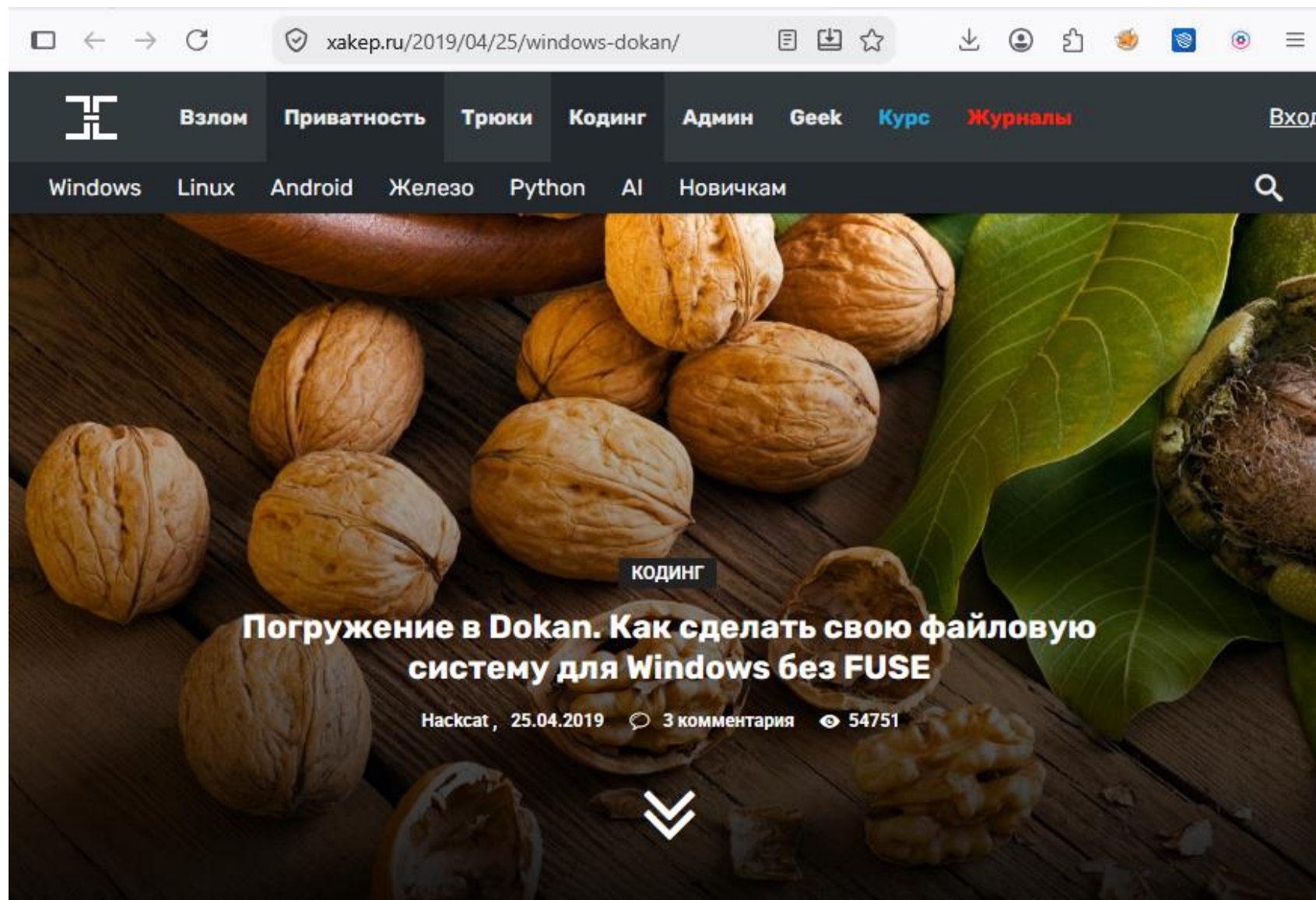
ЧТО СЛУЧИЛОСЬ? (WHAT)

