OFFZONE 2024

Культурный центр ЗИЛ, 22–23 августа
г. Москва, ул. Восточная, д. 4, к. 1

22 августа, четверг	Main track
10:00–10:30	**Открытие**
10:30–11:30	**Keynote address** **Корень зла** **Сергей Голованов** Главный эксперт, «Лаборатория Касперского» В докладе пойдет речь об инцидентах информационной безопасности за последние 20 лет. Рассмотрим их причины, в том числе истинные, обычно скрытые от широких масс Сложность: easy
11:30–12:30	**Угнать за 5 СМС: история об RCE в модемах Telit** **Александр Козлов** Ведущий эксперт, «Лаборатория Касперского» **Сергей Ануфриенко** Руководитель группы, «Лаборатория Касперского» А что, если ваш модем можно взломать, отправив всего несколько СМС-сообщений? Доклад посвящен рассмотрению уязвимостей модемов Telit, позволяющих удаленно выполнить произвольный код, обойти проверку цифровой подписи и повысить привилегии выполнения любого пользовательского мидлета до уровня производителя. Спикеры расскажут, как им удалось удаленно активировать Over The Air Provisioning (OTAP) и установить на модем собственный мидлет с максимальными привилегиями — привилегиями производителя Сложность: hard

12:30–13:30

Pentest FreeIPA, или Углубляемся в зоопарк

Михаил Сухов
Руководитель отдела анализа защищенности,
Angara Security

FreeIPA все чаще встречается в отечественных инфраструктурах, в том числе в связи с импортозамещением. Докладчик покажет «внутрянку» FreeIPA и расскажет, какие в ней могут скрываться уязвимости

Сложность: hard

13:30–14:30

[Dev]iceSecOps, или Зачем мы написали инструмент для анализа прошивок

Борис Рютин
Инженер безопасности, «Яндекс»

Никита Лычаный
Инженер безопасности, «Яндекс»

После перехода на сторону защитников любовь к хакингу устройств не отпускала их, поэтому они решили переиспользовать свои умения, но уже и для улучшения безопасности устройств тоже. Так родился инструмент для анализа прошивок YA4FW (Yet Another Analyzer for Firmwares)

Сложность: medium

14:30–15:30

Вредоносное ПО и закрепление в системе: как злоумышленники взламывают Windows?

Жасулан Жусупов
Сооснователь, MSSP Research LAB

Спикер расскажет, как обнаружил несколько нестандартных и необычных методов сохранения вредоносного ПО с помощью модификаций реестра и подмены DLL в Windows Internet Explorer, Win32API Cryptography, Windows Troubleshooting, Microsoft Teams (исправлено в 2024 году) и Process Hacker 2 (исправлено в v3)

Сложность: medium

15:30–16:30

Бинарный композиционный анализ: ищем уязвимые нативные библиотеки в Android-приложениях

Евгений Жуковский
Security Researcher, основатель DAP Solutions

Мобильные приложения, как и большинство других программ, используют компоненты с открытым исходным кодом (OSS). Но насколько внимательно разработчики следят за отсутствием известных уязвимостей в используемых версиях библиотек?

Для определения и отслеживания сторонних зависимостей в продуктах существуют инструменты композиционного анализа (SCA). Однако что делать, если у вас нет исходного кода приложения или его частей?

В докладе будут рассмотрены проведение композиционного анализа бинарных файлов (BSCA) и решаемые при этом задачи на примере анализа нативных библиотек Android-приложений. Также будет рассказано, что интересного было найдено в зависимостях популярных отечественных мобильных приложений

Сложность: hard

16:30–17:30

Хроники red team: Wi-Fi, 0-day и не только

Денис Погонин
Старший специалист отдела анализа защищенности, BI.ZONE

В докладе спикер расскажет про эксплуатируемые уязвимости и векторы атак, применяемые в red team — проектах. В рамках выступления будут рассмотрены цепочки атак для получения первоначального доступа через уязвимости веб-приложений, фишинг и Wi-Fi. Также в докладе будут продемонстрированы поиск 0-day-уязвимостей в приложении Websoft HCM и способы дальнейшего развития атак через инструмент TeamCity

Сложность: medium

17:30–18:30

Как атакующие провели майские: профи или скрипт-кидди?

Иван Сюхин
Руководитель направления группы расследования инцидентов, группа компаний «Солар»

Пока вся страна жарила на дачах шашлыки, команда Ивана реагировала на инциденты!

Первую атаку устроила одна известная группа, вооружившись ngrok, gs-netcat и LockBit 3.0. Спикер разберет некоторый ее инструментарий, а также пошагово проанализирует действия атакующих, чтобы продемонстрировать, что иногда операторы группы не такие уж опытные и профессиональные люди, какими нам их рисует воображение.

Во время второй атаки предположительно проукраинская группировка пыталась разрушить инфраструктуру компании (шифрование хостов, удаление данных, уничтожение ESXi). Для злодеяний атакующие использовали характерную утилиту localtonet. Иван уделит внимание ей, а также расскажет о драйвере для обхода механизмов СЗИ (SOGFN.sys) и другом инструментарии атакующих.

Третью атаку устроила Shedding Zmiy. Там команда Ивана наблюдала изменения в применяемых тактиках и техниках.

Во всех атаках, несмотря на сложности, удалось восстановить первоначальную точку входа, чем спикер также поделится

Сложность: easy

22 августа, четверг — Community track

11:30–12:30

Red team: абьюзим Google для борьбы с Google

Александр Гончаров
Старший специалист по анализу защищенности, Innostage

В последние годы Google усложняет жизнь мошенникам, которые создают фишинговые сайты. И это правильно, однако под удар попадают и пентестеры.

В докладе разберем, как можно использовать OSINT и утечки исходного кода Google для борьбы с Google, рассмотрим способы обхода песочниц, красных страниц и других механизмов защиты Google, которые не узнать простым смертным. Плюс разберем практики, которые применяют топовые red team

Сложность: medium

12:30–13:30

Подпольный цирк: арбитраж на теневых форумах

Александр Забровский
Аналитик отдела мониторинга цифровых угроз, «Лаборатория Касперского»

Этот доклад раскроет всю внутреннюю кухню форумов даркнета. Слушатели узнают, как устроены такие форумы, кто их аудитория, как проходят киберкриминальные сделки и даже как пользователи обманывают своих же «коллег». Спикер разберет всю систему подпольного рынка — от правил форумов и работы гарантов (специализированных сервисов «защиты») до особенностей института репутации и работы здешних судов.

Спикер приведет много примеров из жизни — от неудачных сделок до курьезных конфликтов между пользователями, а также расскажет, как арбитры подпольных форумов решают самые запутанные или анекдотичные дела. Слушателей ждут удивительные и невероятные истории, которые показывают, что даже в теневой сети не обходится без юмора и драмы!

Доклад будет полезен всем интересующимся темой, а также тем, кто занимается защитой от связанных киберугроз: OSINT-специалистам, исследователям кибербезопасности и даркнета, сотрудникам специализированных направлений в компаниях, например digital risk protection, antifraud, threat intelligence

Сложность: easy

13:30–14:30

История одной уязвимости: RCE в телекоммуникационном оборудовании

Алексей Романов
Руководитель направления развития облачных решений кибербезопасности, BI.ZONE

Начиная с 2022 года вопрос замены иностранного ПО встал достаточно остро. В связи с этим на рынке отечественных решений появилось большое количество ПО и аппаратных комплексов.

