

PHDays 2025



30.05.2025



Подходы к построению безопасной архитектуры: от kill chain до метода Сократа

Спикер: Анна Лучник

«Защитники думают списками,
атакующие — графами.
Пока это так,
атакующие побеждают.»

Джон Ламберт

«Defenders think in lists. Attackers think in graphs. As long as this is true, attackers win.»
John Lambert

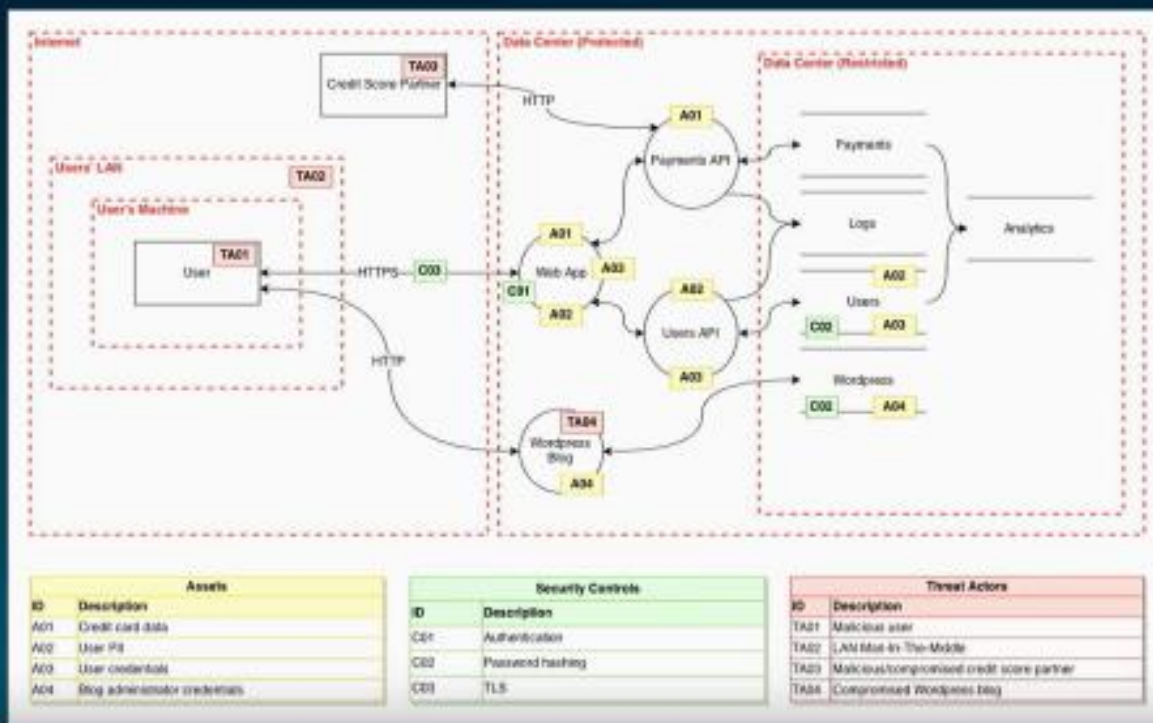


Подходы к построению безопасной архитектуры: от kill chain до метода Сократа

Моделирование потоков данных



Спикер: Анна Лучник

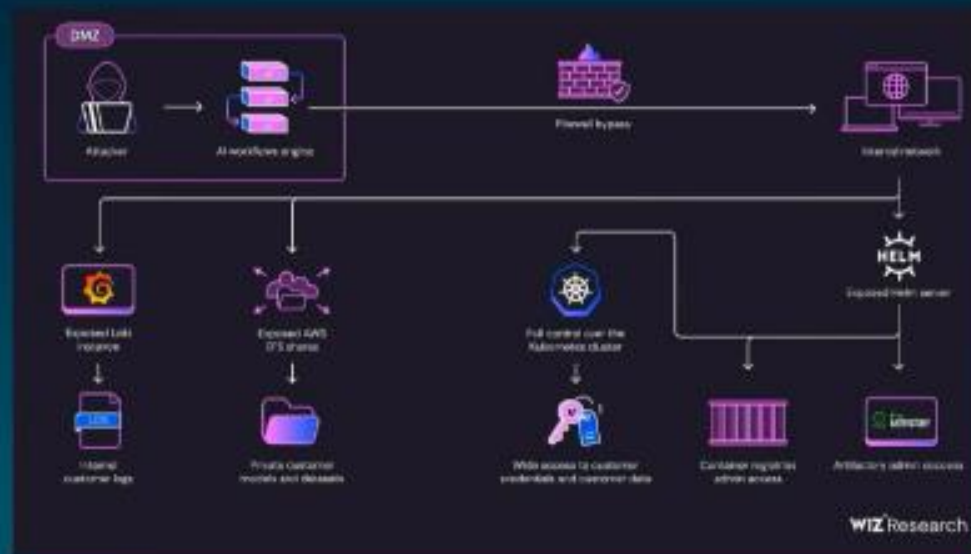


Подходы к построению безопасной архитектуры: от kill chain до метода Сократа

Спикер: Анна Лучник

Доверие к решениям с нулевым доверием

SAPwred от Wiz Research



Подходы к построению безопасной архитектуры: от kill chain до метода Сократа

Спикер: Анна Лучник

Метод Сократа в ИТ: инструмент для разбора решений и архитектур

