

## ПРОГРАММА OFFZONE 2023

Полная программа выступлений

[ОТКРЫТЬ КАРТУ](#)

### 24 АВГУСТА

10:00

#### Открытие

[основной трек](#)

10:45–11:00 | 24 августа

[Track 1](#) [Русский](#) [English](#)

11:00

#### Взломать По-старому Нельзя Взломать По-новому

[основной трек](#)

[Омар Ганиев](#)

Основатель, DeteAct

Кибербезопасность — производная от технологий. Новые технологии создают новые угрозы и новые векторы атак.

Этот итеративный прогресс часто происходит незаметно от нас. Оглянувшись, мы можем увидеть, что в ландшафте кибербезопасности неизменно изменилось за 10 лет, а что поразительным образом осталось неизменным.

Глядя на это, задаешься вопросами: чего нового ждать в следующие 10 лет и стоит ли к этому готовиться?

11:00–12:00 | 24 августа

[Track 1](#) [Русский](#) [English](#)

12:00

#### Выкиньте вашу SKUD! Пентест Wiegand и TM

[dumbmode](#)

Частный консультант по ИБ

Даже если у вас современная SKUD, она может иметь уязвимости, унаследованные от предыдущих поколений. Начнем с 1980 года

11:30–12:30 | 24 августа

[Community track](#) [Русский](#)

12:00

#### SPRUSH: чему нас научили 4 года участия в CTF

[Павел Блинников](#)

Специалист по компьютерной криминалистике, BI.ZONE

Слушателей доклада ждет выжимка из опыта капитана сильной российской CTF-команды

12:00–12:20 | 24 августа

[CTF.Zone](#) [Русский](#)

#### Открытие AntiFraud.Zone

##### Кейс-стади

[Андрей Ильинский](#)

Начальник отдела экспертизы по противодействию мошенничеству, BI.ZONE

12:00–12:30 | 24 августа

[AntiFraud.Zone](#) [Русский](#)

#### Деобфускация и анализ клиентского JavaScript-кода для обнаружения DOM-based XSS

[основной трек](#)

[Андрей Козлов](#)

Специалист по анализу защищенности, «Лаборатория Касперского»

Основная цель доклада — описание нового, разработанного докладчиком, автоматизированного метода анализа JavaScript-кода, использующего статический и динамический анализ, а также сравнение результатов его работы с существующими автоматизированными сканерами веб-уязвимостей

12:00–13:00 | 24 августа

[Track 1](#) [Русский](#) [English](#)

#### AppSec на OSS — придется програть (на основе реального опыта «Дзен»)

[Андрей Борисов](#)

Руководитель направления в отделе информационной безопасности «Дзен», VK

Что сделали в «Дзен» на open source, с какими столкнулись проблемами, сколько всего пришлось исправлять и дописывать и к чему в итоге пришли.

Поговорим об основных инструментах и бенефитах на примере самой большой контентной платформы России

12:00–13:00 | 24 августа

[AppSec.Zone](#) [Русский](#)

#### Основные тренды кибермошенничества в финансовой сфере и методы противодействия

[Юрий Лысенко](#)

Заместитель директора Департамента информационной безопасности, Банк России

Предупрежден, значит вооружен. Для хищения денег у граждан злоумышленники используют все более изощренные сценарии. В результате тысячи людей страдают от их действий, теряют деньги, которые в некоторых случаях копили годами. Знания о том, как противодействовать мошенникам, помогут в нужную минуту принять правильное решение.

Представитель Банка России расскажет о распространенных мошеннических схемах, а также мерах, принимаемых регулятором в целях противодействия хищению денежных средств

12:30–13:00 | 24 августа

[AntiFraud.Zone](#) [Русский](#)

#### Параноидальный ноутбук

[GreenHamster](#)

Все знают, что такое полнодисковое шифрование, но мало кто это использует. А если и задумывается, то, как правило, откладывает на потом, так как не хочется переустанавливать систему и терять родные настройки.

Цель доклада — напомнить, что можно многое ничего и не теряя, и показать на примере, как можно усилить защиту своего устройства, приложив немного усилий

12:30–13:00 | 24 августа

[Community track](#) [Русский](#)

#### Корреляционный анализ поточных систем

[Андрей Сергеев](#)

Старший специалист сертификационной лаборатории, ООО «СФБ Лаборатория»

В CTF-соревнованиях (Capture the Flag) есть задачи на знание криптографии. Для того чтобы их решать, нужно иметь некоторую теоретическую базу. В докладе Андрей постарается разобраться с основами корреляционного анализа, применяемого к поточным системам.

Поточные алгоритмы предоставляют интерес для криптографического сообщества. Например, в подложной телефонной связи в разное время использовались различные алгоритмы семейства A5 (2G), SNOW (3G), ZUC (5G). Также в 2015 году американский институт стандартов и технологий (NIST) организовал конкурс легковесных алгоритмов (lightweight cryptography), которые могут использоваться в маломощных устройствах (например, IoT). Одним из финалистов конкурса стал алгоритм Grain-128AEAD. Такой интерес к поточным системам обусловлен их высокими скоростными характеристиками и простотой программной/аппаратной реализации.

Анализ поточных систем требует рассмотрения специальных методов анализа. В открытой литературе был предложен ряд методов, основанных на наблюдении зависимости (корреляции) между знаками зашифрованного текста и внутреннего состояния алгоритма. Андрей рассмотрит хорошо известные методы корреляционного анализа: Зигенталера (T. Siegenthaler) и «быстрый» метод Майера — Штафельбаха (W. Meier and O. Staffelbach)

12:30–13:10 | 24 августа

[CTF.Zone](#) [Русский](#)

13:00

#### Антифрод. Новые сервисы в ПС «Мир»

[Алексей Ипатов](#)

Руководитель центра противодействия мошенничеству, НСПК

Алексей представит информацию о разворачиваемых в платежной системе сервисах, направленных на выявление и пресечение мошеннической активности

13:00–13:30 | 24 августа

[AntiFraud.Zone](#) [Русский](#)

#### NetRunner 2023: гаджеты хакера из будущего, которые можно достать уже сегодня

[Scan87](#)

Пентестер

Да, киберпанк еще не наступил, но, если уж очень хочется окунуться в футуристическую антиутопию? В своем докладе Scan87 предложит подборку из необычных девайсов и гаджетов, которые если не облегчат жизнь, то уж точно заставят почувствовать себя круто! А еще вызовут множество вопросов у коллег...

13:00–13:30 | 24 августа

[Community track](#) [Русский](#)

#### 5 лайфхаков для Mobile DevSecOps

[Юрий Шабалин](#)

Генеральный директор, «Стингрей Технолоджиз»

Все знают, как устроен стандартный процесс разработки web-приложений, как наилучшим способом встраивать в него инструменты безопасности. Но мало кто задумывается о том, что разработка мобильных приложений имеет свои нюансы и особенности, зная которые можно существенно улучшить эффективность проверок на безопасность.

