SOC-аналитик с нуля.

Полное руководство для старта в профессии

Tiers · Alert triage · False positives · Enrichment · Escalation · Metrics · Реальные кейсы · Карьерный путь



ОДИН АНАЛИТИК · ОДНА СМЕНА · 99% — ШУМ

ЛИСТАЙ · 20 СЛАЙДОВ ›

Security Operations Center

SOC — это не комната с мониторами. Это команда, которая замечает атаку, пока она ещё происходит, и останавливает её.



ЛЮДИ

Аналитики дежурят по сменам 24/7. Кто-то всегда следит за очередью событий.

ПРОЦЕССЫ

Чёткие playbooks, чтобы разные аналитики действовали одинаково в одинаковых ситуациях.

ТЕХНОЛОГИИ

Инструменты, которые собирают логи, ищут паттерны и генерируют алерты.

ЕДИНСТВЕННАЯ РАБОТА, КОТОРАЯ ДЕЙСТВИТЕЛЬНО ВАЖНА

Атакующий проникает · Двигается тихо · Добирается до данных · Нанесён ущерб

SOC ВМЕШИВАЕТСЯ ЗДЕСЬ

КАК ДОЛГО АТАКУЮЩИЙ МОЖЕТ ОСТАВАТЬСЯ НЕЗАМЕЧЕННЫМ

Без мониторинга — недели — месяцы

С работающим SOC — минуты — часы

Чем раньше SOC замечает активность, тем меньше данных уходит.
Эта разница — результат работы всей команды, процессов и технологий.

Кто работает в SOC

Алерты приходят не сами — за ними стоят люди.
У каждого уровня свои задачи, без которых SOC не работает.

TIER 1

Аналитик триажа

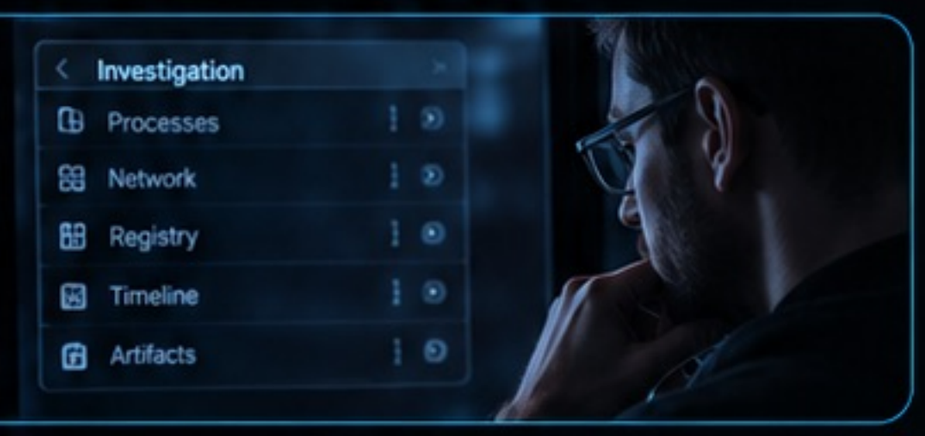
Работает с очередью алертов. Быстро определяет: это шум или реальный инцидент.



TIER 2

Аналитик реагирования на инциденты

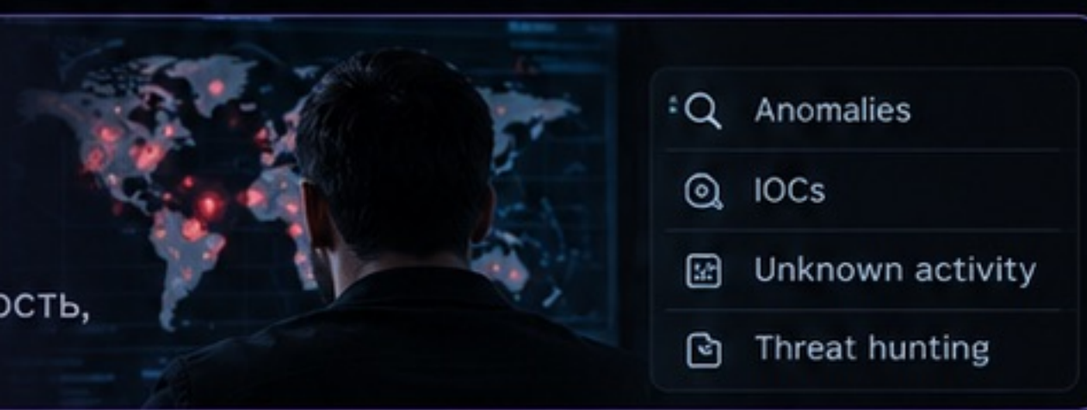
Разбирает то, что эскалировал L1.
Глубже анализирует: хосты, пользователи, таймлайны.



TIER 3

Threat hunter

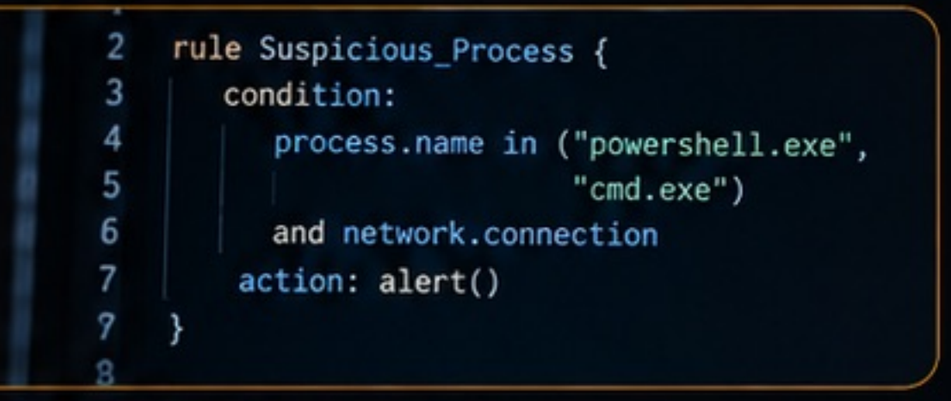
Не ждёт алертов. Ищет то, что системы не обнаружили: аномалии, скрытую активность, новые TTP.