Поиск истины через диалог,
вопросы и критическое мышление.

1. Утверждение: "Нам нужно внедрить XDR".
2. Уточнение: "Что именно вы понимаете под XDR?"
3. Контексты: "Где это реально помогает, а где нет?"
4. Логика: "Не дублирует ли это уже внедренный SIEM?"
5. Альтернативы: "А что если ничего не менять?"



Что делать?



При внедрении новых систем и
редизайне рассматривать комплексную
архитектуру и безопасность

Мыслить комплексно

- Графами
- Связями
- Потоками данных
- Вместо списков требований и лучших практик

Следить за стыками

- Между системами
- Между компаниями
- Между границами доверия

Не доверять неявно

- Решениям Zero Trust
- Цепочкам поставок
- Партнерам и подрядчикам
- Обновлениям
- Любым системам

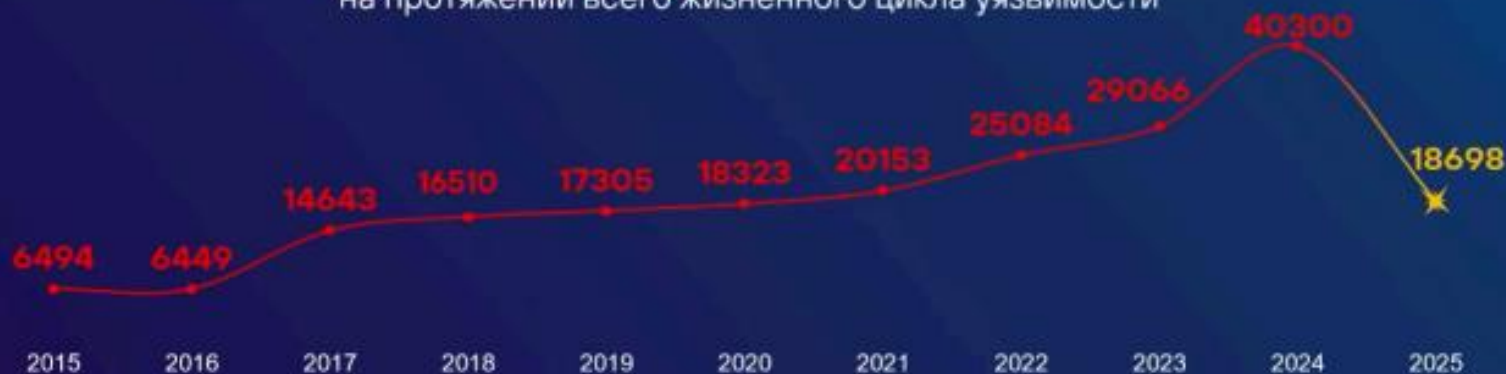


VOC для уязвимостей, SOC для мониторинга: различия и точки пересечения двух ключевых подразделений ИБ