Со значительным приростом новых утилит и оборудования также выросли и риски кибербезопасности, так как новоиспеченные продукты могут иметь множество уязвимостей и неполадок.

В ходе доклада будет рассказана история одной критической уязвимости, которая была обнаружена в прошивке российского телекоммуникационного оборудования. Она позволяла неаутентифицированному пользователю несанкционированно выполнить программный код

Сложность: medium

14:30–15:30

Разработка стратегий уклонения от EDR

Кирилл Комогоров
Специалист по тестированию на проникновение, BI.ZONE

Доклад посвящен основам архитектурного строения СЗИ класса EDR в контексте ОС семейства Windows.

Спикер рассмотрит основные составляющие EDR: с точки зрения атакующей стороны — на предмет исследования возможности обхода, а со стороны защиты — на предмет противодействия уклонению от обнаружения EDR-решением

Сложность: hard

15:30–16:30

Под маской AI: обнаружение вредоносного кода в ML-моделях

Татьяна Курмашева
Основатель, AI Security Technologies LLC

Доклад посвящен возможностям детектирования вредоносного кода в моделях машинного обучения, структуре файловых форматов, используемых для их хранения, процессу запуска моделей и существующим векторам атак. Также спикер представит результаты реального исследования популярных публичных репозиториев

Сложность: medium

16:30–17:00

Накопление крешей при непрерывном фаззинге с помощью CASR

Илья Егоров
DevOps-инженер, «СберТех»

При непрерывном фаззинге часто возникают креши, похожие на старые или дублирующие их. CASR предлагает метод автоматического отбрасывания дубликатов и распознавания похожих крешей

Сложность: hard

17:00–18:00

PCI-exploit

Егор Коледа
Исследователь безопасности устройств, 0x08

Сказ о том, что такое DMA-атаки, как их делают и, конечно, как можно их удешевить, найдя уязвимости в доступном оборудовании

Сложность: medium

22 августа, четверг — AppSec.Zone

12:30–14:00

BI.ZONE Bug Bounty: итоги года

Евгений Волошин
Директор департамента анализа защищенности и противодействия мошенничеству, BI.ZONE

Андрей Лёвкин
Руководитель продукта BI.ZONE Bug Bounty, BI.ZONE

Сергей Крайнов
Начальник управления экспертизы кибербезопасности, Сбер

Роман Мылицын
Руководитель направления перспективных исследований и инновационных проектов, «Группа Астра»

Артём Бельченко
Независимый исследователь

Российские компании уже оценили багбаунти как эффективный инструмент анализа защищенности внешнего периметра. Крупнейшие организации из финансовой отрасли, госсектора, IT-сферы, ритейла и других значимых секторов экономики все активнее выходят со своими программами на платформы.

Эксперты BI.ZONE и других организаций обсудят развитие рынка багбаунти в России, поделятся результатами работы платформы BI.ZONE Bug Bounty и впечатлениями ее пользователей

15:00–16:00

Bug bounty: простые критические баги

Алексей Лямкин
Эксперт отдела Bug Bounty, VK

Доклад посвящен тому, как небольшие ошибки могут привести к критическим для бизнеса угрозам

Сложность: medium

16:00–17:00

Гори, гори ясно, чтобы не погасло. Выгорание как тренд современной ИБ

Сергей Зыбнев
Пентестер, Awillix

Артём Бельченко
Независимый исследователь

Доклад про выгорание. Откуда оно появляется? Почему мы так часто выгораем? И надо ли с ним что-то делать?

Сложность: easy

17:00–18:00

Платформа для автоматизации процессов фаззинга: проблемы и решения

Виктория Егорова
Заместитель директора департамента анализа безопасности, ПАО «Группа Астра»

Алексей Панов
Руководитель направления динамического анализа, ПАО «Группа Астра»

Все знают о том, что фаззинг — необходимый этап анализа безопасности для любого продукта. Когда перед вами одно небольшое приложение, не возникает сложностей в том, чтобы его пофаззить, но что, если речь идет об операционной системе?

Спикеры расскажут, почему их команда пришла к тому, что ей нужна своя платформа автоматизации процессов фаззинга. Также слушатели узнают о существующих платформах и о тех случаях, когда эти решения не подходят

Сложность: hard

18:00–18:30

Как фолзят SCA-решения

Алексей Москвин
Независимый исследователь

Даниил Садырин
Независимый исследователь

Докладчики докажут, что при подборе пакетов в разрабатываемый проект важно оценивать уязвимости в компонентах не только по отдельности, но и в совокупности — для безопасности всего проекта

Сложность: medium

22 августа, четверг — AntiFraud.Zone

11:50–12:30

Мошенничество в автомобильных грузоперевозках: номиналы

Фарид Джафаров
Ассоциация безопасности логистики

Грузоперевозки — это системообразующая отрасль, без которой не существует ни одно государство. Мошенники, конечно, не оставили без внимания это поле деятельности и всячески пытаются завладеть чужим имуществом. В докладе будет рассказано о виде мошенничества, который коснулся и логистики, а конкретнее — автомобильных грузоперевозок. Почему номинальных директоров становится все больше и какие бывают последствия — попробуем разобраться вместе

Сложность: easy

12:30–13:15

Как картинки в интернете забирают деньги и данные

Сергей Бнятов
Руководитель направления мониторинга и расследования киберинцидентов, Ecom.tech (ex Samokat.tech)

Спикер расскажет, что такое digital risk monitoring и почему это важно.

Как цифровые риски расширяют потенциальную поверхность атаки на организацию и чем может помочь знание, что происходит вокруг бренда? Зачем это надо SOC? Как собрать свою дата-модель для мониторинга бренда, а также проверки на коленке и Python? Слушатели доклада узнают ответы на эти вопросы

Сложность: hard

13:15–13:45

Фрод сегодня и что нас ждет завтра

Александр Большунов
Руководитель направления, департамент кибербезопасности ПАО Сбербанк

Рассмотрит популярные мошеннические схемы, с которыми пришлось столкнуться компаниям и людям в этом году. Как кибермошенники используют генеративный ИИ и на какие цифровые следы стоит обратить внимание? Почему схема FakeBoss все еще работает и как с этим всем бороться?

Сложность: medium

13:45–14:30

Применение deep learning в антифроде. Опыт Сбера

Кирилл Вышегородцев
Исполнительный директор научно-исследовательской лаборатории кибербезопасности, Сбер

Андрей Пинчук
Начальник управления моделирования и развития AI департамента противодействия мошенничеству, Сбер

Градиентный бустинг уже много лет является SotA в задачах антифрода. А можно ли существенно улучшить результаты с теми же источниками данных?

Доклад посвящен последним исследованиям в области применения современных deep learning — технологий для противодействия мошенничеству

Сложность: hard

14:30–15:15

О, снова мошенники! Как построить свой антифрод с нуля?