В рамках доклада поговорим про эти особенности и про то, как их использовать, как получить наиболее эффективный результат от инструментов, где и какие проверки можно использовать, на каких этапах они дают наилучший результат

13:00–13:30 | 24 августа

[AppSec.Zone](#) [Русский](#)

#### Эксплуатация уязвимостей HTTP Request Splitting

[основной трек](#)

[Сергей Бобров](#)

Старший специалист по анализу защищенности, «Лаборатория Касперского»

В своем докладе Сергей расскажет об уязвимостях HTTP Request Splitting / CRLF Injection в проксировании HTTP-запросов пользователя между веб-серверами. Будут освещены методы обнаружения подобных уязвимостей при автоматическом сканировании и варианты их эксплуатации на примере популярной багбаунти-программ

13:00–14:00 | 24 августа

[Track 1](#) [Русский](#) [English](#)

#### Пресс-конференция

##### BI.ZONE Bug Bounty: итоги года

[Евгений Волошин](#)

Директор по стратегии, BI.ZONE

[Дмитрий Гадарь](#)

Вице-президент, директор департамента информационной безопасности, «Тинькофф»

[Андрей Левкин](#)

Руководитель продукта BI.ZONE Bug Bounty, BI.ZONE

[Рамазан Рамазанов \(r0hack\)](#)

Багхантер, руководитель отдела внешних пентестов DeteAct

Компании усиливают эффективность в обнаружении кибербезопасности и объединяя усилия штатных специалистов по кибербезопасности и багхантеров. Востребованность российских багбаунти-платформ растет, особенно на фоне ухода международных площадок с рынка.

На пресс-конференции подведем итоги года — расскажем, как за это время изменился рынок багбаунти и как изменились мы

13:00–14:30 | 24 августа

[Press.Zone](#) [Русский](#)

#### Противодействие мошенничеству в 2023 году: опыт и практика «Альфа-Банка»

[Евгений Винокуров](#)

Руководитель дирекции противодействия кибермошенничеству, «Альфа-Банк»

В своем докладе Евгений остановится на следующих пунктах:

- Социальная инженерия с участием кредитных средств.
- Проблемы решения.
- Проблемы инфообмена и чего не хватает в этой части

13:30–14:00 | 24 августа

[AntiFraud.Zone](#) [Русский](#)

#### Бумажная безопасность для атакующего

[Николай Уманец](#)

Директор по безопасности, «Ростелеком Контакт-Центр»

Зачем хакеру/пентестеру нужно знать стандарты ИБ. Как благодаря этим данным построить правильный вектор атаки

13:30–14:00 | 24 августа

[Community track](#) [Русский](#)

#### Фиолетовый — цвет боли!

[Максим Ильин](#)

Руководитель SOC и развития продукта сканирования уязвимостей, SolidLab

[Игорь Ландырев](#)

Специалист по анализу защищенности, Awillix

Спикеры расскажут о командной работе над инцидентами, частых проблемах в кейсах взаимодействия, покажут кусочек хорошего кейса с обходом дефендера и поделятся опытом масштабирования знаний, полученных в ходе тестирования. Предложат концепцию для развития команд. Вам понравится!

13:30–14:00 | 24 августа

[AppSec.Zone](#) [Русский](#)

#### Эксплуатация режима отладки в Chromium, Node и WebDriver

[Денис Погонин](#)

Старший специалист отдела анализа защищенности, BI.ZONE

В докладе Денис расскажет о получении RCE при отладке приложения на Node и использовании WebDriver (ChromeDriver, GeckoDriver), рассмотрит протокол DevTools для доступа к файлам и исполнению JS-кода и его применение для решения заданий CTF. Кроме того, продемонстрирует возможности постэксплуатации систем через режим отладки в браузерах

13:30–14:10 | 24 августа

[CTF.Zone](#) [Русский](#)

14:00

#### Построение UBA на данных CRM, DLP и пользовательской активности

[Сергей Серов](#)

Руководитель группы разработки антифрод-моделей, «Тинькофф»

Доклад посвящен поиску аномального поведения пользователей в системах банка и применению ML в этом направлении. Сергей расскажет о том, как на основе данных из множества источников построена модель выявления необоснованных действий сотрудников.

Особое внимание уделяется системе DLP, которая предотвращает события с хостов и сработкой рисковыми правил. С помощью обогащения этих данных другими факторами проводятся ранжирование и оценка критичности событий

14:00–14:30 | 24 августа

[AntiFraud.Zone](#) [Русский](#)

#### Нет прошивки — есть ачивки. 15 уязвимостей и другие находки в ПЛК Mitsubishi FX5U

[основной трек](#)

[Антон Дорфман](#)

Ведущий специалист отдела анализа приложений, Positive Technologies

Алгоритм исследования недокументированного протокола: получить прошивку устройства, в цикле перевернуть прошивку и пострелять пакетами в устройство, восстановить протокол, найти уязвимости. Что делать, если прошивку невозможно получить? Кажется бы, остается только black box — анализ и что-то еще. Об этом «что-то еще» и пойдет речь в докладе.

Антон покажет способы получения информации для восстановления протокола, опишет результаты исследования: строение протокола, скрипты для работы с ним, 15 найденных CVE — и приправит все это демонстрациями работы PoC для некоторых багов

14:00–15:00 | 24 августа

[Track 1](#) [Русский](#) [English](#)

#### Почему не всем связям можно доверять?

[Евгений Уткин](#)

Руководитель отдела разработки транзакционных решений по противодействию мошенничеству, BI.ZONE

Евгений расскажет, как можно повысить доверие к связям между объектами расчета для борьбы с социальной инженерией и другими сценариями захвата контроля. Узнаем, какой функциональности должно обладать онлайн-обогащение для борьбы с такими сценариями мошенничества

14:30–15:00 | 24 августа

[AntiFraud.Zone](#) [Русский](#)

#### Повышаем безопасность GitLab CE

[Савелий Красовский](#)

Инженер безопасности, разработчик, X5 Tech

Многие компании используют GitLab для организации разработки, однако в Community Edition, которым пользуется большинство компаний, недопустимо значительное количество улучшений безопасности.