Спикер: Кирилл Демин

... a little bit of stats

Временные рамки эксплуатации уязвимостей
остаются непредсказуемыми и могут варьироваться
на протяжении всего жизненного цикла уязвимости



Данные cvedetails.com

CVE с публичным эксплойтом $\approx 10-15\%$

CVE, использованные в атаках $\approx 1-2\%$

VOC для уязвимостей, SOC для мониторинга: различия и точки пересечения двух ключевых подразделений ИБ

Спикер: Кирилл Демин

А что со сканерами?

- Разрозненные сканирования
- Длинные отчёты сканеров, которые не обрабатываются должным образом
- Отсутствие выстроенного процесса приоритизации уязвимостей
- Долгие сроки исправления, накопление техдолга
- Отсутствие централизации
- Неполная инвентаризация
- Неполное покрытие патчами и ограниченность компенсирующих мер
- Отсутствие постконтроля за устранением уязвимостей



VOС для уязвимостей, SOC для мониторинга: различия и точки пересечения двух ключевых подразделений ИБ

Спикер: Кирилл Демин

VOС — новый уровень управления уязвимостями

Vulnerability Operations Center – это специализированная команда, набор технических решений и процессов, которые отвечают за управление уязвимостями от “А” до “Я”.

VOС занимается превентивной безопасностью, а SOC реагированием. Вместе они дополняют друг друга для создания глубоко эшелонированной защиты.



VOC для уязвимостей, SOC для мониторинга: различия и точки пересечения двух ключевых подразделений ИБ

Спикер: Кирилл Демин

Базовые задачи VOC

- Глубокая инвентаризация активов
- Мониторинг поверхности атаки
- Непрерывное сканирование уязвимостей
- Сбор, нормализация и обогащение данных об уязвимостях
- Оценка риска
- Приоритизация
- Планирование и координация remediation
- Выбор методов и средств устранения уязвимостей
- Устранение
- Валидация и цикл проверки
- Отчётность и метрики
- Наблюдение за ландшафтом угроз и внешними исследованиями



VOC для уязвимостей, SOC для мониторинга: различия и точки пересечения двух ключевых подразделений ИБ

Спикер: Кирилл Демин

VOC — заблуждения

VOC **!=** замена SOC

VOC **!=** часть SOC

VOC **!=** VM
SOC **!=** SIEM

VOC — не технология
VOC — отдельное подразделение со своей командой, тех. решениями и процессами

VOС для уязвимостей, SOC для мониторинга: различия и точки пересечения двух ключевых подразделений ИБ

Спикер: Кирилл Демин

VOС — новый уровень управления уязвимостями

Vulnerability Operations Center – это специализированная команда, набор технических решений и процессов, которые отвечают за управление уязвимостями от “А” до “Я”.

VOС занимается превентивной безопасностью, а SOC реагированием. Вместе они дополняют друг друга для создания глубоко эшелонированной защиты.



VOС для уязвимостей, SOC для мониторинга: различия и точки пересечения двух ключевых подразделений ИБ

Спикер: Кирилл Демин

VOС — новый уровень управления уязвимостями

Vulnerability Operations Center – это специализированная команда, набор технических решений и процессов, которые отвечают за управление уязвимостями от “А” до “Я”.