Катя Тьюринг
Специалист по борьбе с мошенничеством

Спикер разберет на примере коммерческой компании, как оценить ущерб от мошенников, сделать подготовительные шаги, а потом запустить антифрод, который будет работать

Сложность: medium

15:15–15:45

Противодействие кибер-мошенничеству в 2024 году

Евгений Винокуров
Руководитель дирекции предотвращения кибермошенничества, АО «Альфа-Банк»

В рамках доклада спикер затронет следующие темы:

- Общий объем фрода. Изменения в статистике по фроду по отношению к прошлому году. Доля фрода с оформлением кредитов.
- Внедрение новой функциональности в «Альфа-Банке»: запуск звонка в приложении «Альфа-Мобайл».
- Решения по социальной инженерии (обмен с БКИ, ответственность за сбор и хранение согласий на обработку данных, мошеннические звонки)

Сложность: medium

15:45–16:15

Новый виток Buhtrap: схема с веб-инжектом

Андрей Мансуров
Старший аналитик по противодействию мошенничеству, BI.ZONE

Доклад посвящен деятельности финансово мотивированной киберпреступной группировки Buhtrap. Спикер разберет новую схему с веб-инжектом, с помощью которой мошенники открыли новый способ кражи денежных средств у российских организаций

Сложность: hard

16:15–17:00

Telco fraud

Петр Алферов
Директор по управлению уровнем фрода и гарантированию доходов, «билайн»

В докладе пойдет речь об источниках мошеннического трафика и развитии антифрод-защиты операторов связи и телекоммуникационной отрасли

Сложность: medium

17:00–17:30

Автоштрих там правит бал(л): подпольный бизнес на программах лояльности

Вера Коленикова
Специалист отдела расследования высокотехнологичных преступлений, F.A.C.C.T.

Доклад включает обзор теневого рынка по сбыту баллов лояльности крупного ритейла. Спикер расскажет о «дампах», «штрихах», несанкционированном доступе в систему процессинга программы лояльности и о том, что с этим делать (а еще немного о том, кто в этом виноват)

Сложность: hard

17:30–17:50

No pasaran? Боты: непрекращающаяся борьба на невидимом фронте

Дмитрий Криков
Технический директор, NGENIX

Боты могут составлять до 90% трафика типичного маркетплейса. Для IT- и ИБ-команд веб-приложений так называемые умные боты — парсеры, скраперы, скальперы и др. — могут стать источником множества проблем. Паразитный бот-трафик — причина роста нагрузки на IT-инфраструктуру, дополнительных затрат и финансовых потерь, угроз безопасности. При этом боты умеют искусно имитировать поведение реальных пользователей и быть ниже радаров систем защиты от киберугроз, так что их идентификация — очень нетривиальная задача.

Спикер расскажет о различных способах идентификации ботов и методах борьбы с ними, основываясь на собственном опыте отражения бот-атак в условиях реального мира. Тема будет интересна IT- и ИБ-специалистам, работающим в сфере веб-приложений

Сложность: medium

17:50–18:10

Кредитные финансовые пирамиды: новый тренд или хорошо забытое старое?

Мадина Ажахметова
Исполнительный директор управления организации расследований департамента безопасности,
ПАО Сбербанк

Спикер считает, что это новый вызов для всех субъектов финансового рынка в сфере борьбы с внешним мошенничеством. А финансовая пирамида и есть внешнее мошенничество, приводящее к все большим потерям обычных людей, которые не осознают последствий от своих действий. Это приводит к фатальным ошибкам и, как результат, может принимать разного рода формы и величину ответственности.

Мадина приведет конкретные примеры работы и поделится способами противодействия через призму практики Сбера

Сложность: medium

18:10–18:30

Как мы распознаём фейковые отзывы и работаем с ними

Андрей Будилов
Руководитель группы антифрода, «Яндекс»

Доклад посвящен тому, зачем люди оставляют фейковые отзывы на различных сервисах, а также какой вред это наносит UGC-платформе и всем ее пользователям. Спикер определит основные метрики измерения успеха антифрода и разберет несколько AI-подходов, которые успешно применяются для поиска фейковых отзывов в «Яндексе»

Сложность: medium

22 августа, четверг	CTF track

11:30–12:00

CTF и жизнь

Павел Блинников
Руководитель группы исследования уязвимостей, BI.ZONE

Одна из главных претензий сторонних наблюдателей к соревнованиям типа CTF заключается в том, что участники решают «нереалистичные» таски.

В открывающем докладе CTF track Павел представит свое видение связи соревнований с реальной жизнью. Он расскажет, как скилы, полученные на CTF, могут пригодиться в реале — и опосредованно, и напрямую

Сложность: easy

12:00–12:30

Многогранный CTF: применяем идею тасков вне соревновательных CTF

Георгий Зайцев
Специалист отдела анализа приложений,
Positive Technologies

Георгий попробует рассказать о том, что концепция CTF-таска не ограничивается применением внутри соревновательных CTF, и изложит свою философию в отношении создания тасков

Сложность: easy

12:30–13:00

Как войти в браузерную безопасность?

Юрий Паздников
Младший специалист по тестированию, BI.ZONE

В докладе будут описаны способы входа в сферу браузерной эксплуатации. Спикер расскажет, как на практике применить знания, полученные в ходе решения CTF

Сложность: medium

14:00–15:00

Криптография на решетках и почему ее не стоит бояться

Александр Соколов
Младший консультант по безопасности, Aztec Labs

Кирилл Кудрявцев
Neplox audit group

Доклад посвящен криптографии на решетках, а также применению алгоритма LLL в криптоанализе. Спикеры разберут подходы к построению решеток и рассмотрят неочевидные примеры с CTF

Сложность: hard

15:00–16:00

Хакерские техники на службе инженера ИБ v1.1

Артём Артамонов
Security Vision

В своей практике Артём, работая инженером в IT и особенно в ИБ, накопил достаточно большое количество случаев, когда сроки горят, проект нужно закрывать, но в рабочей инфраструктуре заблокировано чуть меньше, чем все, а бюрократия/люди/регламенты и черт знает что еще не позволяют осуществить нужные работы. Приходилось изворачиваться и использовать околохакерские техники для обхода таких ограничений. Этими историями он и хочет поделиться.

Версия 1.1, обогащенная

Сложность: easy

22 августа, четверг — AI.Zone

11:30–12:20

Self-hosted LLMs в кибербезопасности

Дмитрий Лекомцев
Ведущий специалист по машинному обучению и исследованию данных, BI.ZONE

Докладчик расскажет о преимуществах локальных больших языковых моделей (LLM) перед популярными онлайн-сервисами. Будут затронуты вопросы выбора моделей, оценка стоимости их обучения и способы снижения затрат, а также новые риски, связанные с использованием LLM. Спикер продемонстрирует AI-ассистента в BI.ZONE EDR на базе self-hosted LLM

Сложность: medium

12:20–12:40

Как использовать всю мощь ChatGPT и не бояться утечек

Александр Смирнов
Старший инженер продуктовой безопасности, «Циан»

В докладе спикер расскажет, как в «Циане» реализовали единый безопасный отказоустойчивый расширяемый механизм для взаимодействия сотрудников и сервисов с внешними LLM (такими, как ChatGPT).

Поговорит о том, как они смогли начать контролировать организацию интеграции, отправляемые данные и доступные лимиты. Разберет подводные камни и бенефиты внедрения

Сложность: medium

12:40–13:10

Few-shot в SOC

Игорь Гоц
Инженер по информационной безопасности, «Яндекс»

Рассмотрит, сможет ли техника few-shot prompting с использованием LLM помочь выполнить оценку срабатывания SIEM

Сложность: easy

13:10–13:30

Threat Intel с помощью LLM для LLM

Юрий Лебединский
Ведущий эксперт, ПАО Сбербанк

Чтобы быть в курсе последних уязвимостей систем, в которых используется генеративный ИИ, специалистам по кибербезопасности приходится обращаться к большому количеству научных публикаций и новостей.