ENGINEER

Инженер Detection

Пишет и дорабатывает правила, настраивает инструменты, чтобы очередь алертов была качественной.



```
rule Suspicious_Process {
  condition:
    process.name in ("powershell.exe",
                     "cmd.exe")
    and network.connection
  action: alert()
}
```

MANAGER

SOC lead

Отвечает за покрытие, процессы, метрики и то, чтобы команда была готова — сегодня и завтра.



СМЕНА

04/20

DETECT
INVESTIGATE
RESPOND

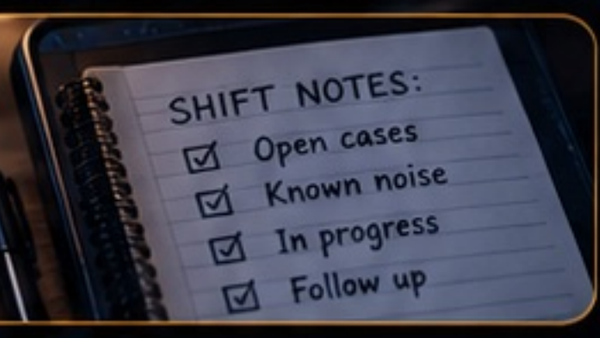
Один день в жизни SOC

SOC никогда не спит. Твоя смена начинается там, где кто-то другой её закончил.

08:00

Handover

Изучаешь заметки с предыдущей смены. Открытые кейсы, известный noise, всё, что ещё в работе.



08:20

Queue sweep

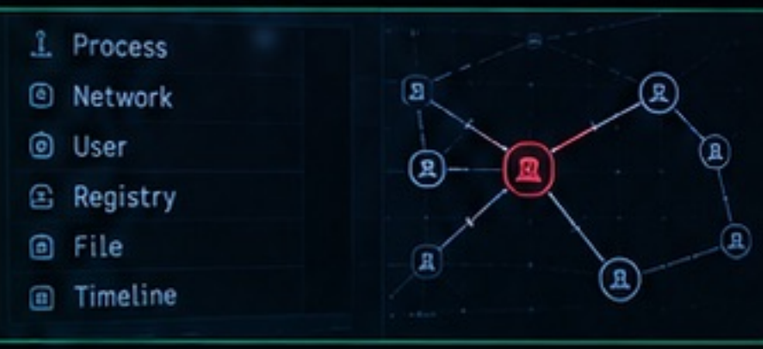
Просматриваешь ночные алерты, сортируешь их по severity. Быстро отсекаешь то, что выглядит как скоординированная активность.



09:00

Triage block

Основная часть работы. Разбираешь алерты: исследуешь, проверяешь, делаешь вывод. Повторяешь это десятки, а иногда и сотни раз.



13:00

Escalation

Два кейса не закрываются. Грамотно оформляешь их и передаёшь на Tier 2.



15:00

Tuning notes

Отмечаешь правило, которое сработало ~90 раз на безвредном процессе. Предлагаешь доработку, чтобы уменьшить noise.

```
rule Suspicious_Process {
    condition:
        process.name in ("powershell.exe",
                         "cmd.exe")
        action: alert()

}   # false positives -> tune
```

17:00

Handover

Передаёшь смену следующему аналитику. Оставляешь заметки, чтобы он продолжил с того места, где ты остановился.



ЛИСТАЙ • 20 СЛАЙДОВ >

PEOPLE • PROCESS • TECHNOLOGY

Откуда поступают данные в SOC

DETECT
INVESTIGATE
RESPOND

Ты не можешь обнаружить то, что не видишь. Всё, что происходит в источниках ниже, отправляет свои логи в одно место, чтобы их можно было анализировать вместе.

ENDPOINT

События процессов, входы, изменения файлов и другие действия на устройствах.

NETWORK

Сетевые соединения, DNS-запросы, трафик и события с сетевого оборудования.

IDENTITY

Кто вошёл, откуда и с какими правами (Active Directory, SSO, MFA и другие источники).

CLOUD

Вызовы API, изменения конфигурации, события в облачных сервисах (AWS, Azure, GCP и др.).

EMAIL

Отправители, ссылки, вложения, события фильтрации и доставки.

WEB

HTTP(S) запросы, посещения сайтов, заблокированные домены и события с прокси / web gateway.

Платформа логов

Одно место для поиска. Всё, что происходит ниже, случается ещё до того, как ты увидишь alert.

СБОР — Принимаем все логи из источников.

→

НОРМАЛИЗАЦИЯ — Приводим данные к единым полям.

→

КОРРЕЛЯЦИЯ — Связываем события из разных источников.

→

ОБНАРУЖЕНИЕ — Срабатывают правила и создаются alert.

КАК ЭТО РАБОТАЕТ

06/20

Путь лога до инцидента

DETECT
INVESTIGATE
RESPOND

Четыре ступени, которые превращают разрозненные события в реальный инцидент. Так выглядит модель мышления в SOC.