Гипотеза

Обнаруживаем на хакер.ru что Dokan может использоваться для создания скрытых разделов, а это техника T1564.005 MITRE ATT&CK

Получили второй

🚩 Red Flag 🚩



ГДЕ/КАК СЛУЧИЛОСЬ? (WHERE/HOW)

Факты:

- Активность локальной УЗ administrator
- Цепочка входов на узел:

logged_users

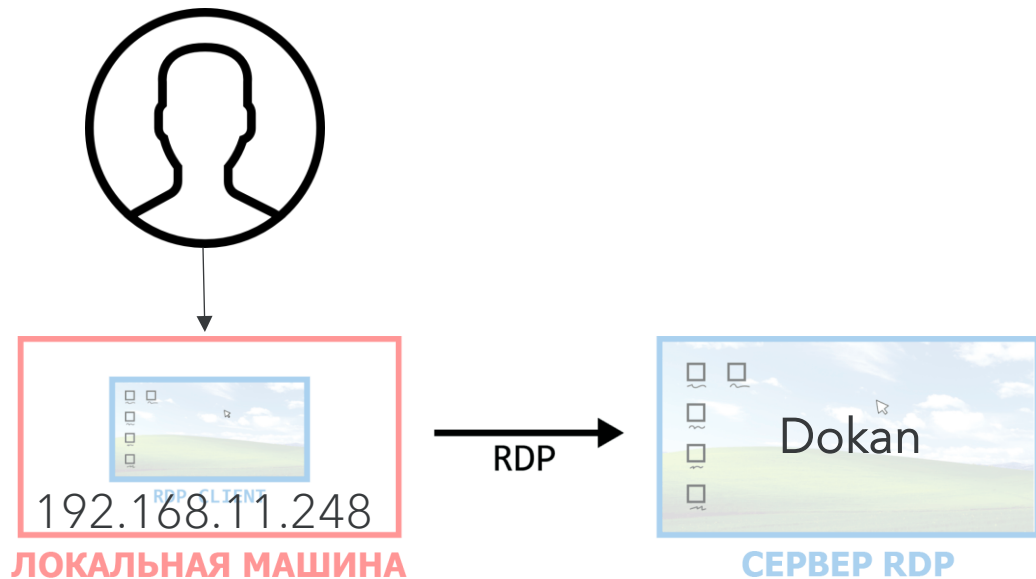
```
01:15:53 MSK: nt authority\anonymous logon (logon type: 3 - Network) from 192.168.11.248;  
01:16:19 MSK: domain_name\administrator (logon type: 3 - Network) from 192.168.11.248;  
01:22:44 MSK: host_name\administrator (logon type: 10 - RemoteInteractive);  
01:33:16 MSK: host_name\administrator (logon type: 3 - Network) from 192.168.11.248;
```

Гипотеза

Последовательность входов в IRP выглядит как повышение привилегий, выполненное за 7 минут с одного и того же адреса 192.168.11.248

Это третий  Red Flag 

КТО ВИНОВНИК (WHO)?



Факт

- Мы знаем адрес источника входов (RDP и Network) - 192.168.11.248

Далее нам нужно найти учетную запись виновника - кто именно подключался с адреса 192.168.11.248.