В ходе доклада слушатели узнают, почему «нельзя просто взять и использовать» большие языковые модели для отбора научных статей. Юрий представит концепцию идеальной системы threat intelligence и расскажет о разработанной системе отслеживания публикаций, которая может использоваться для отбора статей не только по кибербезопасности ИИ, но и в других областях

Сложность: medium

13:30–14:35

Генеративные и мультимодальные модели для обнаружения и классификации фишинговых сайтов

Юрий Иванов
Технический директор, руководитель направления ML, «АВ Софт»

Владимир Ларькин
Инженер по машинному обучению, «АВ Софт»

Ян Токарев
Инженер по машинному обучению, «АВ Софт»

Доклад охватывает современные методы обнаружения фишинговых сайтов и защиты брендов. Рассматриваются два основных направления: семантический поиск новых фишинговых сайтов с использованием генеративных моделей и крупных языковых моделей (LLM), а также мультимодальное обнаружение фишинговых ссылок, включающее визуальный анализ, анализ контента и лингвистический анализ URL страницы.

Объясняется процесс генерации семантических запросов для адаптивного поиска фишинговых сайтов, учитывающий как семантику, так и контекст атак. Особое внимание уделяется технологиям обработки естественного языка (NLP) и компьютерного зрения (CV).

Приводятся архитектуры моделей, особенности их обучения, метрики эффективности, а также функциональность системы в целом. Представлены примеры успешного применения этих методов для защиты брендов и предотвращения кибератак. Доклад завершается ключевыми выводами, демонстрацией работы системы и рекомендациями по внедрению

Сложность: medium

14:35–15:15

Нужно больше данных: прогнозирование метрик CVE за счет их взаимной трансформации

Дмитрий Левшун
Старший научный сотрудник, Санкт-Петербургский Федеральный исследовательский центр Российской академии наук

Доклад посвящен исследованию эффективности методов ансамблевого и глубокого обучения в задаче прогнозирования метрик CVSS на основе их взаимной трансформации. Уникальность решения заключается в использовании метрик CVSS третьей версии для прогнозирования метрик CVSS второй и наоборот.

Спикер раскроет подробности собранных наборов данных и результаты, полученные для прогноза каждой из метрик, а также опишет особенности полученных результатов, возникшие трудности и пути их решения

Сложность: hard

15:15–16:10

Ваше лицо кажется мне знакомым: разведка, анализ и методы атак на ML в системах распознавания лиц

Александр Мигуцкий
Специалист отдела перспективных технологий, Positive Technologies

Мы живем в мире, где системы распознавания лиц используются практически везде: от валидации возраста и биометрической идентификации в режиме онлайн до видеонаблюдения и оплаты в реальном мире. Неудивительно, что алгоритмы машинного обучения, используемые в этих системах, совершили скачок за последние 10 лет. В данном докладе спикер сделает обзор технологий для распознавания лиц, атак и методов обхода, а также продемонстрирует две новые атаки, направленные на онлайн- и офлайн-системы распознавания. Данные атаки были успешно применены в существующих коммерческих и опенсорс-системах распознавания лиц

Сложность: hard

16:10–16:50

Отравленные документы: как атаковать RAG-пайплайны

Владислав Тушканов
Руководитель, Kaspersky MLTech,
«Лаборатория Касперского»

Retrieval Augmented Generation (RAG) — одна из основных парадигм разработки приложений на основе LLM, которые работают с большими текстами. При этом значительная часть LLM-систем уязвима перед атаками типа indirect prompt injection, когда внешние непроверенные данные включают в себя вредоносные инструкции. Насколько легко заставить RAG-систему, получившую на вход зловредный документ, начать выполнять не те инструкции, которые хотел разработчик? На примере ChatGPT покажет несколько приемов, которые позволяют сделать такие атаки эффективными

Сложность: medium

16:50–17:30

tRAGедия LLM. Эксплуатируем бэкдоры в базе знаний RAG

Артём Булгаков
Пентестер, BI.ZONE

Руслан Махмудов
Эксперт по направлению анализа защищенности, BI.ZONE

Спикеры расскажут про архитектуру RAG в LLM, про основные векторы атак через внедрение вредоносного документа и способ их оптимизации

Сложность: medium

17:30–18:10

Отравление данных в LLM и новые риски мультиагентных систем

Данил Капустин
AI Engineer, Raft Digital Solutions

Доклад посвящен актуальным проблемам безопасности в области больших языковых моделей и мультиагентных систем. Спикер расскажет о ключевых угрозах, приводящих к отравлению данных. Также он рассмотрит, как чрезмерная автономность ИИ может привести к новым уязвимостям, и раскроет стратегии защиты от этих угроз

Сложность: easy

18:10–18:30

Pentest Copilot, или Как я создал AI-помощника по пентесту

Данила Урванцев
Специалист по анализу защищенности, УЦСБ

Доклад о том, чего позволяет достичь подгрузка экспертных материалов в базу знаний LLM

Сложность: easy

22 августа, четверг — Workshops

12:00–15:00

Мониторинг атак и защита подручными средствами в режиме real-time (defence на примере CTF)

Сергей Сидорин
Преподаватель, CyberED

Что будем делать

Проанализируем 3 типа атак и определим, какие решения по блокировке необходимо принять.

Продолжительность: 3 часа.

В программе

- Сбор метрик.
- Их анализ.
- Принятие решения.
- Блокировка.

Что потребуется

- Linux;
- Iptables, nginx + wireshark

Сложность: easy

15:30–18:30

«Мешок картошки»: интересные особенности и практический анализ Potato-атак

Владислав Бурцев
Аналитик threat intelligence, «Лаборатория Касперского»

Что будем делать

Проверим работоспособность эксплоитов на Windows, а еще сформулируем гипотезы и принципы для создания правил детектирования.

Продолжительность: 3 часа.

В программе

- Предварительные задания.
- Fixed Potatoes.
- Modern Potatoes.
- Общие паттерны Potato-атак.
- Митигации и детектирование.

Что потребуется

- Windows VM + Visual Studio Community Edition + Sysinternals Suite;
- Kali Linux VM

Сложность: medium/hard

23 августа, пятница	Main track

11:00–12:00

Безопасность бинарных приложений в «Яндексе»

Павел Черемушкин
Старший инженер по информационной безопасности, «Яндекс»

Приложения, перед которыми стоит задача высокой производительности, зачастую пишутся на небезопасных с точки зрения использования памяти языках программирования, таких как C и C++.

В «Яндексе» множество сервисов разрабатывается на C++. Среди них — и доступные исключительно для внутренних пользователей, и опубликованные в open source: YDB, YT, userver и др.