LOGS
TELL
A STORY
—

LOG

2 400 000

Сырые данные. Пользователь вошёл в систему, создан файл. Без контекста это просто запись.

```
user=jdoe  action=logon  result=success
```

```
2024-11-20 10:14:23  INFO  User
2024-11-20 10:14:23  INFO  Auth
2024-11-20 10:14:24  INFO  Sess
2024-11-20 10:14:25  INFO  File
```

EVENT

8 400

Лог обогащается контекстом: парсится, нормализуется и становится частью общей картины.

```
logon · jdoe · FIN-WS-114 · 03:12
```

User Logon
Host: FIN-WS-114
Source: Windows
User: jdoe
Time: 03:12

ALERT

310

Срабатывает правило. Система замечает отклонение и говорит: на это стоит посмотреть.

```
rule: logon from a new country
```

New country login detected
User: jdoe
Country: DE (Germany)
Previous: UA (Ukraine)
Risk score: 85

INCIDENT

2

Аналитик подтверждает: это реальная и потенциально опасная активность. Начинается реагирование.

```
case #4021 · confirmed
```

INCIDENT CONFIRMED
User: jdoe
Type: Suspicious login
Severity: High
Status: In progress

Анатомия одного алерта

OBSERVE
ANALYZE
INVESTIGATE
RESPOND

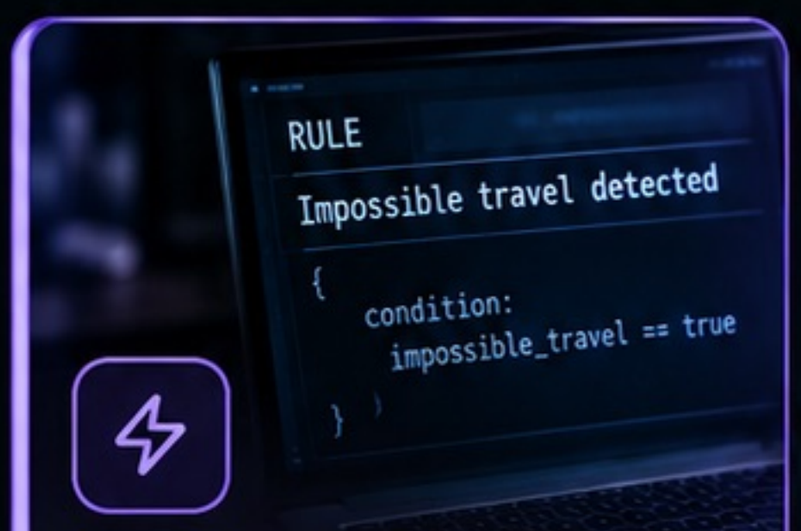
SOC

SAME
LOGS
DIFFERENT
STORIES

Прежде чем делать выводы, разберись в каждом поле. Новички смотрят только на заголовок и упускают суть, которая скрыта ниже.

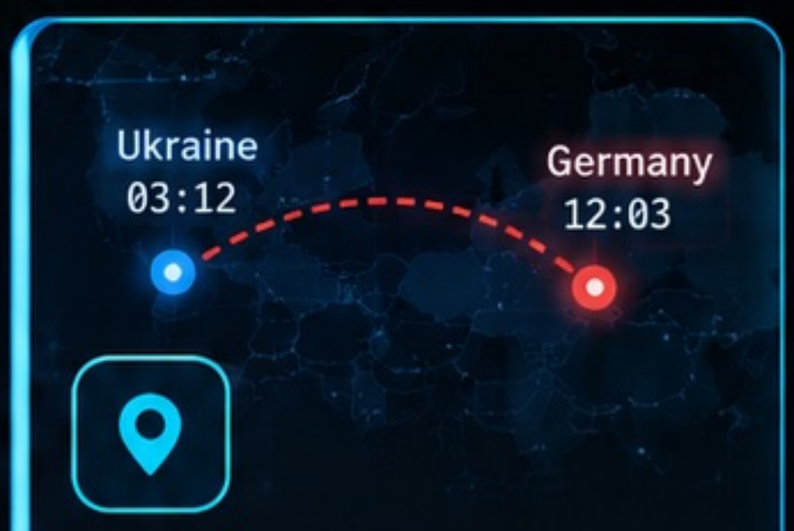
ALERT #A-40912 — HIGH

RULE	Impossible travel detected	— название правила
USER	finance.svc@corp.local	— кто (учётная запись)
HOST	FIN-WS-114	— на каком устройстве
TIME	03:12 local	— когда (время) • first seen — когда впервые замечено
DETAIL	2 sign-ins • 9 min apart	— фактические детали
SOURCE	Identity provider sign-in log	— источник события



Что сработало?

Расшифруй название правила и его условие. Это, например, проверка на **impossible travel** — входы из разных стран за короткое время.



Кто и откуда?

Это учётная запись из финансового отдела. Вход с ноутбука в Украине, через 9 минут — с другого устройства в Германии. Такое расстояние за это время физически невозможно.



Это нормально?

Сравни с привычной активностью за последние 30 дней. Если пользователь регулярно входит из разных стран — возможно, это легитимно. Если нет — это серьёзный признак компрометации.