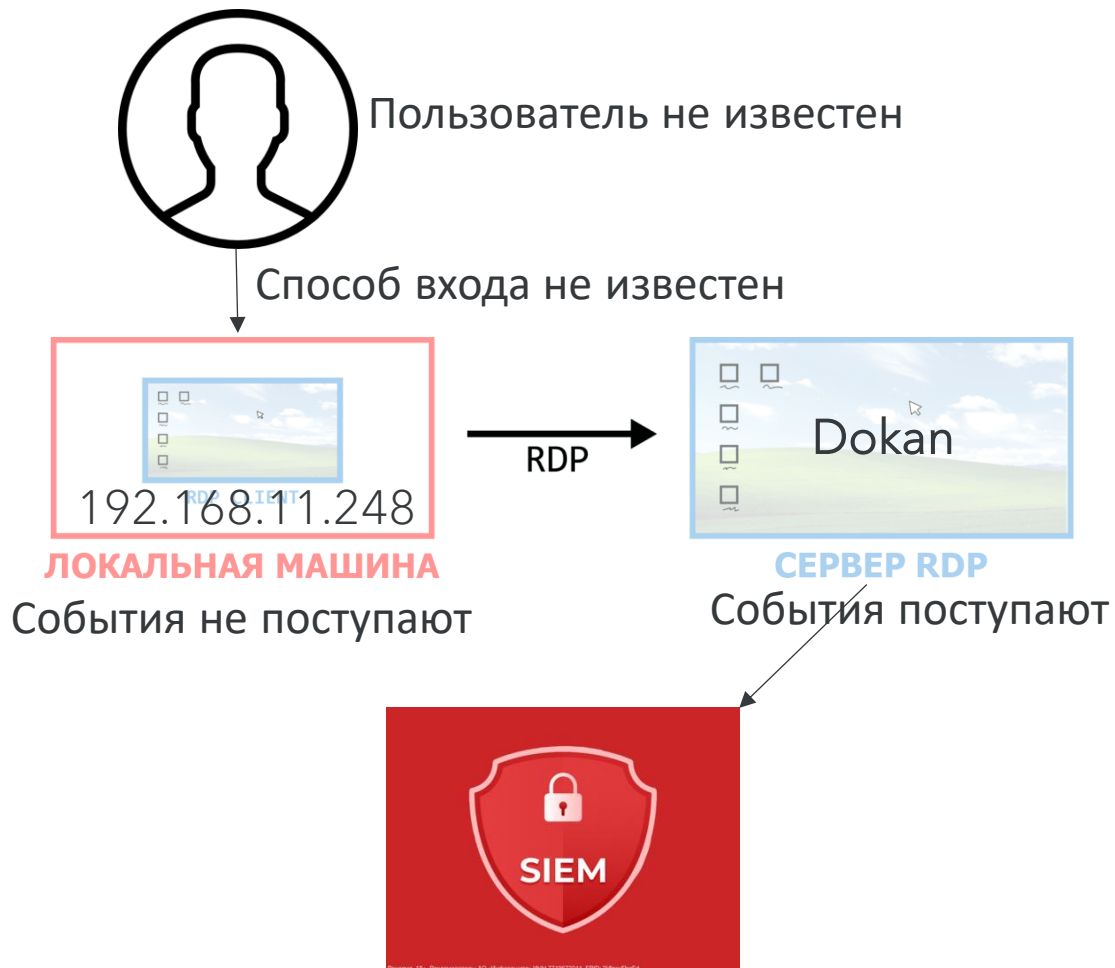
Для этого заходим в SIEM и ищем события интерактивного входа с персональной УЗ.

**МЫ УЗНАЛИ IP-АДРЕС УЗЛА, С КОТОРОГО ПРОИСХОДИЛИ УДАЛЕННЫЕ
ВХОДЫ ПО RDP, РЕШИЛИ ПОСМОТРЕТЬ СОБЫТИЯ С ЭТОГО УЗЛА В SIEM И...**



...ИХ НЕТ

КТО ВИНОВНИК (WHO)?