Докладчик расскажет о подходах в обеспечении безопасности таких сервисов, экспериментах с автоматизацией поиска уязвимостей при помощи фаззинга, а также о наиболее интересных уязвимостях, которые были выявлены за последнее время на внутренних аудитах или найдены внешними исследователями в рамках программы «Охота за ошибками»

Сложность: medium

12:00–13:00

Побеги из контейнеров: Kubernetes 2024 edition

Дмитрий Евдокимов
Founder & CTO, Luntry

Николай Панченко
Ведущий специалист обеспечения безопасности K8s и Cloud, Т-Банк

Тема побегов из контейнеров в K8s не нова. Ввиду эволюции экосистемы и инструментов IT в кластере появляются новые возможности. Но новые возможности, как известно, порождают новые уязвимости! Это ведет к тому, что в инфраструктуре K8s появляется возможность эксплуатации новых векторов атак для побега из контейнера. При этом старые векторы также стабильно присутствуют и не дают о себе забывать. В рамках доклада спикеры на примерах рассмотрят векторы для побегов, которые стоит знать, помнить и учитывать в 2024 году

Сложность: medium

13:00–14:00

Фильтрация eBPF в Kubernetes, или Веселый рафтинг по реке сетевых данных с подводными камнями

Алексей Рыбалко
Специалист по защите сред контейнеризации,
«Лаборатория Касперского»

Технологии фильтрации сетевых потоков данных в контейнерной среде — первоочередной инструмент для защиты от проникновения злоумышленников в корпоративную сеть.

Для перехвата и анализа передаваемых данных применяется несколько подходов, среди которых внедрение service mesh, служебных sidecar-контейнеров в Kubernetes Pod, внедрение агентов защиты в контейнеры. Но все подобные подходы забирают существенный процент ресурсов кластера, поскольку на каждый контейнер с полезной нагрузкой нужен сопутствующий ему sidecar либо агент.

Более легковесная и быстрая технология — централизованная проверка запросов на подключение сессий в ядре Linux на узле Kubernetes с помощью технологии eBPF. Однако, не зная броду, здесь легко напороться на массу подводных камней.

Спикер расскажет, как его команда из «Лаборатории Касперского» путешествовала по реке сетевых данных, лавировала в ней, а в итоге совершила глубоководную охоту и обуздала eBPF.

Доклад будет полезен всем, кто занимается или планирует нырять в тему защиты Kubernetes (то есть буквально каждому), а также сочувствующим на берегу

Сложность: medium

14:00–15:00

Охота на краснокнижного мусанга

Наталья Шорникова
Ведущий аналитик разведки киберугроз,
«Лаборатория Касперского»

Андрей Гунькин
Старший вирусный аналитик MDR-сервиса,
«Лаборатория Касперского»

Спикеры расскажут об APT-группе ToddyCat, которая проводила шпионские атаки на государственные учреждения в странах Юго-Восточной Азии и в Российско-Евроазиатском регионе. Подробно разберут инструменты, используемые этой группой для доступа к удаленной инфраструктуре и шпионажа, а также опишут способы их детектирования в инфраструктуре

Сложность: hard

15:00–16:00

Грозовые облака: расследования инцидентов в облачных инфраструктурах

Антон Степанов
Ведущий специалист по компьютерной криминалистике,
BI.ZONE

Докладчик расскажет об опыте расследований в облачных инфраструктурах.

Тренд сезона — атаки типа trusted relationships. А что, если атаковать провайдера облачных услуг и получить доступ к клиентским консолям администрирования или гипервизорам? В этом случае задача получения доступа к клиентским данным сильно упрощается.

У команды докладчика было несколько кейсов с расследованиями, где оказались скомпрометированы именно провайдеры облачных услуг. Докладчик расскажет об особенностях расследований, об узких местах и сложностях, с которыми столкнулась команда. Поделится мнением о том, как детектировать такие атаки и что делать клиентам облачных провайдеров для уменьшения рисков компрометации

Сложность: medium

16:00–17:00

Обход защитного механизма V8 sandbox

Юрий Паздников
Младший специалист по тестированию, BI.ZONE

V8 sandbox — новый защитный механизм JavaScript-движка, используемого в браузерах, основанных на Chromium. В докладе описан способ обхода этого защитного механизма с помощью найденной уязвимости, а также новая техника эксплуатации

Сложность: hard

17:00–18:00

All-in-one REST API: безопасность, инструментарий и полезные советы

Валентин Мамонтов
Инженер по безопасности приложений, Swordfish Security

Докладчик разберет возможности использования open-source-инструментов для защиты OpenAPI-спецификации и ее роль в безопасности API

Сложность: medium

18:00–18:30

Закрытие

23 августа, пятница — Fast track

10:00–10:30

MPoS'tor: компрометация мобильного PoS-терминала

Георгий Хоруженко
Независимый исследователь ИБ

В работе представлены результаты анализа системы offline-оплаты, центральным элементом которой является мобильный терминал (mobile PoS). В частности, представлен метод удаленной компрометации терминала (посредством протокола Bluetooth), который приводит к возможности перехвата данных платежных карт пользователей

Сложность: hard

10:30–11:00

Заблокирован, но не сломлен: горизонтальное перемещение после блокировки пользователя в AD

Владислав Воробьев
L2-аналитик SOC, «Информзащита», IZ:SOC

Спикер расскажет, почему блокировка пользователя может не остановить его дальнейшее продвижение в инфраструктуре и какие средства борьбы стоит применять

Сложность: medium

11:00–11:30

Одно кольцо, чтоб миром править: анализ архитектуры и исследование механизмов безопасности умного кольца QRing R02

Григорий Пагуба
Научный сотрудник, Институт компьютерных наук и кибербезопасности Санкт-Петербургского политехнического университета Петра Великого

В докладе будет описан процесс проведения исследований аппаратной части и прошивки умного кольца QRing R02, а также связанного с ним приложения для ОС Android с точки зрения информационной безопасности и опыт патчинга прошивки кольца

Сложность: easy

11:30–12:00

(Не)безопасность устройств интернета вещей на примере небольшого исследования одного мультипротокольного USB-модема

Иван Зорин
Независимый исследователь

Несмотря на громкие инциденты вокруг таких IoT-ботнетов, как Mirai, до сих пор существует огромное количество устройств, безопасность которых оставляет желать лучшего. А при определенных навыках и некоторой удаче небезопасное устройство и само можно превратить в вектор атаки на другие устройства. При этом вовсе не обязательно обладать глубочайшими навыками аппаратного анализа и обратной разработки.

Доклад предназначен для широкого круга специалистов, интересующихся темой безопасности встраиваемого ПО, и представляет собой одно из исследований аппаратного устройства программными средствами, в рамках которого приводятся основы изучения ПО современных устройств на базе операционных систем семейства GNU/Linux

Сложность: medium

12:00–12:30

Сетевой фингерпринт на скорости канала

Руслан Трифонов
Младший разработчик, CyberOK

Automated network fingerprint, готовые решения для поиска продуктов и протоколов

Сложность: medium

12:30–13:00

Одна атака у водопоя, чтоб править всеми

Георгий Кумуржи
Независимый исследователь

Спикер поможет слушателям посмотреть на тему проведения атак у водопоя свежим взглядом. На примерах разберет, какие преимущества может получить злоумышленник в результате внедрения вредоносного JS-кода в легитимные сервисы организации, а вишенкой на торте станет подробный разбор cyber kill chain, позволяющего в несколько шагов закрывать большинство pentest- и red team — проектов

Сложность: medium

13:00–13:30

LOLApps — подножный корм хакера

Кирилл Магаськин
Младший специалист по расследованию компьютерных инцидентов, «Лаборатория Касперского»

Доклад посвящен необычным способам использования легитимных приложений в атаках, обнаруженных в ходе расследования инцидентов

Сложность: medium

13:30–14:00

Почему важно писать собственные правила SAST и как это делать правильно

Артур Сакольчик
Application Security, Positive Technologies

Статический анализ кода является важной практикой в обеспечении безопасности и качества программного обеспечения. Однако использования стандартных правил, предлагаемых большинством SAST-инструментов, не всегда достаточно для выявления всех возможных уязвимостей и проблем, специфичных для конкретного проекта или организации.