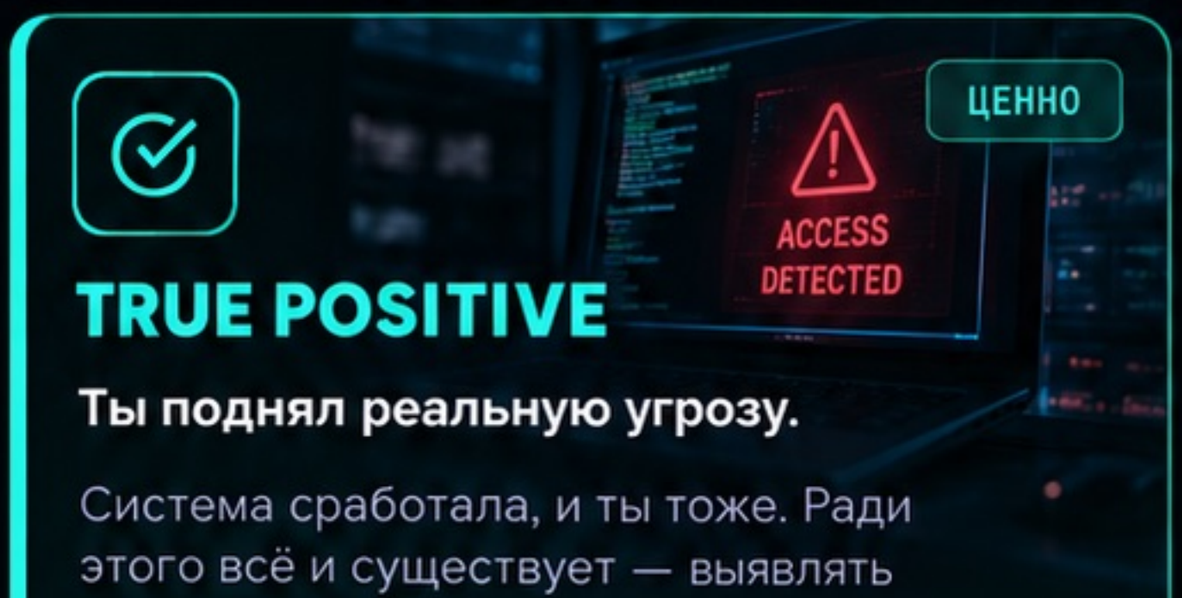
РЕЗУЛЬТАТ

08/20

OBSERVE
ANALYZE
INVESTIGATE
RESPOND

Четыре возможных исхода алерта

Каждый алерт в SOC заканчивается одним из этих сценариев. Только один из них меняет карьеру и это не самый шумный.



TRUE POSITIVE

Ты поднял реальную угрозу.

Система сработала, и ты тоже. Ради этого всё и существует — выявлять реальные атаки.

ЧТО ДЕЛАТЬ

Эскалировать, приложить артефакты и передать на дальнейшее реагирование.



FALSE POSITIVE

Ты поднял ложную тревогу.

Выглядит подозрительно, но угрозы нет. Такое бывает — важно закрыть алерт и добавить паттерн, чтобы правило стало точнее.

ЧТО ДЕЛАТЬ

Закрыть алерт и предложить исключение или доработку правила.



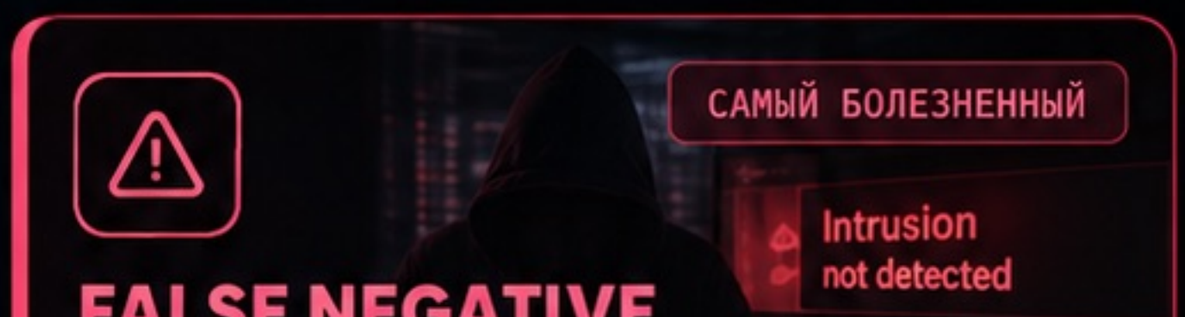
TRUE NEGATIVE

Ты не стал эскалировать, и всё ок.

Угроза есть, но она не актуальна для нашей среды. Твоя спокойная проверка сэкономила время всей команде.

ЧТО ДЕЛАТЬ

Ничего. Тихий анализ — тоже работа, и она важна.



FALSE NEGATIVE

Ты пропустил реальную угрозу.

Атака прошла незамеченной, а признаков не было. Такой сценарий учит больше всего — поэтому разберись, как это произошло, и добавь правило.

ЧТО ДЕЛАТЬ

Искать артефакты, восстановить картину и написать недостающее правило.

Пять вопросов каждый раз

Триаж — это не интуиция. Это одни и те же пять вопросов, заданные в правильном порядке, пока не появится ясность.

OBSERVE
ANALYZE
INVESTIGATE
RESPOND

SAME QUESTIONS BETTER ANSWERS

1 Что именно сработало?

Открой правило. Прочитай условие (rule) целиком, а не только название. Что конкретно совпало?

```
rule Suspicious_Process {
  condition:
    process.name == "powershell.exe"
    and network.outbound == true
}
```

2 Кто и к чему это относится?

Какой пользователь, какой хост, какие данные? Учитывай контекст. Администратор домена — не тестовая учётная запись.

user	jdoe
host	FIN-WS-114
data	C:\Finance\report.xlsx
domain	corp.local

3 Для них это нормально?

Проверь последние 30 дней. Насколько это частое событие? Это самый быстрый способ выявить false positive.



4 Что происходит дальше?

Проверь соседние события во времени. Это часть большего сценария? Эскалация, боковое перемещение или, наоборот, единичный случай?

03:11	Process started	powershell.exe
03:12	Network connection	146.70.12.3
03:13	File created	report.xlsx
03:14	Process ended	exit code 0

5 Могу ли я это подтвердить?

Если есть дополнительные артефакты и поведение подтверждается — это эскалация. Если доказательств нет — возвращаемся к настройке правила.

procmon.log	Found
network.pcap	Found
merged events	Correlated

LESS NOISE MORE IMPACT

КОНТЕКСТ

Контекст меняет ответ

Один и тот же alert может оказаться как пустяком, так и серьёзным инцидентом. Всё решает контекст, который ты добавляешь перед выводом.



RAW ALERT

Sign-in from an unusual location

GEO
Из какой страны и впервые ли мы видим вход?

ASSET
Насколько критичен этот хост или учётная запись?

IDENTITY
Кто этот пользователь и к каким данным имеет доступ?

INTEL
Есть ли сведения об этом источнике в threat intelligence?

ЗАКРЫТ • FALSE POSITIVE

Менеджер по продажам. Известный паттерн поездок. Корпоративный ноутбук, MFA пройден, та же страна, что и в прошлой поездке.