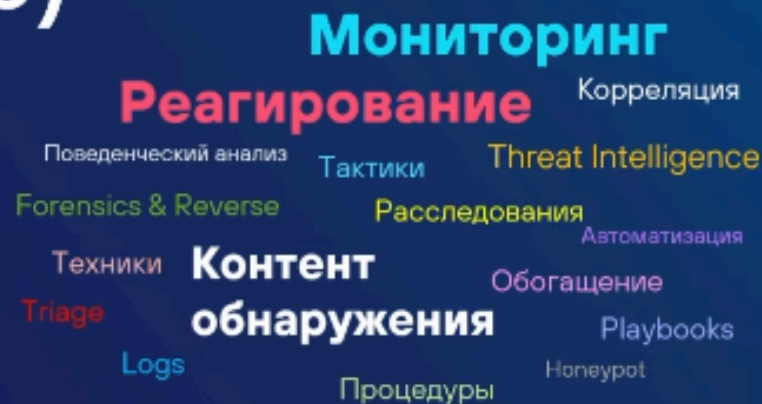
VOС занимается превентивной безопасностью, а SOC реагированием. Вместе они дополняют друг друга для создания глубоко эшелонированной защиты.



VOC для уязвимостей, SOC для мониторинга: различия и точки пересечения двух ключевых подразделений ИБ

Спикер: Кирилл Демин

SOC — единый операционный центр (всё ещё)



SOC остаётся ключевым элементом защиты, но его эффективность возрастает, когда он получает дополнительный контекст от VOC и защищаемую инфраструктуру с меньшим количеством уязвимых активов

VOC для уязвимостей, SOC для мониторинга: различия и точки пересечения двух ключевых подразделений ИБ

Спикер: Кирилл Демин

Разделение ролей

SOC

— ловит преступников, проникающих или уже проникших в дом



VOC

— проверяет дыры в заборе, занимается починкой незапертых дверей и окон, чтобы в дом не влезли



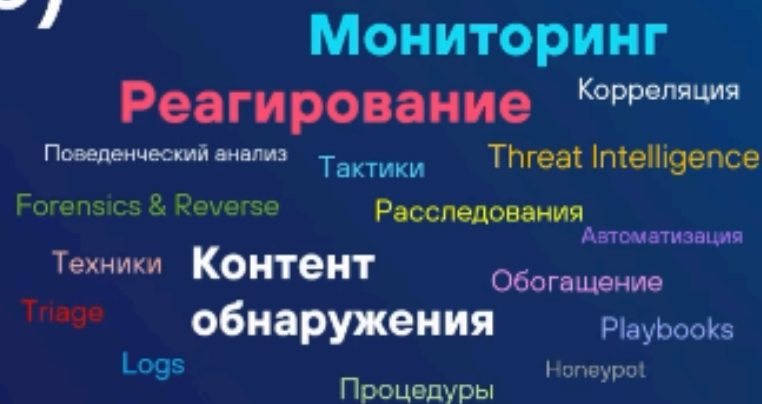
Правильно реализованный **VOC** не конкурирует с **SOC** за ресурсы, а усиливает эффективность!



VOC для уязвимостей, SOC для мониторинга: различия и точки пересечения двух ключевых подразделений ИБ

Спикер: Кирилл Демин

SOC — единый операционный центр (всё ещё)



SOC остаётся ключевым элементом защиты, но его эффективность возрастает, когда он получает дополнительный контекст от VOC и защищаемую инфраструктуру с меньшим количеством уязвимых активов

Легитимные C2: как популярные сервисы работают на хакеров

Спикер: Александр Кириченко

Telegram abuse



Victim



Adversary

- Malware connects to Telegram Bot via API
- Receives commands from C2 and executes
- Sends additional information from host

- Creates Telegram Bot
- Runs commands via Telegram Bot



Легитимные C2: как популярные сервисы работают на хакеров

Спикер: Александр Кириченко

Telegram communication

GetUpdates

GET [https://api.telegram.org/bot/\[bot-token\]/getUpdates](https://api.telegram.org/bot/[bot-token]/getUpdates)

Receives an array of updates (messages) bot receives

Webhooks

GET [https://api.telegram.org/bot/\[bot-token\]/setWebhook](https://api.telegram.org/bot/[bot-token]/setWebhook)

Sends an HTTPS POST request to the specified URL containing a JSON-serialized Update

In this case, the malware connects to the webhook to receive updates.