Внедрение собственных правил на SAST-инструмент становится неотъемлемой практикой, поскольку позволяет учитывать уникальные требования, архитектурные особенности и бизнес-логику приложения

Сложность: easy

14:00–14:30

Скрытые ловушки в яблочном раю: раскрывая угрозы macOS

Ирина Колягина
Ведущий специалист по анализу киберугроз, BI.ZONE

Спикер кратко опишет методы обхода встроенных механизмов безопасности macOS и новые способы обнаружения угроз

Сложность: medium

14:30–15:00

Ломаем «Битрикс» через мобилку: как мобильные приложения помогают пробить инфраструктуру заказчика

Александр Ларин
Специалист по тестированию на проникновение, «Ти Хантер»

Как взломать веб-приложение, используя альтернативные каналы аутентификации? Об этом и расскажет докладчик и приведет реальный пример, как при пентесте одного веб-приложения от «полного ничего» его команда получила «полное все», используя уязвимости в мобильном приложении и немного OSINT.

Помимо этого, спикер опишет еще несколько примеров из своей практики, когда мобильные приложения прямо или косвенно помогали компрометировать веб

Сложность: medium

15:00–15:30

IRonBRO — DIY-веб-изоляция для защиты от интернет-угроз

Николай Клендар
Независимый исследователь

Подавляющее число кибератак на организации происходит при использовании интернет-ресурсов. Встроенные в NGFW и Secure Web Proxy категоризаторы не успевают классифицировать сайты. Блокировка неизвестных ресурсов и работа в режиме белых списков повышают безопасность, но приводят к недовольству пользователей и снижению их продуктивности. Осложняет ситуацию использование end to end — шифрования, что не позволяет проводить антивирусную проверку и выявлять утечку информации даже с использованием TLS-инспекции.

В рамках доклада спикер рассмотрит решение, реализующее технологию веб-изоляции для защиты от интернет-угроз. Использование этой технологии позволяет решить проблему безопасного доступа к интернет-ресурсам, исключить возможность взаимодействия с командным центром управления зараженного компьютера и передачу опасного содержимого на компьютер пользователя

Сложность: easy

15:30–16:00

Инфильтрация и эксфильтрация данных через RDP в ходе пентеста

Денис Душенев
Заместитель начальника отдела защищенности по инфраструктурному тестированию, Compliance Control

Иногда во время проведения пентеста мы подключаемся к удаленному серверу по RDP. Если сервер имеет высокий уровень защищенности, то обычные методы копирования файлов на сервер / с сервера не будут работать. Спикер рассмотрит способ передачи данных с помощью клавиатурного ввода и отображения рабочего стола. Также слушатели узнают о возможных способах обнаружения таких методов передачи файлов

Сложность: medium

16:00–16:30

From source maps to secrets

Егор Боровинских
Ведущий специалист по информационной безопасности, ООО «Веблок»

Разработчики все чаще стали оставлять открытые source maps в своих веб-приложениях. Благодаря этому любой пользователь может просмотреть исходный код в его первозданном виде. Что же могло пойти не так?

Сложность: medium

16:30–17:00

SBOM в SIEM для реагирования на инциденты и защиты облачной инфраструктуры

Алексей Вишняков
Старший инженер DevSecOps, «Яндекс Облако»

Спикер расскажет о том, какую информацию о сборках следует хранить в SBOM, а также о вызовах и преимуществах отправки SBOM в SIEM-систему.

Доклад будет посвящен тулингу CycloneDX для генерации SBOM, обогащению его недостающими метаданными о сборке и артефактах, контролю целостности приложений (FIM), поиску уязвимостей в сторонних компонентах (SCA), помощи SBOM в реагировании на инциденты кибербезопасности и вызовам внедрения контролируемых сборок в компании «Яндекс Облако»

Сложность: medium

17:00–17:30

Что делать, если не знаешь, что делать, или Пентест диалекта ISO 8583

Юрий Бычук
Специалист по тестированию на проникновение, Compliance Control

Павел Попков
Специалист по тестированию на проникновение, Compliance Control

Опыт проведения пентеста неизвестного диалекта спецификации ISO 8583

Сложность: medium

17:30–18:00

Новый инцидент, или Как я снова встретил MikroTik

Владислав Азерский
Ведущий специалист по реагированию на инциденты и цифровой криминалистике, F.A.C.C.T.

Ни для кого не секрет, что в ходе проведения атак злоумышленники перемещаются по сети не только на рабочие станции IT-администраторов или контроллеры домена, но и на сетевое оборудование. В докладе будет представлен разбор инцидента кибербезопасности, связанного с MikroTik. Также спикер рассмотрит различные гипотезы по проверке сетевых устройств MikroTik на факт компрометации

Сложность: easy

23 августа, пятница	Threat.Zone

10:00–10:20

Mind the intelligence gap

Олег Скулкин
Руководитель управления кибербразведки, BI.ZONE

Мы постоянно сталкиваемся с белыми пятнами — видим только часть целого. От этого нельзя избавиться полностью, но мы можем побороться. Самое время начать!

Сложность: easy

10:20–11:10

Это не проблема, это расходы: как теневые ресурсы помогают злоумышленникам реализовывать целевые атаки

Дарья Себякина
Старший продуктовый маркетолог, BI.ZONE

В атаках на российские компании часто используется не только самописное, но и коммерческое вредоносное ПО, которое можно купить на теневых ресурсах по подписке с включенным сервисным обслуживанием и регулярными обновлениями. Зачастую разработчики таких программ запрещают использовать их для атак территории РФ, однако в последнее время это правило неоднократно нарушалось.

Здесь же, на теневых форумах и в чатах, можно встретить объявления по продаже первоначальных доступов в корпоративные сети, а также предложения о помощи в реализации дальнейших этапов целевых атак.

Означает ли это, что реализовать атаку можно, даже не обладая серьезными техническими навыками? Спикер разберет этот вопрос в рамках доклада, посвященного коммерческому вредоносному ПО, которое используют в целевых атаках на российские компании.

Слушатели узнают, какие задачи нужно решить злоумышленнику, чтобы реализовать атаку, и каким образом можно получить необходимые инструменты для проведения атаки. В конце Дарья приведет примеры коммерческого вредоносного ПО для реализации атак

Сложность: easy

11:10–12:00

Ничего киберкриминального

Полина Бочкарева
Специалист по анализу данных об угрозах, BI.ZONE

Хактивизм уже давно стал способом донесения своей позиции до мирового сообщества. Однако начиная с 2022 года подобные атаки обрели новую форму, когда действия злоумышленников не подвергаются осуждению или преследованию, а, наоборот, одобряются и порой даже поддерживаются на государственном уровне. Доклад будет посвящен обзору «взлома как заявления» и хактивизму как явлению последних нескольких лет в отношении организаций отечественных и СНГ. Будут разобраны основные группы, которые принимали участие в атаках, их мотивы, способности и какие методы донесения своей правды и идей они использовали

Сложность: easy

12:00–12:50

Вымогатели для самых маленьких

Лада Антипова
Руководитель отдела реагирования и цифровой криминалистики, Angara Security

Программы-вымогатели по-прежнему остаются большой головной болью для всех, от малого бизнеса до крупных корпораций.