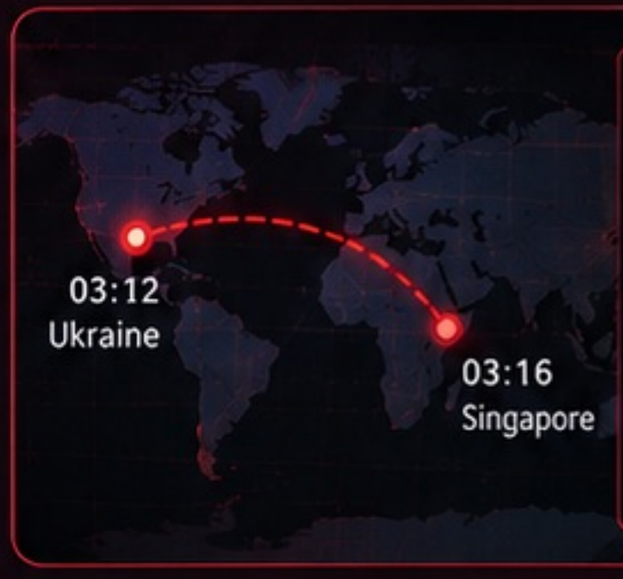
User sign-in — Success

User	a.petrov@corp.com
Location	Germany
Device	Corp laptop
MFA	✓ Passed
Last seen	1 week ago

- Роль: обычный пользователь
- MFA: пройден
- История: регулярные поездки

ЭСКАЛИРОВАН • TIER 2

Учётная запись финансового сервиса. Нет MFA. Новая страна в 03:12, а через 4 минуты — смена пароля.



Suspicious activity

User	finance.svc
Location	Singapore
MFA	Not configured
Action	Password change
Risk	High

- Роль: сервисная учётная запись
- MFA: не настроен
- История: нет прежней активности

ЛИСТАЙ • 20 СЛАЙДОВ >

CONTEXT · BETTER DECISIONS · STRONGER SOC

Серьёзность не равно приоритет

OBSERVE
ANALYZE
INVESTIGATE
RESPOND

Инструмент присваивает alert'у уровень серьёзности на основе правила. Приоритет — это то, что этот alert действительно может затронуть.

СЕРЬЁЗНОСТЬ (SEVERITY)	НИЗКАЯ ЦЕННОСТЬ (LOW VALUE)	ОБЫЧНАЯ (NORMAL)	КРИТИЧНЫЙ АКТИВ (CRITICAL ASSET)
ВЫСОКАЯ (HIGH)	P2	P1	P1
СРЕДНЯЯ (MEDIUM)	P3	P2	P1
НИЗКАЯ (LOW)	P4	P3	P2

SAME SIGNAL DIFFERENT IMPACT

Alert средней серьёзности на domain controller может иметь **более высокий приоритет**, чем критичный alert на test box.

Девяносто одинаковых alert'ов из одного backup job — это **один ticket**, а не девяносто.

OBSERVE
ANALYZE
INVESTIGATE
RESPOND

Закрыть или эскалировать?

Не нужно быть уверенным на 100%, чтобы закрыть alert. Важно понимать, почему имеющихся данных недостаточно для эскалации.

SAME
DATA
DIFFERENT
DECISIONS

Могу ли я доказать, что это произошло?

ДА

НЕТ

ЗАКРЫТЬ

Когда есть достаточные данные

Зафиксируй вывод
Опиши, что именно ты увидел и почему это не инцидент.

Укажи сработавшее правило
Чтобы в будущем можно было учитывать паттерн.

Обоснуй, почему это безопасно
Например: backup job, known scanner, legitimate travel.

Отметь правило, если шумит
Это часть triage, а не лишняя работа.

ЭСКАЛИРОВАТЬ

Когда есть признаки, но нужны другие

Опиши, что ты увидел
Факты с таймштампами, без предположений и эмоций.

Перечисли, что проверил
Включая то, что недоступно или не удалось установить.

Укажи, что осталось неясным
Открытые вопросы — это ключ для следующего уровня.

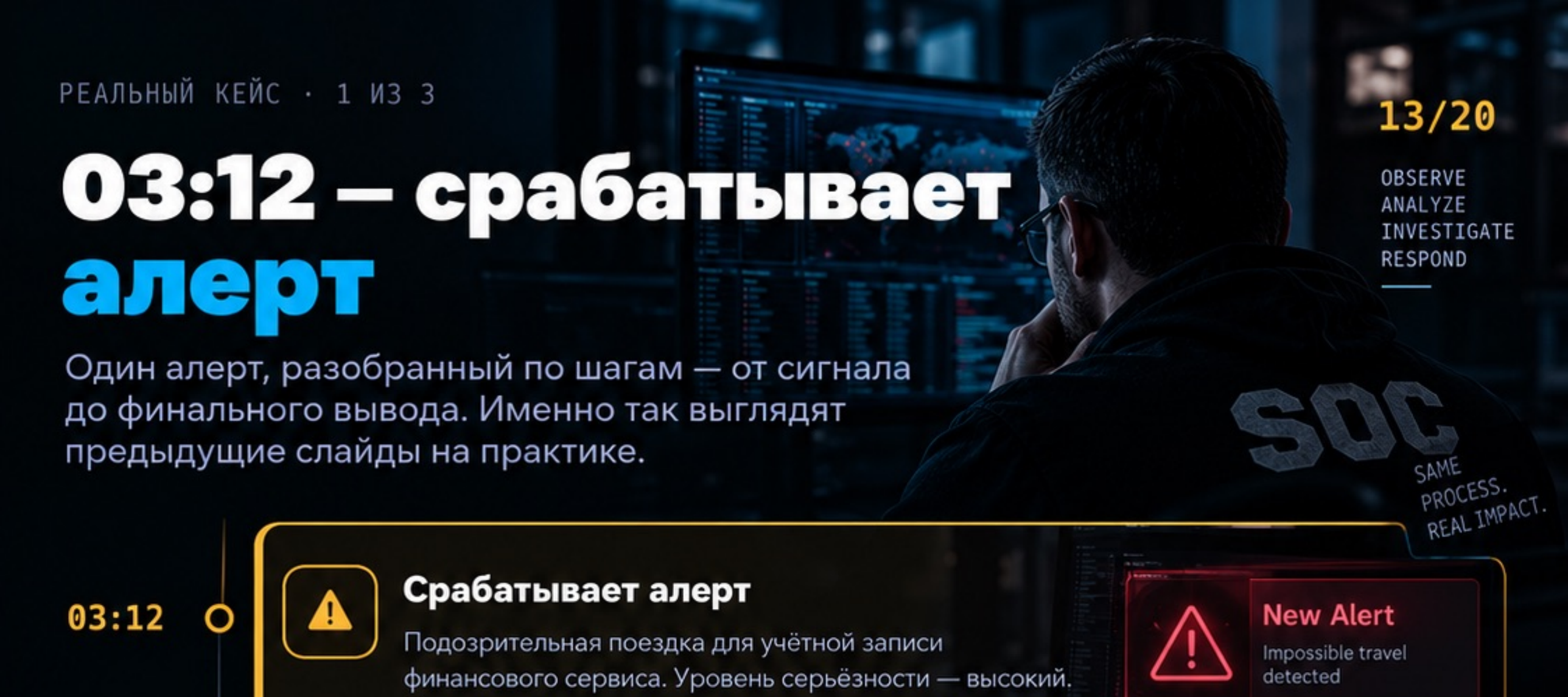
Добавь таймштампы и контекст
Это помогает Tier 2 быстрее продолжить расследование.

