360° Ampire

КОНФЕРЕНЦИЯ КИБЕРПОЛИГОНОВ

Вместе против цифровой уязвимости

24 апреля

г.Москва, Кибердом

360° Ampire

Зачем ИБшнику Red Team и как исследовательские навыки влияют на усиление защиты

Василий Кравец,

Начальник отдела ИИТ,
АО «ПМ»

Ampire 360°

Отдел ИИТ

О моей команде

Обо мне

- CVE-2019-14743
- CVE-2019-15316
- CVE-2019-17180
- CVE-2019-19247
- CVE-2019-19248
- CVE-2019-20383
- CVE-2020-23967
- CVE-2021-25261
- CVE-2021-25263
- CVE-2022-28226
- CVE-2022-28225
- CVE-2023-5993
- CVE-2023-7016

О команде

6 сертификатов OSCP

3 сертификата OSWE

1 сертификат OSEP

1 сертификат OSWP

Более **45** лет опыта в ИБ

Более **200** завершенных проектов

Время атаки

Типовое время захвата домена

На основании опыта команды за 2024-2025 год:

При проведении работ «черным ящиком»: **10 часов**

При проведении работ «серым ящиком»: **2 часа**

Ampire RedTeam

Роль занятий RedTeam в обеспечении безопасности:

- Узнать типовые сценарии атак
- В «ручном режиме» провести атаки
- Понять, как выглядит «чужая» сеть с точки зрения атакующего
- Оценить возможности использования легитимных сервисов для атак
- Успеть все это за 2 часа

Ampire 360°

Философия

Что такое безопасность?

Безопасность – это…

360° Ampire

… не состояние, а процесс

Нельзя «зафиксировать» безопасность, она постоянно меняется, так как меняется и состояние оцениваемой системы внутри и снаружи.

У безопасности как у процесса есть жизненный цикл.

Внутренний период

Начальные этапы:

Давайте сделаем побезопаснее

Внутренний период

360° Ampire

Начальные этапы:

Давайте сделаем побезопаснее

Изучаем Best Practice

Внутренний период

360° Ampire

Начальные этапы:

Давайте сделаем побезопаснее

Изучаем Best Practice

Проводим аудит

Внешний период

Существенные мероприятия:

Исследование возможностей

Внешний период

Существенные мероприятия:

Исследование возможностей

Анализ защищенности

Внешний период

Существенные мероприятия:

Исследование возможностей

Анализ защищенности

Точечные исследования

Внешний период

360° Ampire

Существенные мероприятия:

Исследование возможностей

Анализ защищенности

Точечные исследования

Пентест

Пост-защита

Что еще можно сделать:

RedTeaming

Учения Blue Team

Purple Teaming

Bug Bounty

Чем поможет Ampire?

360° Ampire

Начальные этапы:

Давайте сделаем побезопаснее _Ampire Junior

Изучаем Best Practice _Ampire Junior

Проводим аудит

Чем поможет Ampire?

Существенные мероприятия:

Исследование возможностей	_Ampire Red Team
Анализ защищенности	_Ampire Red Team
Точечные исследования	_Ampire Red Team
Пентест	_Ampire Red Team

Чем поможет Ampire?

Что еще можно сделать:

RedTeaming	_Ampire Red Team
Учения Blue Team	_Ampire Blue Team / CSIRT
Purple Teaming	
Bug Bounty	

360° Ampire

Благодарю за внимание!