В последние полтора года Савелий решил углубиться в некоторые вопросы, привнеси в том или ином виде некоторые премиум-функции в CE, а в некоторых случаях доработать уже существующие фичи

14:30–15:00 | 24 августа

[AppSec.Zone](#) [Русский](#)



## C O до 1. O подготовков новичков в мире CTF-соревнований

**Георгий Зайцев**

Ака @ggreg0r0, в прошлом наставник и методист олимпиадного отделения по CTF Московской школы программистов (МШП)

Доклад про организацию курса по CTF для совсем новых (тех, кто еще ни одного таска в жизни не решил)

**14:30–15:10 | 24 августа**

📍 CTF.Zone 🌐 Русский

**15:00**

### Как устроен мошеннический кол-центр?

**Александр Большунов**

Ведущий эксперт департамента кибербезопасности, ПАО Сбербанк

**15:00–15:30 | 24 августа**

📍 AntiFraud.Zone 🌐 Русский

### Взлом DeFi-протокола Conic Finance. Как крадут миллионы долларов не выходя из дома

**angkasawan**

OSINT-аналитик, энтузиаст безопасности Web 3.0 и независимый специалист по компьютерной криминалистике

В докладе разберем основные принципы работы протокола Conic Finance, какие уязвимости в коде допустили разработчики и как они были проэксплуатированы

**15:00–15:30 | 24 августа**

📍 Community track 🌐 Русский

### Самое слабое звено: разбираемся в атаках на цепочки поставок

**Олег Скулкин**

Руководитель управления киберразведки, BI.ZONE

В последние годы атаки на цепочки поставок перестали быть прерогативой спонсируемых государствами групп. Управление киберразведки BI.ZONE известно как минимум несколько случаев, когда финансово мотивированные хакеры, например операторы программ-вымогателей, использовали данный метод для получения первоначального доступа к своим целям.

В ходе доклада Олег расскажет, что представляют собой подобные атаки, и на реальном примере разберет, на каких этапах жизненного цикла можно их обнаружить и предотвратить возможный ущерб

**15:00–16:00 | 24 августа**

📍 Track1 🌐 Русский 🗣 English

### ББусидо — путь багхантера

**Алексей Лямкин**

Эксперт, VK

**Пётр Уваров**

Эксперт, VK

- Багбаунти — важный элемент в системе многоуровневой защиты сервисов VK.
- Как в VK происходит валидация и оценка уязвимости.
- Ветки развития в багбаунти.
- Путь багхантера: как VK видит рост багхантера и критичность найденных уязвимостей.
- Кейсы и примеры самостоятельного докручивания присланных багов до высокого импакта.
- Как происходит раскрытие отчетов на площадках.
- Топ интересных багов, найденных на российских площадках

**15:00–16:00 | 24 августа**

📍 AppSec.Zone 🌐 Русский

### COM Objects: Ancient Knowledge

**Владислав Бурцев**

Аналитик threat intelligence, «Лаборатория Касперского»

Ты знаешь, как работает технология COM, и изучишь основные подходы к исследованию Windows. Воркшоп включает практические задания: написать свой COM-объект, AMSI Provider и клиент для взаимодействия с системными COM-серверами

**15:00–17:00 | 24 августа**

📍 Воркшопы 🌐 Русский

### Атака CRC Forge: принцип работы и возможные риски

**Кирилл Комогоров**

Специалист по тестированию на проникновение, BI.ZONE

Слушатели доклада смогут познакомиться с принципом работы помехоустойчивого кода CRC-64 и узнать область его применения. Также будет рассмотрена коллизионная атака на данный код, включая ее математические основы. В заключительной части доклада Кирилл представит зрителям собственный скрипт автоматизации атаки, кратко продемонстрирует работу коллизионной атаки, а также поговорит о возможных методах ее предотвращения

**15:30–15:50 | 24 августа**

📍 CTF.Zone 🌐 Русский

### Фантомная загрузка DLL

**Евгений Васильев aka @Not\_C\_Developer**

Пентестер, OSEP

Техника обхода антивируса, которая включает в себя загрузку легитимной DLL, инжект вредоносного кода, а затем исполнение

**15:30–16:00 | 24 августа**

📍 Community track 🌐 Русский

**16:00**

### Buy Now. Pay Later?

**Дмитрий Русаков**

Антифрод-аналитик, «Яндекс»

Доклад посвящен практическим вопросам противодействия мошенничеству в онлайн-сервисах рассрочки (BNPL), с которыми пришлось столкнуться на собственном опыте выстраивания защиты BNPL-сервиса от фрода

**16:00–16:30 | 24 августа**

📍 AntiFraud.Zone 🌐 Русский

### Текущий state развития CTF-движения и информационной безопасности для российских школьников

**Даниил Иванькин (@dDanissimo)**

Независимый исследователь

Небольшое полевое исследование в форме ретроспективы о CTF-движении в России для школьников и его дальнейших перспективах

**16:00–16:30 | 24 августа**

📍 Community track 🌐 Русский

### История появления CTF-площадки Codeby

**Алексей Морозов**

Руководитель отдела AppSec (Defensive), «Тинькофф»

Алексей расскажет, как пройти путь от CTF-команды до организации CTF как сервиса: построить с нуля свою площадку и превратить это в сервис. Мемы по теме прилагаются

**16:00–16:40 | 24 августа**

📍 CTF.Zone 🌐 Русский

### Логические уязвимости повышения привилегий в ОС Windows

**основной трек**

**Василий Кравец**

Начальник отдела исследований информационных технологий, «Перспективный мониторинг»

В докладе будет рассказано о логических уязвимостях в ПО для ОС Windows. Будут рассмотрены основные методы и техники их эксплуатации, разобраны кейсы и даны советы, как избежать таких уязвимостей в разработке. Также спикер поделится опытом взаимодействия с вендорами, в чьих продуктах были обнаружены уязвимости

**16:00–17:00 | 24 августа**

📍 Track1 🌐 Русский 🗣 English

### Бизнес-партнеры по ИБ: ожидания vs реальность

**Георгий Руденко**

Начальник отдела менеджмента процессов ИБ, «Райффайзен Банк»

**Алексей Гуськов**

Бизнес-партнер по информационной безопасности, «Райффайзен Банк»

Спикеры расскажут про свой опыт внедрения Information Security Business Partners:

- предпосылки появления и ожидания от роли;
- фреймворк работы IS BP (полный жизненный цикл работы);
- основные подводные камни при внедрении IS BP;
- примеры и вызовы в работе BP;
- дальнейшие планы по развитию

**16:00–17:00 | 24 августа**

📍 AppSec.Zone 🌐 Русский

### Уменьшаем поверхность атаки в GitLab CI

**n0nvme**

Независимый исследователь

Рассмотрим, как можно обойтись без доступа к Docker-сокету при сборке образов контейнеров

**16:30–16:45 | 24 августа**

📍 Community track 🌐 Русский

### Эволюция антифрода

**Николай Дощ**

Директор по развитию продуктов и сервисов, «Фаззи Лоджик Лабс»

За последнее несколько лет в платежной инфраструктуре произошел существенный сдвиг с точки зрения векторов и технологий мошеннических атак. В частности, банковских клиентов активно атакуют с помощью так называемой социальной инженерии, а этот вид мошенничества занял лидирующие позиции в мире. Но так было не всегда.