Эскалация без нужды стоит времени и денег.
Закрывать реальные неинциденты — тоже навык. Новички часто делают наоборот.

OBSERVE
ANALYZE
INVESTIGATE
RESPOND

03:12 — срабатывает алерт

Один алерт, разобранный по шагам — от сигнала до финального вывода. Именно так выглядят предыдущие слайды на практике.



03:12

Срабатывает алерт

Подозрительная поездка для учётной записи финансового сервиса. Уровень серьёзности — высокий. Пока нет признаков, что кто-то уже успел отреагировать.

New Alert
Impossible travel detected

03:14

Изучаем весь алерт

Два успешных входа с интервалом девять минут из двух стран. Та же учётная запись, тот же тип сессии.

Time	Event	Location
03:12	Successful login	Ukraine
03:21	Successful login	Singapore

03:16

Проверяем идентичность

Это сервисная учётная запись. Интерактивные входы из неожиданных стран для неё нехарактерны и не должны происходить.

finance.svc — service account

Type	Service Account
MFA	Not configured
Interactive logon	Not expected

03:19

Смотрим, что считается нормой

История за последние 30 дней: у этой учётной записи никогда не было интерактивных входов. Такой сценарий не встречался ни разу.

Интерактивные входы (30 дней) 0

1 янв 8 янв 15 янв 22 янв 29 янв

03:22

Финальный вывод

Это не легитимная поездка. Используются учётные данные, которым не место в таком сценарии.

Threat
Credential misuse

03:22 — расследование

Каждый alert — это вопрос. Ответ почти всегда находится в деталях и нескольких минутах вокруг события.

OBSERVE
ANALYZE
INVESTIGATE
RESPOND

SAME ALERTS DIFFERENT STORDS

03:03 — **9 неудачных входов подряд**
С одного источника, один за другим.
185.199.110.25
Ukraine

03:12 — **1 успешный вход**
Сработал наш alert.
185.199.110.25
Ukraine

03:16 — **Создано правило пересылки (mailbox rule)**
Автоматическая пересылка, затем удаление.
New inbox rule
auto-forward

03:20 — **Проверен второй аккаунт**
Тот же источник, новый username.
185.199.110.25
Ukraine

КАК ЭТО СВЯЗАНО?

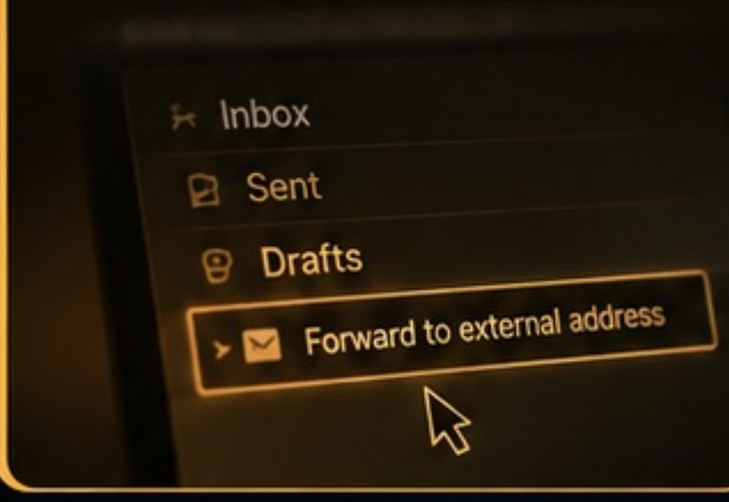
Password spray

Девять неудачных попыток, затем один успешный вход — это не опечатка, а типичная атака.



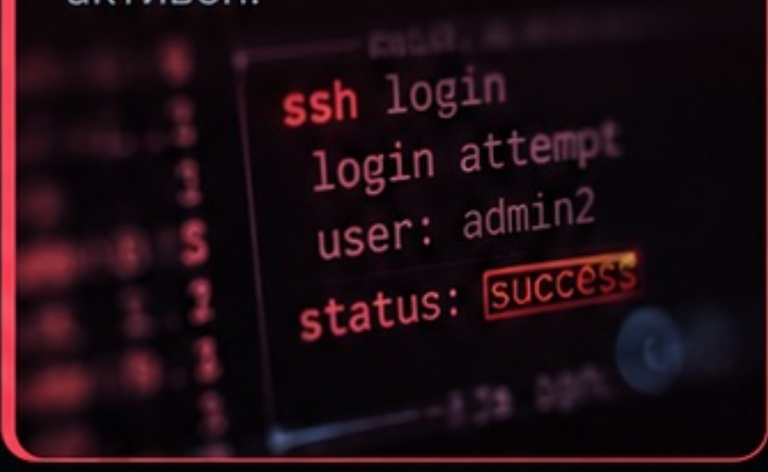
Persistence

Создание mailbox rule обеспечивает доступ даже после смены пароля.