Легитимные C2: как популярные сервисы работают на хакеров

Спикер: Александр Кириченко

Detection

Detection Technologies:

- SIEM, EDR, Suricata, Yara

URL pattern:

- https://api.telegram.org/bot*
- Log Sources: Proxy, NGFW, Sysmon, EDR, DNS

Accessing to api.telegram.org from command-line:

- powershell.exe Invoke-RestMethod

Network Connection to api.telegram.org from non-browsers, non-Telegram Desktop App

- Log Sources: Sysmon, EDR



Telegram API Methods used by malware:

Method	Purpose
getUpdates	Check for incoming commands
sendMessage	Send information about victim, log execution, credentials
sendPhoto	Send Screenshots
sendDocument	Data exfiltration, send command execution result
getFile / getMe	Test API / check Bot
deleteMessage	Remove artifacts



Легитимные C2: как популярные сервисы работают на хакеров

Спикер: Александр Кириченко



Сегментирование и зонирование локальной сети

Спикер: Артем Чуйков

Методы проникновения во внутреннюю сеть

**3
место**

Отсутствие
сегментации
сети



Уязвимости
учетных
записей

Недостатки
конфигурации
сети

Уязвимости
в коде

Другие



Сегментирование и зонирование локальной сети

Спикер: Артем Чуйков

Единая сеть «Репкина ферма»



1. Широковещательный домен
2. Доступ всех ко всему
3. Разнотипный трафик



Источник угрозы



Мы же умные! У нас такого не бывает!

1. Ошибки проектирования и конфигурирования.
2. Инертность мышления.
3. Несогласованность действий различных команд.
4. Экономические причины.
5. Отсутствие или преднамеренное игнорирование регламентов.



Сегментирование и зонирование локальной сети

Спикер: Артем Чуйков



Сегментирование и зонирование локальной сети

Спикер: Артем Чуйков



Сегментирование и зонирование локальной сети

Спикер: Артем Чуйков

Защищаемся от посторонних

phd X pt

Моя сеть – мои правила. Некоторые технологии безопасности.

- DHCP Snooping – Владелец у DHCP должен быть только один
- IP source guard – Сверяем выданные IP
- ARP inspection – Защищаемся от ARP-спуфинга
- Port Security – Подключаем только то, что знаем
- IEEE 802.1X – Авторизируемся при подключении



Сегментирование и зонирование локальной сети

Спикер: Артем Чуйков

Защищаемся от посторонних

phd X pt

Моя сеть – мои правила. Некоторые технологии безопасности.

- DHCP Snooping – Владелец у DHCP должен быть только один
- IP source guard – Сверяем выданные IP
- ARP inspection – Защищаемся от ARP-спуфинга
- Port Security – Подключаем только то, что знаем
- IEEE 802.1X – Авторизируемся при подключении