Доклад будет посвящен эволюции мошеннических схем и технологий противодействия им с использованием международных статистических данных, актуальной информации об атаках на устройства самообслуживания и мошеннических схемах, использующих методы социальной инженерии. Николай приведет примеры инцидентов, которые происходили в РФ и некоторых странах Европы

**16:30–17:00 | 24 августа**

📍 AntiFraud.Zone 🌐 Русский

### Как реклама следит за тобой?

**Андрей Косоруков (dot)**

Независимый исследователь

В своем докладе Андрей расскажет о прошлом, настоящем и будущем таргетинга интернет-рекламы и не только

**16:45–17:00 | 24 августа**

📍 Community track 🌐 Русский

**17:00**

### Гайдлайн «Как сгореть, но не подать вида»

**Инженер kringxovich**

Независимый страдалец [не] в ИБ

Набор случаев по обычным мирно-инженерно-тракторным задачам, в которые случайно влез инфобез и создал ДРАМУ (обычно весьма странную, и чаще даже не создал, а усерил). В общем, окolorабочие байки, чтобы погреть уши и посмеяться :)

**17:00–17:15 | 24 августа**

📍 Community track 🌐 Русский

### Необычные атаки с применением широко распространенных программ для удаленного управления

**Алина Суханова**

Независимый исследователь

Приходила ли тебе когда-нибудь мысль, что твоими утилитами для удаленного доступа может воспользоваться кто-то еще? Поговорим об атаках на малый и средний бизнес и о возможности их осуществления в результате неграмотного использования широко известной утилиты для удаленного доступа

**17:00–17:30 | 24 августа**

📍 AntiFraud.Zone 🌐 Русский

### УАТВ: как сделать быструю и легкую чек-систему

**Дмитрий Зотов**

Капитан CTF-команды kks

Дмитрий расскажет о том, как делали еще одну чек-систему для CTF, для чего она нужна, какие проблемы встретили и как будут развивать ее в будущем

**17:00–17:40 | 24 августа**

📍 CTF.Zone 🌐 Русский

### Современная автоматизация обратной разработки в декомпиляторе HexRays

**основной трек**

**Семён Соколов**

Специалист, Positive Technologies

В своем докладе Семён кратко расскажет про существующие инструменты автоматизации обратной разработки, а также представит новые

**17:00–18:00 | 24 августа**

📍 Track1 🌐 Русский 🗣 English

### Безопасный OSS — работать и терпеть!

**Константин Крючков**

Эксперт по безопасности open source, Swordfish Security

Разработка с использованием сторонних компонентов — это то, что спасет ваш time-to-market, но только до тех пор, пока не начать заниматься безопасностью и лицензионной чистотой.

Доклад о том, почему поиск уязвимостей в компонентах с открытым исходным кодом — это боль и страдание и как сделать его удобнее для команд разработки и безопасности. Обзор актуальных проблем, подходов, классификаций, баз уязвимостей и методов защиты при работе с OSS

**17:00–18:00 | 24 августа**

📍 AppSec.Zone 🌐 Русский

### Символьное исполнение смарт-контрактов в блокчейне TON

**@hacker\_volodya**

Независимый исследователь

В своем докладе @hacker\_volodya расскажет о том, как разрабатывает символьное исполнение для контрактов в TON на базе SMT-решателя Z3, какие подводные камни были и в чем отличия от аналогичных фреймворков для EVM-блокчейнов.

Покажет, как оно работает на конкретных контрактах, как с помощью собственного фреймворка находить в них косяки и доказывать заданные свойства

**17:15–17:30 | 24 августа**

📍 Community track 🌐 Русский

### Обратный взгляд на реверс-инжиниринг

**Борис Рютин**

Исследователь безопасности

Обратная разработка — это изучение кода объекта исследования с целью понять, как он работает. Реверс-инжиниринг может использоваться не только для анализа безопасности, но и для улучшения производительности и создания новой функциональности. В рамках доклада Борис предложит вместе обсудить, так ли это

**17:30–17:45 | 24 августа**

📍 Community track 🌐 Русский

### Между скамером и мулом

**Дмитрий Дудков**

Прессейл-менеджер продукта по противодействию мошенничеству, F.A.C.C.T.

В чем преуспели киберпреступники, почему стоит обратить пристальное внимание на мулов и как с этим всем бороться

**17:30–18:00 | 24 августа**

📍 AntiFraud.Zone 🌐 Русский

### Рутина сработок: поможет машинное обучение?

**Артём Менисов**

Специалист в области применения технологий искусственного интеллекта для решения задач по обеспечению информационной безопасности

Займемся настройкой чувствительности средств защиты информации, а также поговорим о важности оперативного реагирования на компьютерные инциденты и о том, как его обеспечить. Ты познакомишься с кейсами, в том числе робастными решениями

**17:30–19:30 | 24 августа**

📍 Воркшопы 🌐 Русский

### Voltage glitching для самых маленьких

**Егор Коледа (@radioegor146)**

Независимый исследователь ИБ

Рассказ о том, как это едят и как спикер этого наелся

**17:45–18:00 | 24 августа**

📍 Community track 🌐 Русский

**18:00**

### Реверс Python C

**Павел Ближников**

Специалист по компьютерной криминалистике, BI.ZONE

Доклад об анализе одного странного исполняемого файла в ходе расследования инцидента

**18:00–18:15 | 24 августа**

📍 Community track 🌐 Русский

### Подосинтовики

**Александр Гончаров**

Специалист по тестированию на проникновение, Innostage

Речь пойдет об OSINT в CTF. Александр пройдет по основным инструментам, которые чаще всего применяются в тасках, а также разберет большое количество реальных примеров

**18:00–18:40 | 24 августа**

📍 CTF.Zone 🌐 Русский



## MikroTik Nightmare

основной трек

Caster

Эксперт по сетевой безопасности

Авторское исследование о безопасности оборудования Mikrotik в жанре offensive. Будут рассмотрены недостатки безопасности RouterOS, техники pivotинга, эксплуатационные, MitM-атак, угона трафика, а также специальный ремикс на работу s0137, в рамках которого Caster нашел новый способ L2-тунелирования против машин на Windows с использованием маршрутизатора Mikrotik

18:00–19:00 | 24 августа

Track 1 Русский English

## 25 АВГУСТА

10:00

### Ломаем CI/CD

Павел Сорокин

Ведущий инженер по ИБ, Ozon

Посмотрим на особенности безопасности компонентов CI/CD и пайплайнов, в целом большая часть остается за рамками классических пентестов

10:00–12:00 | 25 августа

Воркшопы Русский

### LockPick: как это сделано?

ostara

Независимый исследователь ИБ

Зафод Библброкс

Независимый исследователь ИБ

Как и всегда, ostara и Зафод Библброкс расскажут и наглядно покажут, что нужно было сделать, чтобы открыть замок. Разбор стендовых квестов, немного процесса подготовки и долгие гифки!