Still active

Попытка входа во второй аккаунт в 03:20 — значит, злоумышленник всё ещё активен.



OBSERVE
ANALYZE
INVESTIGATE
RESPOND

03:26 — вывод и закрытие

От alert'а до сдерживания прошло 14 минут. Итоговый отчёт — не формальность, а то, что помогает учиться и становиться сильнее.

ЧТО СДЕЛАЛ TIER 2 ДАЛЬШЕ?

Отключил учётную запись — 03:26

→

Завершил активные сессии — 03:27

→

Удалил правило пересылки (mail rule) — 03:31

→

Сбросил и расширил проверку (re-scope) — 03:40

ИТОГ, КОТОРЫЙ ЗАФИКСИРОВАЛ АНАЛИТИК

VERDICT	**True positive • компрометация учётной записи**	CLOSED
EVIDENCE	9 неудачных входов, 1 успешный вход, создано правило пересылки (mail rule) через 4 минуты	
SCOPE	1 service account, 1 mailbox, второй аккаунт также проверен	
ACTION	Учётная запись отключена, активные сессии завершены, правило пересылки удалено	
OPEN	Источник учётных данных пока неизвестен	INVESTIGATE
HANDOFF	Передано Tier 3 для поиска того же источника в других аккаунтах	

Никто не запомнит, как ты рассуждал.
Останется только твой кейс-ноут — пиши его так, чтобы им мог воспользоваться кто угодно.

PEOPLE
PROCESS
TECHNOLOGY
SECURITY

С чем ты на самом деле работаешь

Tools
Detect
Investigate
Respond

Эти шесть категорий инструментов покрывают почти всё, с чем сталкивается SOC. Сначала пойми категорию, потом запомни конкретные решения.

Log Platform

Собирает всё в одном месте и запускает правила детекции, которые генерируют alerts.

03:14:27	INFO	User login successful
03:14:32	WARN	Failed authentication
03:14:33	INFO	Process created
03:14:35	ERROR	Suspicious activity detected
03:14:37	INFO	Connection from new IP

Endpoint Agent

Видит процессы, файлы и команды непосредственно на устройстве.

Processes
File system
Registry
Network
Commands

Endpoint Protected

Automation

Выполняет рутинные шаги playbook'а до того, как ты откроешь кейс.

Trigger → Enrich → Check → Respond

Threat Intel

Подсказывает, известны ли IP, hash или домен как вредоносные.

185.199.110.25 Malicious

Reputation	Malicious
First seen	2022-11-04
Sources	VirusTotal, AbuseIPDB

Sandbox

Безопасно запускает подозрительные файлы и показывает, что они делают.

sample.exe
Execution started...
Monitored 1423 actions
Suspicious behavior detected
Report generated

Case System

Здесь alert превращается в тикет с владельцем, историей и всеми артефактами.

#4578 Suspicious login activity — Open

Owner	@ @analyst
Priority	High
Tags	initial-access, valid-credentials

Слова, которые ты услышишь в первый день

Половина успеха в SOC — говорить на одном языке.
Вот ключевые термины, которые встретятся сразу.

DETECT
INVESTIGATE
RESPOND
REPEAT

IOC

Индикатор компрометации.

Конкретный след, который оставляет злоумышленник: хеш файла, домен, IP, URL.

hash · domain · IP · URL

SHA256: a3f5e8c9...
Domain: bad-domain.com
IP: 185.199.110.25
URL: hxxp://malicious

TTP

Тактики, техники и процедуры.

Как атакует злоумышленник, а не что он оставил. TTP помогают понимать его поведение и выбирать нужные инструменты.

tactics · techniques · procedures

INITIAL ACCESS
EXECUTION
PERSISTENCE
IMPACT

BASELINE

Нормальная картина активности.

То, как система обычно выглядит. Без baseline любой шум кажется подозрительным.

normal · behavior · profile

Normal activity
Anomaly

PLAYBOOK

Пошаговый план.

Готовые действия для конкретного типа alert'а, чтобы не изобретать велосипед в 3 часа ночи.

steps · response · consistency

Incident Playbook
- [x] 1. Triage
- [x] 2. Investigation
- [x] 3. Containment
- [ ] 4. Eradication
- [ ] 5. Recovery

USE CASE

Сценарий детекции.

Что именно мы хотим выявлять, плюс правило и данные, которые это ловят.

detection · rule · data

```
IF    multiple_failed_logins
AND   same_source_ip
THEN  create_alert()
```

DWELL TIME

Время нахождения в системе.

Как долго злоумышленник оставался незамеченным. Чем меньше — тем лучше.

detection · response · risk

3 days
Initial access — Detected

TUNING

Настройка правил.

Делаем так, чтобы правило не срабатывало на то, что не является угрозой.

false positive · noise · accuracy

Sensitivity
False positives
Coverage

CONTAINMENT

Сдерживание.

Останавливаем распространение угрозы. Не исправляем навсегда и не чистим — просто локализуем.

isolate · block · limit

Host isolated
Network access blocked

Как оценивают эффективность SOC

Четыре метрики показывают, как работает SOC.
Три из них про скорость. Одна — про здравый смысл.