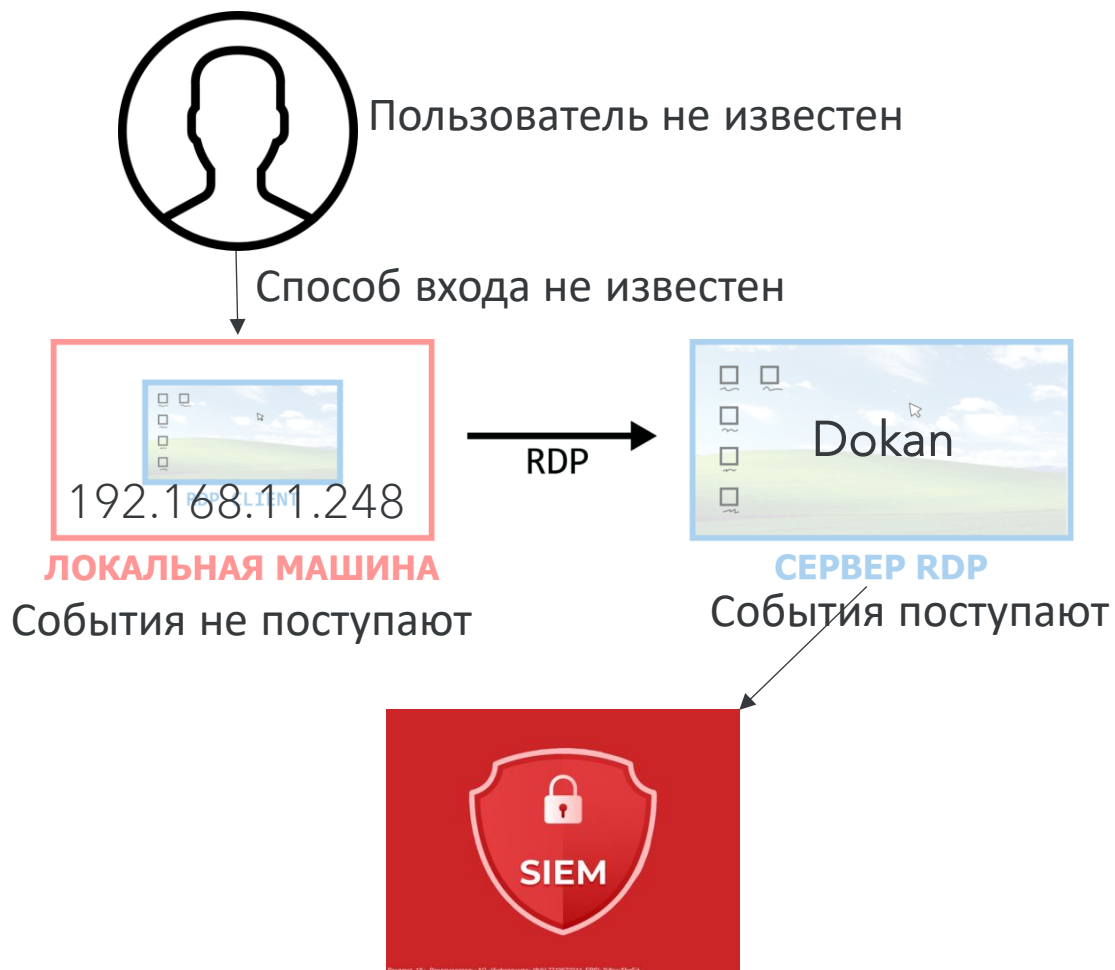


Факт

- Удаленные входы (RDP и Network) происходили с неизвестного узла, события с которого в SIEM не поступают

Получили четвертый  Red Flag 

СКОЛЬКО RED FLAG СОБРАНО В ХОДЕ РАССЛЕДОВАНИЯ



1.  Ночное время активности
2.  Инструмент ранее не использовался и может создавать скрытые разделы
3.  Повышение привилегий при входе
4.  Вход с неизвестного сетевого узла