10:30–11:00 | 25 августа

Community track Русский

11:00

### Опять забыл комбинацию? Как работают кодовые замки

Scan87

Пентестер

Им доверяют всё: от вещей в чемодане до велосипедов, от дворовых калиток до сейфов. Но так ли оправданно это доверие? В докладе мы поговорим про устройство комбинационных замков, изучим принцип работы и, конечно же, обсудим уязвимости! А в конце мы попробуем ответить на вопрос: «Возможно ли подобрать код к сейфу, как это делают шпионы в фильмах?»

11:00–11:30 | 25 августа

Community track Русский

### Уязвимости в коде, генерируемом нейросетями

Максим Карасев

Системный программист на С

Нейросети, которые становятся повседневным инструментом все большего числа программистов, далеко не совершенны.

Разберемся, почему они допускают ошибки в коде, и как минимизировать риски

11:00–11:30 | 25 августа

Track 2 Русский

### Как пофаззить тысячи приложений: практическое руководство

основной трек

Роман Лебедь

Архитектор кибербезопасности, «Тинькофф»

Документ ориентирован на слушателей, которые знакомы с технологией фаззинга и желают интегрировать ее в собственный SDL.

Роман поделится личным опытом фаззинга корпоративных приложений как со стороны offensive (red team), так и со стороны defensive (AppSec, DevSecOps). Несмотря на единую технологию, инструменты и цель (выявление уязвимостей), для достижения успеха требуются абсолютно разные подходы с каждой стороны — вопреки наличию тысяч запущенных фаззеров, мы все еще наблюдаем уязвимости в самых популярных браузерах.

Будут рассмотрены проблемы существующих подходов и инструментов, сложности их применения для фаззинга тысяч корпоративных микросервисов. Вы узнаете, как применять формальный подход к разработке позволяет предложить гибкий и масштабируемый сервис фаззинга приложений, передать узкую экспертизу в код и делегировать внедрение фаззинг-тестов в команду разработки продукта.

Также Роман покажет, как можно приоритизировать цели для фаззинга на основе автоматизированного анализа поверхности атаки и data-driven-подходов. Бонусом покажет пару примеров обнаружения уязвимостей в коде на memory-safe-языках

11:00–12:00 | 25 августа

Track 1 Русский English

### Багхантинг: кейсы, инструменты и рекомендации

Рамазан Рамазанов (r0nhack)

Багхантер, руководитель отдела внешних пентестов DeteAct

- Почему не получается находить уязвимости на багбаунти?
- Способы багхантинга и кейсы для каждого способа.
- Российский багбаунти: что вообще происходит?

11:00–12:00 | 25 августа

AppSec.Zone Русский

### Символьный SAST из опенсорсных компонентов

Андрей Погребной

Младший специалист, CyberOK

Существует достаточно много открытых SAST-решений, но, как правило, они ограничиваются одной технической анализом, например pattern matching по коду или AST. Более сложные техники, такие как символьное исполнение, в основном встречаются в коммерческих решениях.

В рамках доклада Андрей продемонстрирует, как собрать конвейер SAST, реализующий актуальные техники анализа, из открытых компонентов, приведет результаты тестирования на реальных приложениях

11:30–12:00 | 25 августа

Track 2 Русский

### Разбор задач первого дня на стенде

n0vme

Независимый исследователь

Разберем задачи квеста первого дня и как их можно было решить

11:30–12:30 | 25 августа

Community track Русский

12:00

### CTF как швейцарский нож специалиста

Дмитрий Пинин

Заместитель руководителя лаборатории инновационных технологий и кибербезопасности, AP Security

В этом докладе рассматривается CTF как многосторонний инструмент становления будущего специалиста по информационной безопасности.

Дмитрий расскажет, как силами студентов развивается движение, несмотря на разные трудности, что еще скрывает в себе пункт «играл в CTF», а также на примере покажет способ поиска проблем у начинающих игроков

12:00–12:20 | 25 августа

CTF.Zone Русский

### Когда компьютеры были большими: z/OS penetration testing workflow

Денис Степанов

Старший специалист по тестированию на проникновение, «Лаборатория Касперского»

Александр Коротин

Старший специалист центра компетенций по анализу защищенной информации, «Лаборатория Касперского»

В докладе описывается процесс проведения тестирования на проникновение систем на базе z/OS

12:00–12:30 | 25 августа

Track 2 Русский

### Passwordless authentication. Как WebAuthn может защитить ваше приложение

Александр Чикайло

Старший специалист группы экспертизы защиты приложений, Positive Technologies

Разберем, что такое WebAuthn и как эта технология защищает от атак и уязвимостей, связанных с аутентификацией.

Александр покажет эволюцию методов аутентификации за последние столетие и существующие методы passwordless-аутентификации

12:00–12:30 | 25 августа

AppSec.Zone Русский

### Разнообразие фаззинг-ферм, и зачем делать свою

основной трек

Борис Рютин

Исследователь безопасности

Павел Князев

Реверс-инженер, исследователь безопасности

Тема фаззинга с каждым годом становится все популярнее, и инструментов, помогающих в этом, также становится все больше. Среди них особенно можно выделить фаззинг-фермы. Они представляют собой некоторую оркестрацию над множеством фаззинг-движков, которые оркеструют организовать непрерывное или прерываемое фаззинг-тестирование. Изначально такие фаззинг-фермы чаще всего являются набором из нескольких скриптов, но по мере необходимости они эволюционируют до чего-то колоссального.

Авторы доклада рассмотрят наиболее популярные решения и расскажут про создание своей фаззинг-фермы и о том, чем она отличается от других

12:00–13:00 | 25 августа

Track 1 Русский English

### Небезопасные пейджинговые системы

Антон Острокоцкий

Руководитель отдела пентеста, Deiteriy Lab

Ресторанные пейджеры становятся все более популярными в кафе и на фуд-кортах. При этом технологии, которые они используют, совершенно небезопасны.

В своем докладе Антон расскажет о том, как работают пейджеры, об их функциональности и о различных типах таких устройств. Продемонстрирует уязвимости этих систем на примере нескольких популярных моделей, а также потенциальный импакт от эксплуатации данных уязвимостей

12:30–13:00 | 25 августа

Track 2 Русский

### Поиск и управление находками в «Авито»: расширяемый shift-left, который нельзя построить с DefectDojo

Николай Хечумов

Staff Security Engineer, «Авито»

Николай расскажет про существующую в «Авито» гибкую систему управления находками, где все крутится вокруг событий, стейтов и тотальной автоматизации. Она не только разгружает от текущих, но и собирает массу отличных метрик в динамике

12:30–13:30 | 25 августа

AppSec.Zone Русский

### OSINT как образ мышления

Dukera

СОО, сообщество OSINT mindset

В ходе доклада Dukera опишет решение квестов по OSINT, а также покажет, что методология OSINT может быть полезна не только в профессиональной сфере, но и в обычной жизни

12:30–13:30 | 25 августа

Community track Русский

### Практика пентеста мобильного Android-приложения

Игорь Кривонос

Android-разработчик (Java/Kotlin), специалист по тестированию на проникновение (Android/iOS), инженер по безопасности, Python-разработчик, преподаватель по безопасности мобильных устройств, разработке под Android на Python

Потренируемся в пентесте квазиреального приложения на Android и обсудим подходы к поиску багов и уязвимостей

12:30–14:30 | 25 августа

Воркшопы Русский

### Девиртуализация обфусцированных исполняемых файлов

Илья Титов

Основной реверсер CTF-команды SPRUSH

Разберемся с механизмом обфускации control flow — вида виртуальной машины и возможными способами упрощения анализа таких программ. Обсудим первоначальный анализ, преобразование байт-кода в мнемонический вид и декомпиляцию байт-кода виртуальной машины.