В то время как 2022 и 2023 годы ознаменовались началом повсеместного использования шифровальщиков, исходный код которых был опубликован в сети, с точки зрения малого и среднего бизнеса начал наблюдаться существенный рост случаев заражения малоизвестными штаммами программ-вымогателей. Некоторые из них пропадают с радаров буквально после нескольких атак, а некоторые остаются на более долгий срок: им и посвящен доклад.

Слушатели узнают про первопричины, действия злоумышленников на постэксплуатационном этапе и о том, какие меры для расследования и восстановления нужно принять в первую очередь, а чего делать точно не следует

Сложность: easy

12:50–13:40

Липучий случай: разбираем атаки группировки Sticky Werewolf

Дмитрий Купин
Руководитель отдела по анализу вредоносного кода департамента кибербразведки, F.A.C.C.T.

Доклад посвящен исследованию кибершпионской группировки Sticky Werewolf. В нем представлены цели атак, таймлайн, инструменты, инфраструктура, TTPs и атрибуция

Сложность: medium

13:40–14:30

Взлом через MS Exchange — это не только про уязвимости, или История одной атаки

Алина Суханова
Старший специалист по расследованию компьютерных инцидентов, «Лаборатория Касперского»

Доклад посвящен опыту непростого расследования с неожиданным финалом. Обсудим, какие тактики и техники использовали злоумышленники в зафиксированной атаке, как OSINT помог им в получении первоначального доступа, а также с какими трудностями пришлось столкнуться при исследовании их активности

Сложность: medium

14:30–15:20

Linux endpoint detection: актуальные угрозы и методы обнаружения

Гаго Минасян
Аналитик группы хостового обнаружения, Solar 4RAYS

Linux-угроз становится больше, а с учетом тренда на импортозамещение важность задачи по эффективной защите от них растет. Спикер разберет основные угрозы, которые его команда встречала в реальных расследованиях, и опишет подходы к их эффективному обнаружению

Сложность: medium

15:20–16:10

Путешествие по извилистым тропам: маневры ExCobalt в атаках на российские компании в 2023 и 2024 годах

Владислав Лунин
Старший специалист группы исследования сложных угроз, Positive Technologies

Александр Бадаев
Специалист группы кибербразведки экспертного центра безопасности, Positive Technologies

Спикеры расскажут, как обнаружили разные векторы атак группы ExCobalt на российские компании из различных секторов и какие способы получения первоначального доступа использовала эта группа: фишинг, эксплуатацию таких уязвимостей, как CVE-2023-38831 и CVE-2023-3519, а также supply chain и trusted relationship.

Слушатели узнают об использовании группой ExCobalt руткина Facefish, а также об обширной инфраструктуре злоумышленников. Помимо инфраструктуры злоумышленников, спикеры поговорят об обнаружении на открытых директориях злоумышленников новых вредоносных инструментов, модифицированных стандартных утилит для Linux, а также о бэкдоре GoRed версии v0.0.1.

Кроме того, доклад включает раскрытие особенностей всех найденных версий GoRed и его связей с группировкой ExCobalt

Сложность: medium

16:10–17:00

Инструменты атакующих в 2023 и 2024 годах

Семён Рогачев
Руководитель отдела реагирования на инциденты, ООО «Бастион»

В своем докладе спикер разберет инструменты, которые атакующие использовали в атаках на Linux- и Windows-инфраструктуру и которые наиболее часто встречались в ходе реагирования на инциденты в России. Речь пойдет не только о вредоносных инструментах. В конце доклада спикер даст рекомендации по их обнаружению и анализу

Сложность: medium

17:00–18:00

Пивнельная дискуссия: как изменился ландшафт угроз России в 2024 году

Модератор:
Олег Скулкин
Руководитель управления кибербразведки, BI.ZONE

Елена Шамшина
Руководитель департамента кибербразведки, F.A.C.C.T.

Кирилл Митрофанов
Руководитель команды аналитики разведки киберугроз, «Лаборатория Касперского»

Игорь Залевский
Руководитель исследовательского центра, Solar 4RAYS

Денис Кувшинов
Руководитель департамента threat intelligence, PT ESC

В рамках панельной дискуссии представители различных компаний, специализирующихся на кибербезопасности, обсудят тренды и рассмотрят изменения локального ландшафта угроз в 2024 году

23 августа, пятница — Community track

10:00–10:20

LockPick: сим-сим, откройся!

ostara
Независимый исследователь

Zaf0d
Независимый исследователь

Слушатели узнают об истории и культуре lock picking, параллелях с кибербезопасностью, а также смогут решить небольшую головоломку

Сложность: medium

10:20–11:00

Береги ключи от незнакомцев!

Scan87
Пентестер

Ключ и замок давно стали одними из самых узнаваемых символов безопасности. Про замки было сказано уже очень многое, так что в этот раз доклад будет преимущественно о ключах. Мы дорожим ими, любим их и боимся потерять. Однако потерять ключ — это не самое страшное, что может случиться...

Спикер расскажет про техники, используемые во время физического пентеста для проведения атак на ключи. Будут рассмотрены восстановление по фотографии, способы декодирования и изготовления дубликатов. Речь пойдет о ключах к английским, перфорированным и дисковым замкам, а также будет затронута тема безопасности RFID-карт. Спикер поделится историями из практики, эпичными неудачами и вынесенными уроками

Сложность: medium

12:00–13:00

Сотни, а может быть, даже тысячи багхантеров

Юрий Ряднина
Старший специалист по анализу защищенности банковских систем, Positive Technologies

Веселый доклад про канал «Багхантер», комьюнити и багбаунти. Слушателей ждут мемы, истории, планы, секреты и лайфхаки, а также итоги работы стенда Юрия на OFFZONE — райтап о его конкурсе. Спикер расскажет простым языком про сложные детали

Сложность: medium

13:00–14:00

Безопасность мобильных приложений: что нового в 2024 году?