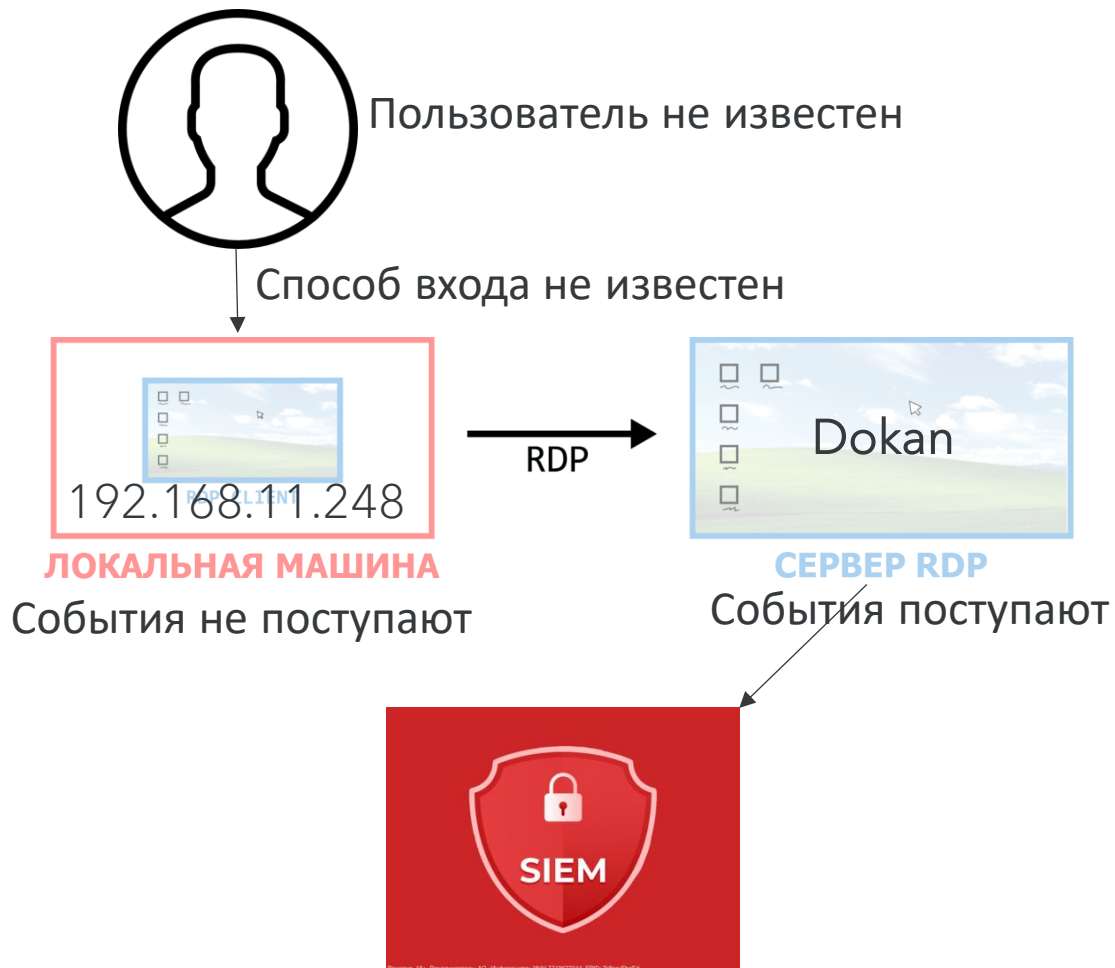




«Сомневаешься в
легитимности -
оповещай»