От тебя потребуются уверенные навыки программирования на C/Python, базовые навыки работы со средами обратной разработки IDA/Ghidra, умение читать и понимать ассемблерный код, а также в простейших случаях декомпилировать его в голове.

На твоём устройстве должны быть 5–10 ГБ свободного места на жестком диске и процессорная архитектура x86\_64 IDA Pro с декомпилятором x86/x64.

Мы дадим тебе задания, слайды, презентации, модули для разработки плагинов Ghidra и IDE для работы с ними

12:30–15:30 | 25 августа

CTF.Zone Русский

13:00

### EAP-Migrot: атака на WPA2-Enterprise и 802.1x

Павел Яковлев

Младший специалист по тестированию на проникновение, «Лаборатория Касперского»

Александр Волков

Младший специалист по тестированию на проникновение, «Лаборатория Касперского»

Wi-Fi-пентест в последнее время теряет популярность. Пробив корпоративной Wi-Fi-точки не обещает перетекания во внутреннюю сеть. А самые интересные точки работают чаще всего только по EAP-TLS.

Протокол EAP-TLS считается самым безопасным решением для аутентификации в корпоративных сетях. На то есть основная причина: использование PKI для авторизации клиента и сервера

13:00–13:30 | 25 августа

Track 2 Русский

### CASR: ваш спасательный жилет в море крешей

основной трек

Андрей Федотов

Руководитель группы исследований и разработки, ИСП РАН

Алексей Вишняков

Старший инженер DevSecOps, «Яндекс.Облако»

CASR — это фреймворк с открытым исходным кодом для анализа аварийных завершений, который создан для решения вопросов, возникающих после фаззинга при исследовании безопасности и разработке программного обеспечения. Он позволяет генерировать отчеты об аварийных завершениях, проводить их дедупликацию и кластеризацию, а также оценку критичности. Более того, CASR интегрирован с современными фаззерами, такими как AFL++, LibAFL и libFuzzer.

CASR поддерживает несколько архитектур (x86, ARM, RISC-V), языков программирования (C/C++/Go/Rust/Python/Java) и включает в себя LibCASR для разработки пользовательских инструментов анализа. Также разработателю предлагается использовать casr-dojo для экспорта аварийных завершений в систему управления уязвимостями DefectDojo. CASR является ценным инструментом для исследователей безопасности и разработчиков, которые сталкиваются с фаззингом и управлением уязвимостями.

Набор инструментов CASR реализует следующий пайплайн анализа аварийных завершений после фаззинга: создание отчетов об аварийных завершениях со всей необходимой информацией для ручного анализа, дедупликацию и кластеризацию аварийных завершений, создание отчетов UBSCAN и выгрузку новых отчетов в систему управления уязвимостями DefectDojo

13:00–14:00 | 25 августа

Track 1 Русский English

### AnyDOOM: исследование безопасности устройства Anycast M4 Plus

Григорий Пагуба

Научный сотрудник Института компьютерных наук и кибербезопасности, Санкт-Петербургский политехнический университет Петра Великого

Документ разделен на две части. В первой Григорий расскажет о проведенных исследованиях безопасности Miracast приемника Anycast M4 Plus.

Во второй части будет поведено о запуске на данном устройстве игры DOOM с помощью знаний об устройстве, полученных во время исследований

13:30–14:00 | 25 августа

Track 2 Русский

### Просто об интересном. Инженерные аспекты анализа ПО в парадигме ФСТЭК России

Дмитрий Пономарев

Заместитель генерального директора — директор департамента внедрения и развития практик РБПО ООО НТЦ «Фобос-НТ», сотрудник Института системного программирования имени В. П. Иванникова РАН, преподаватель МГТУ имени Н. Э. Баумана

Дмитрий расскажет о векторе развития нормативно-правовой базы ФСТЭК России в отношении конкретных инженерных практик, центрах компетенций ФСТЭК России и ИСП РАН по анализу безопасности ядра Linux и критичных компонентов, инженерном сообществе центра компетенций и его информационных ресурсах

13:30–14:00 | 25 августа

AppSec.Zone Русский

### Oops! We did it again, и что с этим делать

Ют@бл

Инженер, Arh29IT (ex DC78182)

PseudoUlicorn

ИТ-специалист, Arh29IT (ex DC78182)

Проблема потери и последующего восстановления данных становится полнее острее с каждым годом, однако не уходит из повестки полностью.

Спикеры расскажут, что делать, если вы все-таки стали «счастливым» и попали в один процент, а также представят алгоритм действий на своем стенде

13:30–14:30 | 25 августа

Community track Русский



14:00

## Безопасность serverless-приложений

[Игорь Гребенец](#)

Эксперт по безопасной разработке, MTC RED

В рамках доклада будет рассмотрена безопасность serverless-приложений и некоторые особенности, связанные с этой темой

14:00-14:30 | 25 августа

[Track 2](#) [Русский](#)

## Kubernetes Pentest All-in-One: The Ultimate Toolkit

[Сергей Канибор](#)

R&D / Container Security, Luntry

Чтобы автоматизировать и ускорить работу при проведении пентеста Kubernetes-кластера, обычно используют различные инструменты. Но что делать, если ты находишься в окружении с ограничением на сеть и сканировать нужные тулзы внутри контейнера невозможно? А если в контейнере файловая система доступна только для чтения?

В этом случае единственное решение — использовать заранее подготовленный docker image, внутри которого будут все необходимые инструменты. В своем докладе Сергей расскажет, как подготовить такой образ и что в нем должно быть. А еще он представит свою open-source-версию, дополненную разными фичами, например обходом обнаружения с помощью сигнатурных движков

14:00-15:00 | 25 августа

[AppSec.Zone](#) [Русский](#)

## Фаззинг для SDL: выбрать, накрыть, раскопать

[основной трек](#)

[Алексей Вишняков](#)

Старший инженер DevSecOps, «Яндекс Облако»

[Вартан Падарян](#)

Заведующий лабораторией, руководитель направления обратной инженерии бинарного кода, ИСП РАН

[Владислав Степанов](#)

Инженер, Института системного программирования имени В.П. Иванникова РАН

Фаззинг-тестирование — одна из базовых технологий, применяемых при разработке безопасного ПО. Осмысленное и продуктивное применение фаззинга требует его глубокой интеграции в процессы разработки ПО и установления связей с другими технологиями: анализом поверхности атаки, функциональным тестированием, санитайзерами, автоматизированным разбором выявленных сбоев.