Юрий Шабалин
Генеральный директор, «Стингрей Технолоджиз»

Спикер расскажет о наиболее значимых уязвимостях и новостях в мобильной безопасности. Рассмотрит новые векторы атак, классные баги и опишет интересные ошибки, найденные в приложениях за последние полгода

Сложность: medium

14:00–15:00

OSINT как образ мышления

Dukera
Co-founder, OSINT mindset

Спикер опишет решение задач OSINT, а также покажет, что методология OSINT может быть полезна не только в профессиональной сфере, но и в обычной жизни

Сложность: medium

15:00–15:30

Протестую! Дилеммы в триаже уязвимостей

Петр Уваров
Руководитель направления Bug Bounty, VK

Триаж уязвимостей для многих — это черный ящик, внутри которого скрыты сложные процессы и механизмы. Понять, как он функционирует, лучше всего на примерах. Слушатели доклада узнают, как построен триаж уязвимостей в VK, какие сложные и неоднозначные ситуации возникают, удается ли с ними справляться и к чему это порой приводит. Багхантерам будет полезно узнать «внутреннюю кухню» вендора, чтобы лучше понимать скрытые процессы и выстраивать эффективную коммуникацию с триажерами

Сложность: easy

16:00–16:30

Pentester's tales

Михаил Дрягунов
Penetration tester, Team Lead at Digital Security

Спикер расскажет несколько историй из практики:

- о звонках спамеров после посещения сайта;
- о расшифровке BitLocker с помощью логического анализатора;
- о том, как получить RCE на кассе самообслуживания, просканировав пару штрихкодов

Сложность: medium

16:30–17:30

PHP 8+. Сага о бэкдорах

Mark_Tauber
Независимый исследователь

В ходе доклада обсудим следующие моменты:

- Что поменялось и с чем возникли проблемы?
- Захват сервера одной строкой. Возможно ли в новых условиях?
- Справляемся с новыми проблемами старыми решениями.
- Защищаемся: ради приличия рассмотрим основные способы защиты и поговорим о предотвращении атак

Сложность: hard

23 августа, пятница — AppSec.Zone

10:00–11:00

Защита от манипуляции временем транзакции в блокчейне Hyperledger Fabric

Игорь Агиевич
Независимый исследователь

О практической безопасности блокчейна Hyperledger Fabric не так много общедоступной информации. При этом блокчейн активно используется уже довольно давно в разных сферах, в том числе в области цифровых финансовых активов.

Доклад посвящен атаке манипуляции временем транзакции и финансовым последствиям на примере концепта уязвимого смарт-контракта, имитирующего цифровой финансовый актив.

Спикер представит свое open-source-решение для защиты от атаки, разработанное на основе клиента NTP-/NTS-серверов и устойчивое к атаке «человек посередине». Это решение могут использовать разработчики смарт-контрактов Hyperledger Fabric вместо самостоятельной защиты от манипуляции временем

Сложность: hard

11:00–12:00

Каскадная AI-валидация дефектов кода

Анна Архипова
Ведущий менеджер по развитию бизнеса, IITD Group

Спикер расскажет о повышении качества работы инструментов статического анализа кода за счет AI-валидации дефектов на основе графового представления сквозных векторов уязвимостей.

В рамках доклада будут рассмотрены следующие темы:

- Проблематика триажа.
- Корреляция дефектов на основе выявления точек пересечения сквозных векторов с использованием графового анализа.
- Подход к минимальному объему метаданных об уязвимости в коде, необходимому для корректной оценки дефектов AI-моделью.
- Алгоритм каскадной AI-валидации дефектов.
- Эффективность и преимущества подхода

Сложность: hard

12:00–13:00

Больше никакой халявы! Интересные баги в e-food-приложениях

Егор Тахтаров
Пентестер, CICADA8

В докладе рассмотрены баги, найденные в программах вознаграждения у вендоров, основная сфера деятельности которых — e-grocery

Сложность: easy

13:00–14:00

Как я «Капсулу Нео» от VK взломал

Владимир Кононович
Старший инженер по обратной разработке, BI.ZONE

Доклад затрагивает практически полный процесс реверс-инжиниринга умной колонки от VK под названием «Капсула Нео» — с момента получения устройства до написания отчета. Также спикер раскроет некоторые особенности реверса IoT. Доклад рассчитан на любую аудиторию (в том числе без знаний в RE)

Сложность: hard

14:00–15:00

Доктор для Docker, или Построение процесса управления уязвимостями в Docker-образах: от исправления до доставки в продакшен

Александр Трифанов
Тех и этих лид, «Авито»

Спикер расскажет о том, как настроили сканирование, верификацию и патчинг Docker-образов, приоритизировали и группировали уязвимости, доставляли фиксы в продакшен и что из всего этого получилось

Сложность: medium

15:00–16:00

Поиск активов и управление риском в коде продуктов

Дмитрий Марюшкин
Руководитель группы продуктовой безопасности, Ozon Fintech

Спикер расскажет, из каких компонентов состоит стереотипный микросервис в продукте и какие уязвимости связаны с этими компонентами, как влияют на общий уровень риска количество и структура объектов, обрабатываемых в API сервиса, хранимых в БД или получаемых в методах клиентов других сервисов, как быстро вынуть из кода структуру этих объектов с помощью правил semgrep и сохранить для последующей аналитики, как прислонить к извлеченной структуре градусник, а также как и где можно использовать извлеченные данные и измеренную температуру

Сложность: medium

16:00–17:00

ApiSecurity 101

Александр Чикайло
Ведущий специалист группы экспертизы защиты приложений, Positive Technologies

Безопасность API — критически важная часть современного ПО. Спикер разберет различные атаки и уязвимости, нацеленные на web API, а также расскажет, как от них защититься

Сложность: medium

17:00–17:25

EPSS: еще один способ приоритизации уязвимостей

Артём Кадушко
Head of Application Security

Слушатели узнают, насколько эффективна EPSS (exploit prediction scoring system) для приоритизации уязвимостей, а также в чем ее плюсы, минусы и отличия от классических способов

Сложность: medium

17:25–17:50

SCA & SAST: курс на автоматизацию триажа

Виталий Гулин
Ведущий инженер по информационной безопасности, ПАО «Ростелеком»

Одна из главных головных болей специалиста по безопасности приложений — разбор срабатываний разнообразных анализаторов уязвимостей, или триаж.

Спикер расскажет, какие есть способы решения этой проблемы. Он рассмотрит методики, которые опробовала его команда, расскажет, с какими трудностями они столкнулись и к каким выводам пришли.

А в конце доклада вас ждут рассуждения о том, насколько целесообразно использование искусственного интеллекта в контексте снижения нагрузки на AppSec-специалистов

Сложность: easy

17:50–18:00

Награждение командой BI.ZONE Bug Bounty победителей и призеров ивента BUGS ZONE 2.0 вместе с VK, «Т-Банком», CICADA8, МТС и «Купером»

23 августа, пятница Workshops

11:00–14:00

Malware persistence techniques: помогаем синим командам в расследовании киберугроз и в изучении популярных persistence-тактик, используемых при APT-атаках

Жасулан Жусупов
Сооснователь, MSSP Research LAB

Что будем делать

Изучим, как устроены различные техники и тактики malware persistence, а также как можно находить новые.

Продолжительность: 3 часа.

В программе

- Что такое malware persistence.
- User privileged techniques.
- Admin privileged techniques.
- Hunting for persistence: from zero to hero (с нуля до продвинутого уровня).

Что потребуется

- Linux (Ubuntu, Kali, Parrot OS);
- VirtualBox или VMWare (Windows 10, Windows 11, Process Hacker, Sysinternals Suite)

Сложность: medium/hard

14:30–17:30

Ломаем CI/CD 2.0

Павел Сорокин
Tech lead, Singleton Security

Что будем делать

Изучим работу с секретами в CI/CD и соответствующие проблемы. Научимся обходить защиты раннеров от PPE.

Продолжительность: 3 часа.

В программе

- Секреты в CI/CD: gitlab variables / vault.
- Интеграция Vault с GitLab и проблемы в ней.
- Интеграция Vault с K8s и проблемы в ней.
- Защита раннеров от poisoned pipeline execution и способы ее обхода.

Что потребуется

- docker;
- kubectl;
- vault (cli)

Сложность: medium

23 августа, пятница	Main track

18:00–18:30

Закрытие