Сок Цзы

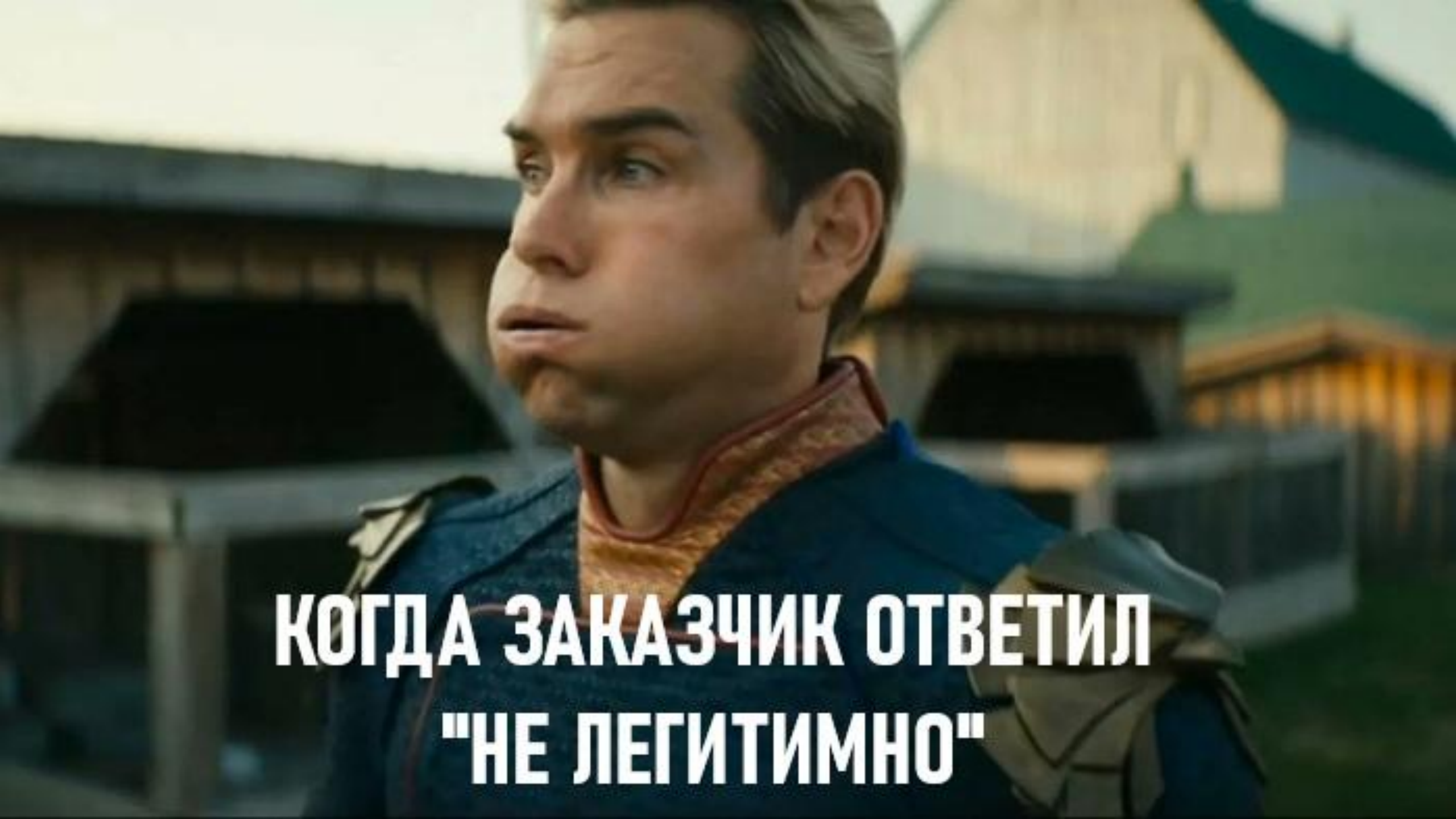
ЗАЧЕМ ЭТО НУЖНО (WHY)?



2 возможных гипотезы:

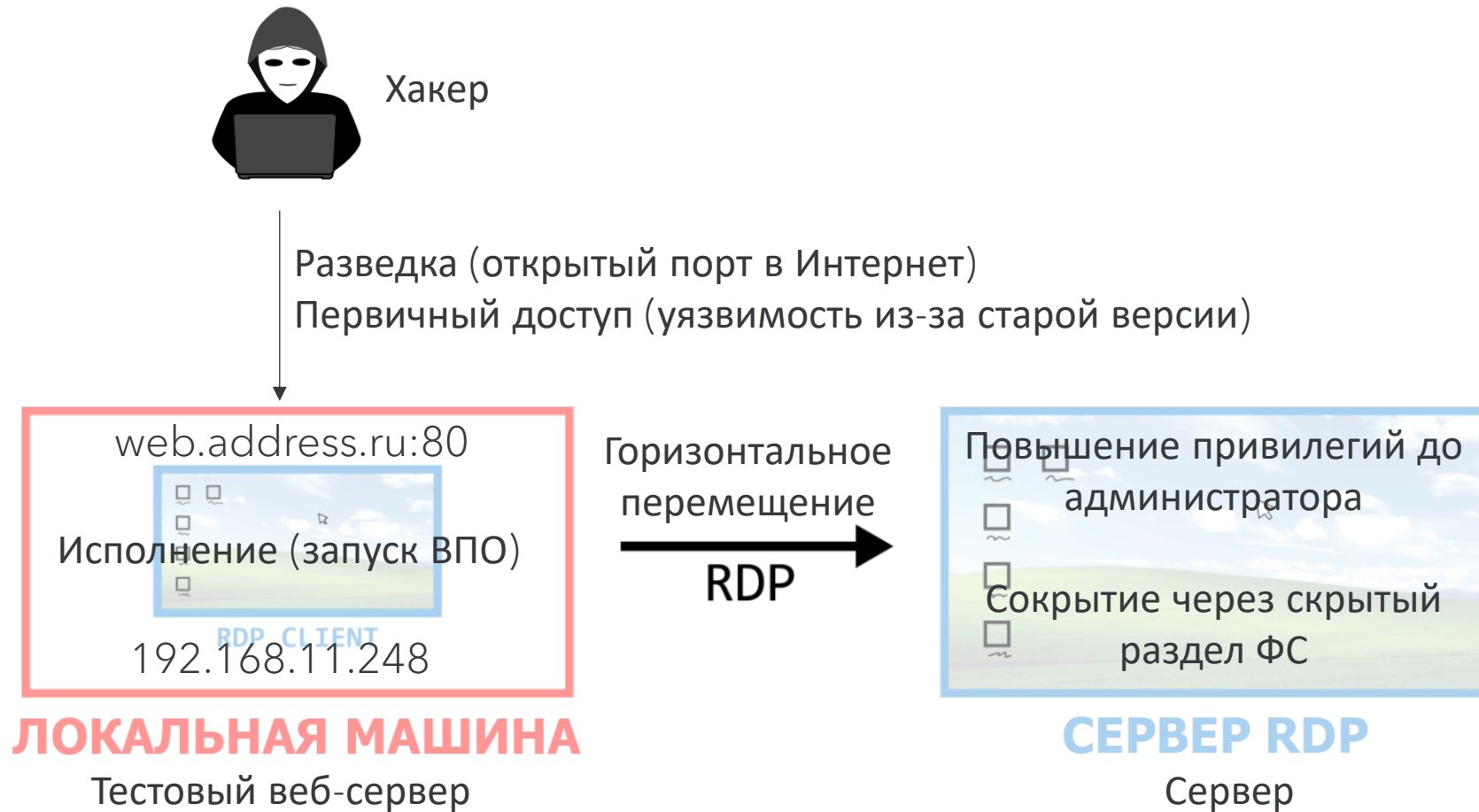
- 1) Администратор вошел с неизвестного (возможно личного) ноутбука и решил установить Dokan на сервере – внутренний нарушитель
- 2) Хакер готовит площадку для развития атаки – внешний нарушитель

Вывод – Срочно оповещаем заказчика и ждем ответ

A close-up shot of a man with light brown hair, looking off-camera to the left with a serious, slightly worried expression. He is wearing a blue uniform jacket with a red patterned collar and a tactical vest. The background is a blurred outdoor setting with traditional-style buildings.