В докладе рассказывается как о самом движке фаззера, так и о вопросе выбора фаззинг-целей. Динамический анализ помеченных данных, скрещенный с интроспекцией виртуальной машины, позволяет находить интерфейсы сложного ПО, через которые нарушитель в первую очередь будет атаковать ваше ПО, и в условиях ограниченных ресурсов расставлять приоритеты по порядку фаззинга. А гибридный фаззинг с динамическим символьным выполнением поможет быстрее достичь хорошего покрытия кода и выявить ошибки, даже если они сразу не приводят к видимым сбоям в работе ПО

14:00-15:00 | 25 августа

[Track 1](#) [Русский](#) [English](#)

## Тестирование gRPC-веб-приложений с помощью Burp Suite

[Илья Даненков](#)

Пентестер, Deiteriy Lab

Доклад посвящен исследованию безопасности веб-приложений, использующих gRPC, при помощи инструмента Burp Suite. Этот инструмент не имеет встроенных возможностей для десериализации protobuf, а имеющиеся на данный момент расширения для Burp Suite не являются широко распространенными и имеют ограниченную функциональность для тестирования gRPC.

Цель доклада Ильи — повысить осведомленность о тестировании gRPC. Также в рамках доклада он представит собственное расширение для исследования gRPC

14:30-15:00 | 25 августа

[Track 2](#) [Русский](#)

## Использование Flipper Zero («Флиппер») в red team — проектах

[Георгий Кумуржи](#)

Главный инженер департамента кибербезопасности, ПАО Сбербанк

В докладе будут рассмотрены практические кейсы применения Flipper Zero при моделировании атак на пользователя, кастомные настройки и прошивки, а также варианты маскировки

14:30-15:00 | 25 августа

[Community track](#) [Русский](#)

15:00

## Сказка о внешних компонентах

[Александр Трифанов](#)

Ведущий (в безопасное будущее) инженер, «Авито»

Спикер расскажет о процессе управления внешними компонентами в «Авито»: как в компании научились сканировать зависимости за десять секунд, блокировать и автоматически исправлять уязвимые зависимости

15:00-15:30 | 25 августа

[AppSec.Zone](#) [Русский](#)

## Nuclei: расширяем возможности современных методов проведения пентеста

[Алексей Висторобский](#)

Пентестер, Awillix

При тестировании на проникновение очень часто многие инструменты незаслуженно остаются без внимания, несмотря на то что имеют огромный потенциал как в области самого тестирования, так и в области его автоматизации.

Доклад будет посвящен инструменту Nuclei и его роли при проведении пентестов. Будут рассмотрены примеры поиска конкретных CVE, разбора готовых шаблонов и примеры интеграции Nuclei с другими инструментами с точки зрения и бизнеса, и пентестов

15:00-15:30 | 25 августа

[Track 2](#) [Русский](#)

## Уязвимости в Bitrix24. Разбор CVE-2022-43959

[Дмитрий Лымбин](#)

Начальник отдела исследований защищенности программного обеспечения, SecWare, DC78412

[Сергей Авдеев](#)

Исследователь защищенности программного обеспечения, SecWare, DC78412

Авторы доклада объяснят, как уязвимости в Bitrix24 могут облегчить злоумышленникам задачу по захвату контроллера домена организации.

Они расскажут, как была найдена уязвимость CVE-2022-43959, почему она возникает и как разработчики ее исправили. Покажут kill-chain-атаки и расскажут, как репродуцировать эту уязвимость

15:00-16:00 | 25 августа

[Community track](#) [Русский](#)

## Провод — это хорошо, провод — это надежно: ресерч решений для автоматизации Wiren Board

[основной трек](#)

[Алексей Усанов](#)

Руководитель HW\_LAB, Positive Technologies

В исследовании были рассмотрены датчики и контроллеры компании Wiren Board, производящей средства домашней и коммерческой автоматизации. В докладе будет рассказано, как удалось реализовать MitM-атаку между датчиком и центральным шлюзом. После чего захотелось обновить на датчике прошивку на свою, однако все обновления оказались зашифрованы.

В результате пришлось разбираться с hardware датчиков и особенностями реализации механизмов защиты внутри микроконтроллеров CigaDevice, что привело к полноценному ресерчу всей линейки микроконтроллеров CigaDevice и нахождению множества критичных уязвимостей. Используя часть из них, получили доступ к некоторым критичным данным и реализовать удаленную эксплуатацию

15:00-16:00 | 25 августа

[Track 1](#) [Русский](#) [English](#)

## Pivoting

[Ярослав Шмелёв](#)

Преподаватель CyberED, призёр Standoff 2022 (в составе команды Invuls)

Поговорим об инструментах для туннелирования трафика, о принципах их работы, разберем варианты организации туннелирования для различных операционных систем.

Рассмотрим такие темы, как легитимные порты, обфускация трафика и маскировка под протоколы. Участники смогут попрактиковаться с виртуальными машинами

15:00-17:00 | 25 августа

[Воркшопы](#) [Русский](#)

## Несколько слов об HQL-инъекциях

[Денис Деревцов](#)

Пентестер, Deiteriy Lab

Иъекции Hibernate Query Language (HQL) продолжают представлять серьезную угрозу для приложений, использующих Hibernate или аналогичные ORM-фреймворки.

В рамках доклада Денис расскажет о распространенных векторах атак, методах их предотвращения и возможных последствиях успешной эксплуатации HQL-инъекций. Также он поделится несколькими примерами HQL-уязвимости, которые были встречены в реальных проектах

15:30-16:00 | 25 августа

[Track 2](#) [Русский](#)

## Пентест языковых моделей в клиентских приложениях

[Артём Семенов](#)

Специалист по тестированию на проникновение, RTM Group

Языковые модели постепенно начинают приходить в клиентские приложения. Мы видим, как банки и некоторые организации применяют их для общения с пользователями и обработки информации.

Но злоумышленники также начинают адаптироваться к этому. Пример — случай атаки на MathGPT, когда киберпреступник смог заставить LLM исполнять код на сервере.

В своем докладе Артём представит методику для проведения пентеста подобных приложений, опишет риски и находки. Также он поделится инструментами для проведения тестирования

15:30-16:30 | 25 августа

[AppSec.Zone](#) [Русский](#)

## Асимметричная криптография на эллиптических кривых

[Александр Соколов](#)

Криптограф из CTF-команды SPRUSH

Познакомимся с утилитами для работы с эллиптическими кривыми, некоторыми протоколами, а также с возможными уязвимостями в этих протоколах.