METRICS DRIVE IMPACT

Чем меньше — тем лучше

MTTD

Среднее время обнаружения

Сколько времени проходит
от первой активности злоумышленника
до срабатывания alert'а.



detections · visibility · time

Чем меньше — тем лучше

MTTR

Среднее время реагирования

Сколько времени проходит
от срабатывания alert'а
до остановки атаки.



response · containment · recovery

Про реальность событий

DWELL

Время присутствия

Как долго злоумышленник находился
в инфраструктуре до того, как его
заметили.



timeline · stealth · history

Чем ниже — тем лучше

FP RATE

Доля ложных срабатываний

Какой процент alert'ов
оказался не угрозой.



noise · tuning · accuracy

Усталость от alert'ов — реальный риск, а не жалоба

Когда 9 из 10 alert'ов оказываются шумом,
люди начинают закрывать кейсы, не читая.
Именно так пропускают десятый.
Настройка правил — это не уборка, а ключевая
часть детекции.

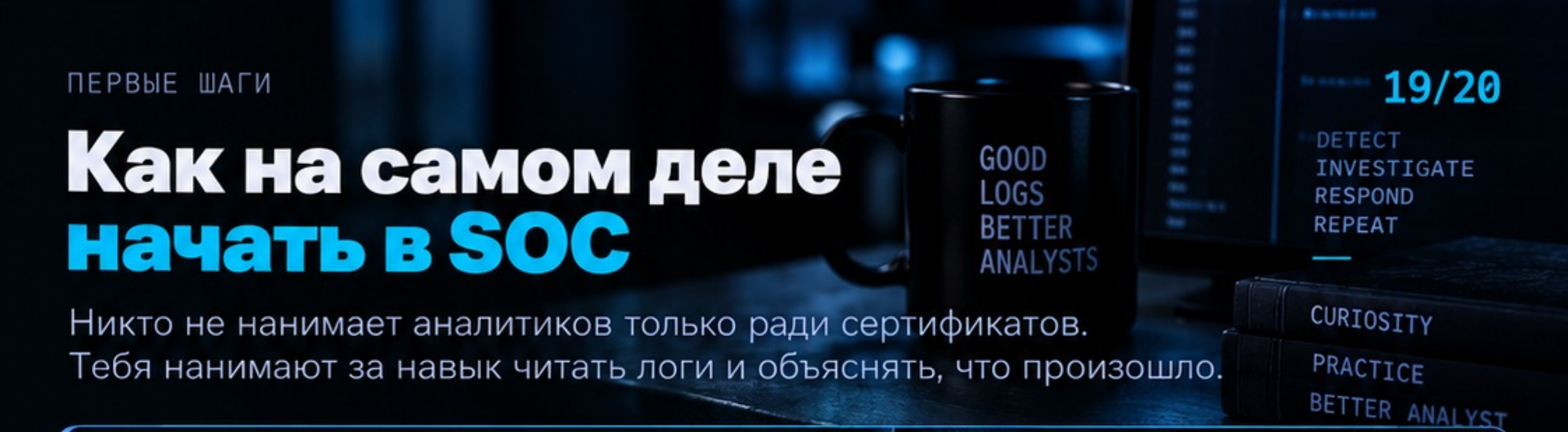
alert fatigue · rule tuning · human factor



ПЕРВЫЕ ШАГИ

Как на самом деле начать в SOC

Никто не нанимает аналитиков только ради сертификатов.
Тебя нанимают за навык читать логи и объяснять, что произошло.



1 Собери, за чем наблюдать

Подойдёт старый ноутбук, виртуальная машина или домашний роутер. Главное — чтобы у тебя был источник логов, который можно анализировать.

home lab · logs · visibility

```
May 10 10:24:01 host sshd[1234]: Failed password
May 10 10:24:17 host sudo: session opened
May 10 10:25:03 host kernel: suspicious activity
May 10 10:25:19 host ufw: BLOCK IN=eth0
May 10 10:25:43 host CRON[5678]: (root) CMD ...
```

ЛЮБАЯ СРЕДА ПОДХОДИТ

2 Научись читать логи «в сыром виде»

Начни с auth logs, web server logs, sign-in logs. Сначала в терминале, без готовых инструментов и дашбордов.

auth logs · web logs · raw logs

```
$ cat /var/log/auth.log | grep 'Failed'
May 10 10:24:17 host sshd[1234]: Failed passwor
May 10 10:24:58 host sshd[1234]: Failed passwor
May 10 10:25:36 host sshd[1234]: Failed passwor
May 10 10:26:01 host sshd[1234]: Accepted passwo
```

ТЕРМИНАЛ ТВОЙ ДРУГ

3 Потренируйся на своём окружении

Сымитируй неуспешный вход, найди его в логах и разберись, что именно произошло. Пройди весь цикл от события до вывода.

simulate · investigate · full cycle

```
$ ssh admin@192.168.1.10
admin@192.168.1.10's password:
Permission denied, please try again.
admin@192.168.1.10's password:
Permission denied, please try again.
```

ЛУЧШИЕ ОШИБКИ — СВОИ

4 Освой один query language

Выбери любой: SQL, KQL, SPL или другой. Синтаксис везде разный, но логика одна.

SQL · KQL · SPL · query

```
SELECT
  source_ip, COUNT(*) as attempts
FROM auth_logs
WHERE status = 'failed'
GROUP BY source_ip
ORDER BY attempts DESC;
```

ОДИН ЯЗЫК ДОСТАТЧНО

5 Разбери три реальных кейса

Оформи мини-отчёты: alert, evidence, итоговый вывод и что осталось неясным. Это похоже на реальные задачи из интервью.

alert · evidence · verdict · open questions

Case 1	Brute force attempt	Closed
Case 2	Suspicious download	Investigating
Case 3	Lateral movement	Open

ПРАКТИКА > ТЕОРИИ

Лучший старт — это практика.
Сертификаты помогут, но именно умение читать логи отличает хорошего аналитика.

ЗНАНИЯ РАБОТАЮТ ЛУЧШЕ

Сохрани этот пост перед своей первой сменой в SOC.

Через неделю ты будешь перечитывать эти слайды совсем другими глазами.

лайк комментируй делись сохрани

ПОДПИСЫВАЙСЯ
@lionsoulbatyshchikov