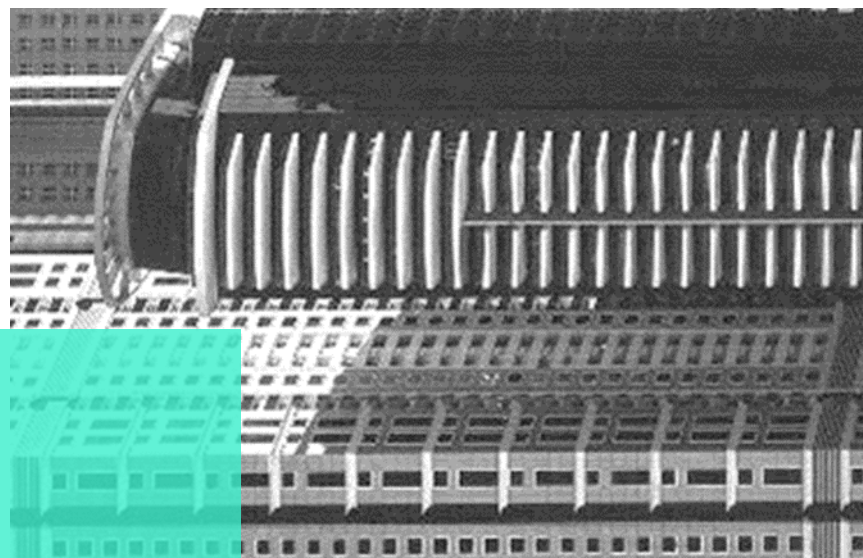
**КОГДА ЗАКАЗЧИК ОТВЕТИЛ
"НЕ ЛЕГИТИМНО"**

ВЫВОДЫ ПОСЛЕ РЕАГИРОВАНИЯ



ПОЧЕМУ АТАКА БЫЛА УСПЕШНО РАСПОЗНАНА

1. Принцип «Знай своего заказчика»
2. Автоматизация быстро собирает нужную информацию
3. Работа в биологические часы
4. Простота оповещения и эскалации
5. Узкое распределение ролей





**КАК ПОПАСТЬ К
НАМ РАБОТАТЬ**

РАБОТА ИНЖЕНЕРА L2 SOC

Преимущества:

1. Полная удаленка с предоставлением техники, в т.ч. из Иркутска
2. Менторство на время испытательного срока
3. Работа в биологические часы 6:00-15:00, 5 дней в неделю (плавающие выходные)
4. Возможность быстрого получения «боевого» опыта и карьерного роста
5. Компания в топе работодателей HH по средним компаниям, есть IT-аккредитация
6. Премии, ДМС, корпоративный мерч

Требования:

1. Понимание методов действий хакеров
2. Понимание сетевых технологий (OSI, маршрутизация, IPv4/IPv6, TCP/UDP, OSPF, SNMP, NTP, DHCP, VLAN)
3. Опыт работы с MaxPatrol/KUMA
4. Знание регулярных выражений
5. Логика + гугл, а не нейросети

Плюсом будет:

- образование/курсы и опыт работы по ИБ
- опыт системного администрирования
- опыт участия в CTF и аккаунты на тренировочных площадках (THM/HTB/Standoff и пр.)
- работа с pet-проектами

dmitry.s.milko@gmail.com

@mityanya135

Милько Дмитрий

ПРИМЕРЫ РЕАЛЬНЫХ КАРЬЕРНЫХ ТРЕКОВ

Студент по ИБ

Стажировка

**Работа в SOC
L2**

**Системный
администратор**

**Погружение в
ИБ**
*СТФ, ТНМ/НТВ,
курсы*

**Работа в SOC
L2**

**Специалист ИБ
другого
профиля**

**Развитие
скиллов**
*ТНМ/НТВ, СТФ,
курсы*

**Работа в SOC
L2**

БЛАГОДАРЮ ЗА ПРОЯВЛЕННЫЙ ИНТЕРЕС

Милько Дмитрий

dmitry.s.milko@gmail.com

[@mityanya135](#)