На воркшопе обсудим, как устроены эллиптические кривые и как их применяют в современной криптографии. Еще поговорим, как важно выбирать параметры для кривых, и рассмотрим криптографические схемы, использующие в основе ECC: ECDH, ECDSA.

От тебя обязательно — знание синтаксиса языка Python, желательны — хотя бы знание представление об алгебраических группах.

На твоём устройстве должны быть библиотеки: PyCryptodome, fastecdsa, py\_ecc для Python. Установи CryptoHack Docker Container и опционально поставь SageMath (он есть в докере CryptoHack).

Мы дадим тебе слайды презентации и интерактивные пошаговые инструкции для практических заданий

15:30-18:00 | 25 августа

[CTF.Zone](#) [Русский](#)

16:00

## Evalsloit: захват сервера одной строкой

[Mark Tauber](#)

Независимый исследователь

Доклад Mark Tauber — развитие темы однострочных веб-эксплоитов в условиях ограниченных прав и функций сервера.

Вопросы, которые предлагает обсудить спикер:

- Способы обхода WAF: как не стать очередной его жертвой?
- Почему тему забросили, какой у нее потенциал и что удалось реализовать в ограниченных условиях работы?
- Как защититься от таких «умников»?

16:00-16:30 | 25 августа

[Community track](#) [Русский](#)

## Скачать фильмы за кредиты без СМС и регистрации: история одного supply chain под Linux

[Леонид Безверщенко](#)

Исследователь угроз информационной безопасности, «Лаборатория Касперского»

[Георгий Кучерин](#)

Исследователь угроз информационной безопасности, «Лаборатория Касперского»

В процессе расследования одного инцидента выяснилось, что популярный менеджер загрузок для Linux скачивал совсем не то, что ожидал пользователь. А что именно, слушатель узнает из этого доклада

16:00-16:30 | 25 августа

[Track 2](#) [Русский](#)

## GigaVulnerability: GD32 Security Protection bypass

[основной трек](#)

[Алексей Коврижных](#)

Исследователь безопасности, Positive Technologies

При разработке аппаратных решений на базе микроконтроллеров производители хотят защитить свою прошивку от попадания в руки злоумышленников. Для этого на большинстве микроконтроллеров реализованы технологии защиты от считывания (readout protection). Так ли хорошо они защищают?

В первой части доклада коротко будет рассказано о существующих атаках на эти технологии. Вторая, основная часть доклада будет посвящена исследованию технологии security protection микроконтроллеров GD32 (CigaDevice) и найденным уязвимостям, позволяющим получить содержимое памяти несмотря на включенную защиту

16:00-17:00 | 25 августа

[Track 1](#) [Русский](#) [English](#)

## Как мы SBOM генерировали и к чему пришли

[Артём Кадушко](#)

Application Security Lead

В докладе Артём расскажет про путь, который он прошел в рамках создания процесса software composition analysis, а именно генерации SBOM-файла. Помимо этого, он объяснит, почему основным инструментом нельзя решить все проблемы в генерации SBOM

16:30-17:00 | 25 августа

[AppSec.Zone](#) [Русский](#)

## Попробуй спрятаться: расширяем возможности обнаружения эксплоитов WinRM

[Антон Величко](#)

Руководитель лаборатории цифровой криминалистики и исследования вредоносного кода, F.A.C.S.T.

Ни для кого не секрет, что атакующие довольно часто используют службу Windows Remote Management для перемещения по инфраструктуре. В докладе Антон расскажет о том, какие артефакты будут указывать на использование WinRM.

Также поговорим о недокументированном артефакте этой службы и как при помощи него быстро выявить эксплуатируемые атакующими хосты, в том числе когда журналы событий были удалены

16:30-17:00 | 25 августа

[Track 2](#) [Русский](#)

## Опять веб, опять сервера и опять всё в \*\*\*\*

[Роман Ананьев](#)

DC78422

Поговорим снова про веб, снова про серверы, снова про инфраструктуру и про то, какие они дырявые. И да, несмотря на то что суются снова и снова новые и новейшие технологии со старыми проблемами. А проблема-то не в них %)

16:30-17:00 | 25 августа

[Community track](#) [Русский](#)

17:00

## Процессы SOC, о которых не напишут в книжках

[Сергей Солдатов](#)

Руководитель центра мониторинга кибербезопасности, «Лаборатория Касперского»

Улучшения — следствие правильного анализа собственных ошибок. В докладе за 15 минут Сергей расскажет о таких ошибках и о том, какие процессы были внедрены в его центре мониторинга кибербезопасности, чтобы этих ошибок не допускать.

Доклад может быть полезен руководителям и методологам SOC, а также тем, кто предоставляет услуги консалтинга

17:00-17:30 | 25 августа

[Track 2](#) [Русский](#)

## Как скрыть свои действия, когда отслеживается каждый шаг

[основной трек](#)

[Иван Гаврилов](#)

AppSec-инженер, Innostage

Современные инструменты безопасности все чаще используют технологию eBPF для мониторинга происходящих на хостах событий. Кажется, что предоставляемые ею возможности и новейшие команды защиты способны видеть все и вся и своевременно предотвращать малейшие попытки компрометации. Или же нет?

В своем докладе Иван рассмотрит сильные и слабые стороны технологии eBPF для задач безопасности, а также возможные методы сокрытия своих действий на примере существующих eBPF-based-инструментов безопасности

17:00-18:00 | 25 августа

[Track 1](#) [Русский](#) [English](#)

## Bugs on the Orbit

[Татьяна Курмашева](#)

Независимый эксперт

С развитием технологий создание и запуск малых космических аппаратов становятся все более доступными. На орбите Земли в функционирующем состоянии уже находятся около 5000 спутников.

В рамках доклада Татьяна представит взгляд на ситуацию с точки зрения информационной безопасности, попутно рассмотрев особенности протоколов и устройств современных малых космических аппаратов

17:00-18:00 | 25 августа

[Community track](#) [Русский](#)



## Малвари и криптография

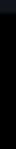
Жасулан Жусупов aka @cocomeleon

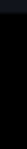
Аналитик угроз, MSSP Global

Доклад посвящен роли криптографии в разработке вредоносных программ и шифрованию полезной нагрузки с использованием классических криптографических алгоритмов. Жасулан расскажет о проведенных практических исследованиях и результатах использования алгоритмов шифрования TEA, Madryga, RC5, A5/1, Z85, DES и др.

Сейчас также исследуется применимость криптографии на основе эллиптических кривых. Слушатели доклада узнают, как это влияет на показатель обнаружения VirusTotal и насколько он применим к обходу антивирусного программного обеспечения

**17:30–18:00 | 25 августа**

 Track 2

 Русский

**18:00**

### Заккрытие

**основной трек**

**18:15–18:30 | 25 августа**

 Track 1

 Русский

 English