Сегментирование и зонирование локальной сети

Спикер: Артем Чуйков

Строим свою сеть



Разрешаем нужное. Запрещаем ненужное



Сегментирование и зонирование локальной сети

Спикер: Артем Чуйков

Строим свою сеть



Разрешаем нужное. Запрещаем ненужное

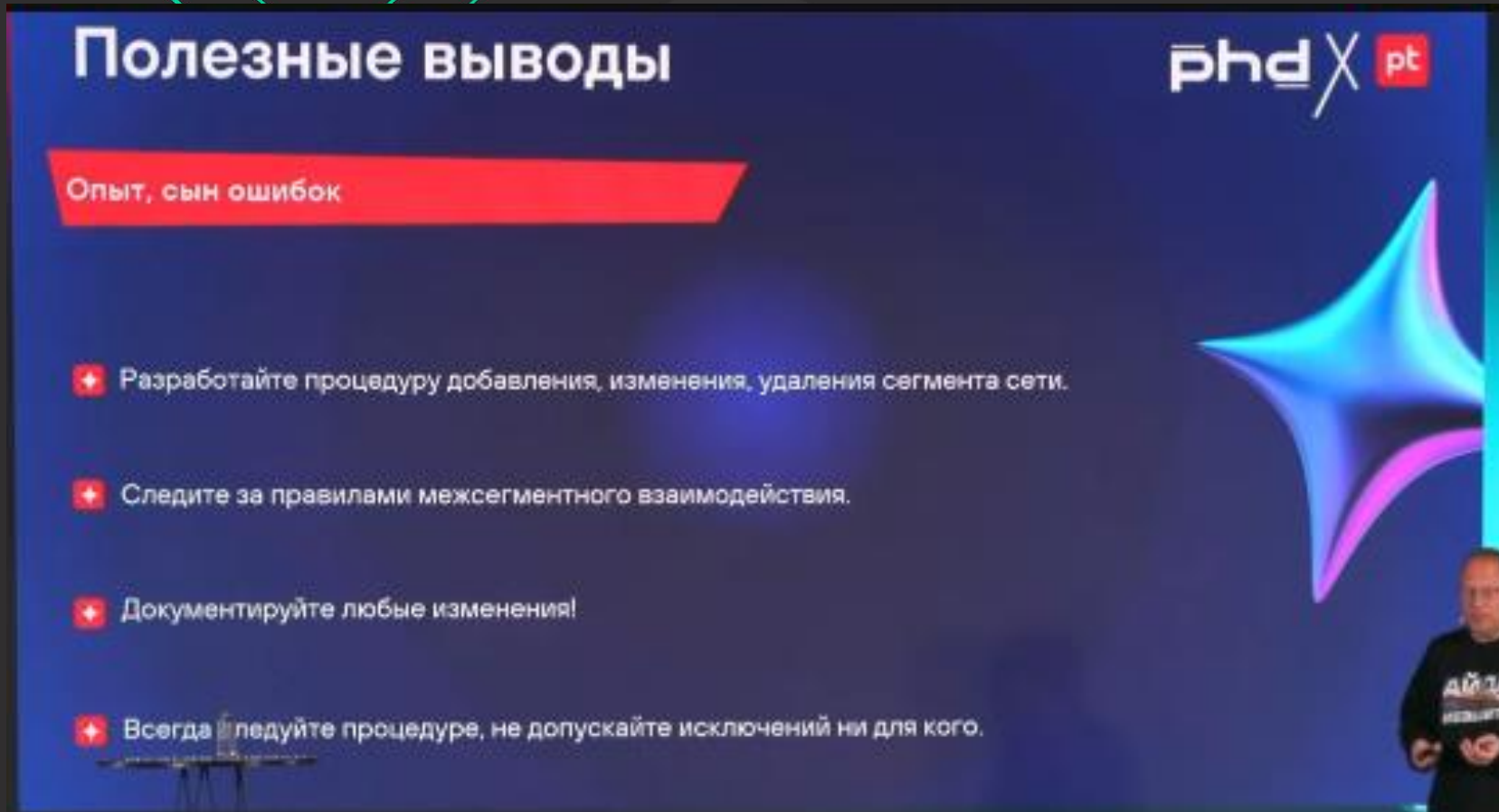


Внутренняя сеть предприятия



Сегментирование и зонирование локальной сети

Спикер: Артем Чуйков



Полезные выводы

Опыт, сын ошибок

- + Разработайте процедуру добавления, изменения, удаления сегмента сети.
- + Следите за правилами межсегментного взаимодействия.
- + Документируйте любые изменения!
- + Всегда следуйте процедуре, не допускайте исключений ни для кого.



Standoff 15





Спасибо за внимание



30.05.2025

