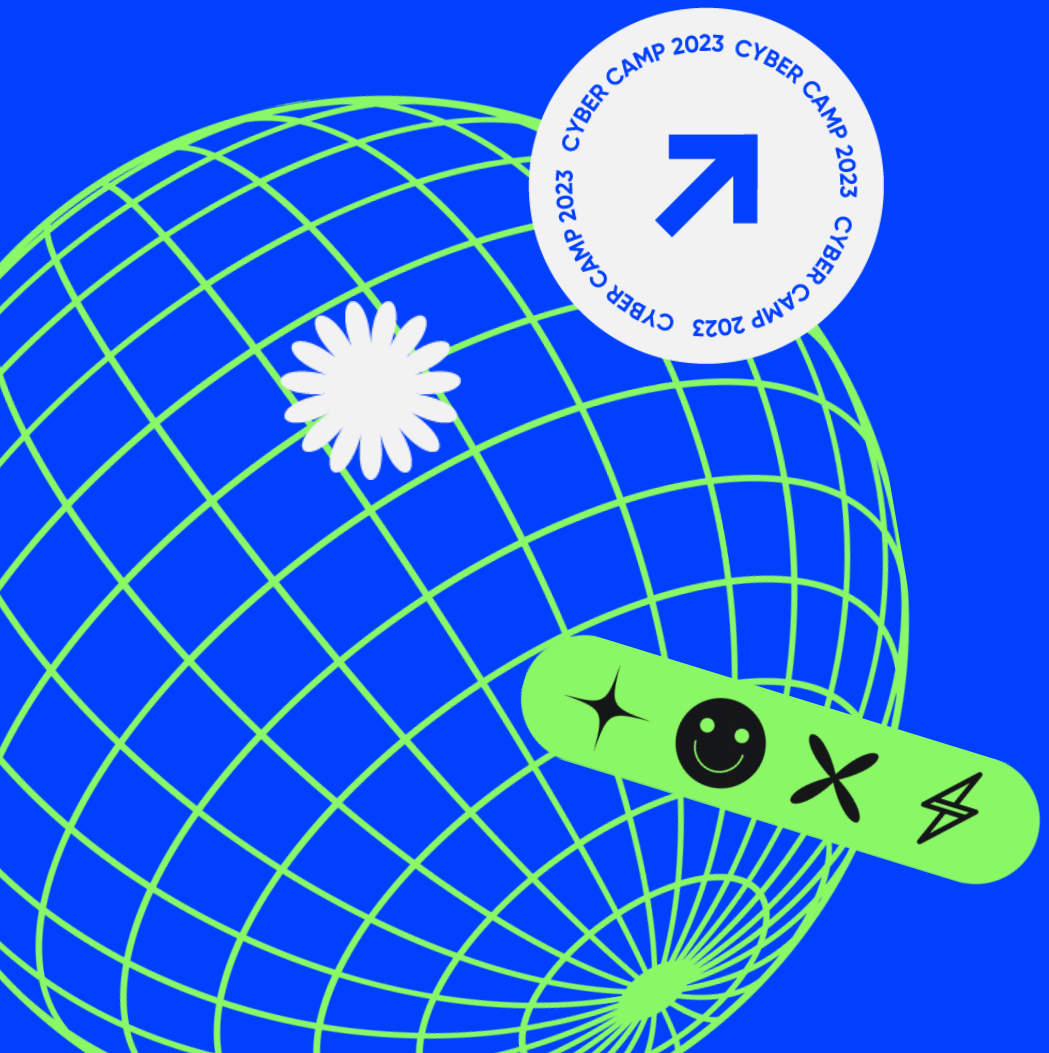
Cyber
Camp
2023



Рекомендации от спикеров

Cyber Camp 2023

Настройка аудита Windows: эффективное детектирование атак

Павел Иванов

Ведущий аналитик центра информационной безопасности, «Инфосистемы Джет»

Книги:

- Teymur Kheirkhabarov. Hunting For PowerShell Abuse

Ссылки:

- Audit Policy Recommendations: https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/audit-policy-recommendations
- Cheat Sheets to help you in configuring your systems: https://www.malwarearchaeology.com/cheat-sheets
- Windows 10 patch/upgrade security settings repair fix-it script: https://www.malwarearchaeology.com/logging
- blacklanternsecurity/blue-resources: https://github.com/blacklanternsecurity/blue-resources/blob/main/Windows_MITRE_Data_Source_Mapping.xlsx
- Параметры политики расширенного аудита безопасности (Windows 10): https://learn.microsoft.com/ru-ru/windows/security/threat-protection/auditing/advanced-security-audit-policy-settings
- Аудит процессов командной строки: https://learn.microsoft.com/ru-ru/windows-server/identity/ad-ds/manage/component-updates/command-line-process-auditing
- Microsoft eventlog mindmap: https://github.com/mdecrevoisier/Microsoft-eventlog-mindmap/tree/main
- Sysmon - DFIR: https://github.com/MHaggis/sysmon-dfir
- Understanding Sysmon Events using SysmonSimulator: https://rootdse.org/posts/understanding-sysmon-events/

Cyber Camp 2023

Как с помощью ML детектировать зловредную активность в зашифрованном трафике

Николай Лыфенко

Руководитель группы анализа трафика, Positive Technologies

Ссылки:

- Рассылка ИБ-новостей, есть раздел AI & Cybersecurity: https://tldrsec.com/
- Рассылка новостей в сфере AI: https://aiweekly.co/
- Сообщество Open Data Science: https://ods.ai/

Cyber Camp 2023

Как бороться с неизвестностью: анатомия таргетированной атаки

Алексей Шульмин

Эксперт по кибербезопасности, «Лаборатория Касперского»

Ссылки:

- Телеграм-чат, посвященный бизнес-продуктам «Лаборатории Касперского»: https://t.me/kss_b2b
- Раздел Analysis на Kaspersky Threat Intelligence Portal: https://opentip.kaspersky.com/

Cyber Camp 2023

TOP-10 криминалистических артефактов Windows при расследовании инцидентов

Артем Семагин

Ведущий аналитик киберкриминалистики центра информационной безопасности, «Инфосистемы Джет»

Книги:

- Brian Carrier. File System Forensic Analysis
- Harlan Carvey. Investigating Windows Systems
- Олег Скулкин. Incident Response Techniques for Ransomware Attacks

Ссылки:

- SANS Digital Forensics and Incident Response: https://www.youtube.com/@SANSForensics
- VMware Memory Forensics - Don't Miss This Important Detail: https://www.youtube.com/@13Cubed
- Awesome Forensics: https://github.com/cugu/awesome-forensics
- The DFIR Report: https://thedfirreport.com/
- Презентация от Trustwave SpiderLabs: https://defcon.org/images/defcon-19/dc-19-presentations/Lenik/DEFCON-19-Lenik-MAC(b)Daddy.pdf

Инструменты (free):

- Zimmerman Tools: https://github.com/EricZimmerman
- NirSoft: https://www.nirsoft.net/computer_forensic_software.html
- Belkasoft Live RAM Capturer: https://belkasoft.com/get
- The Sleuth Kit/Autopsy: https://www.autopsy.com/download/

Cyber Camp 2023

Резервное копирование как часть периметра защиты

Дмитрий Кострюков

Руководитель направления систем резервного копирования, «Инфосистемы Джет»

Ссылки:

- Обеспечение доступности данных и сервисов: показатели RPO, RTO и планирование SLA: https://habr.com/ru/company/veeam/blog/328068/
- Группа обсуждения СРК: https://t.me/RussianBackupUserGroup
- Митап по СРК: https://meetup.jet.su/page34153436.html
- Опыт построения крупных СРК: https://youtu.be/f3zUj6akJL0?si=MZy7fYMlkZDw61dt

Cyber Camp 2023

Переговоры, гормоны и цифровизация

Игорь Беляев

Партнер тренинговой компании, Sellwell

Книги:

- Ванесса ван Эдвардс.
  Наука общения. Как читать эмоции, понимать намерения и находить общий язык с людьми
- Роберт Чалдини.
  Психология влияния. Убеждай, воздействуй, защищайся

Инструменты DevSecOps в облачной среде

Евгений Парфенов
Архитектор облачной платформы, Yandex Cloud

Книги:

- Брюс Шнайер.
  Прикладная криптография
- Project Management Body Of Knowledge

Ссылки:

- Телеграм-канал платформы Yandex Cloud:
  https://t.me/yandexcloudnews

Cyber Camp 2023

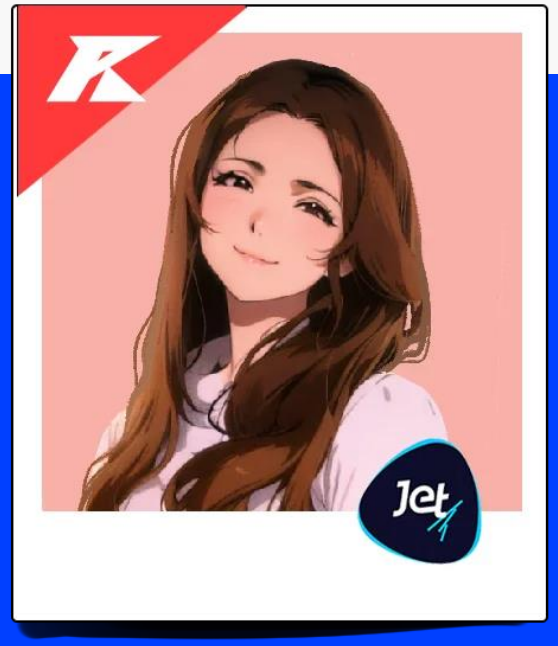
Как хакеры проходят периметр компании: опасное наследие

Георгий Старостин
CISO, АО «СОГАЗ»

Ссылки:

- Лабораторные для развития навыков ИБ и понимания способов атаки и защиты: hackthebox.com
- Обучение для интересующихся web-уязвимостями: https://portswigger.net/web-security
- Раскрытые отчеты Bug Bounty: hackerone.com

In-house фишинг: как делать хорошо



Екатерина Рудая
Менеджер продукта
Jet CyberCamp,
«Инфосистемы Джет»

Книги:

- Дэвид Линден.
  Мозг и удовольствия
- Дэвид Иглмэн.
  Живой мозг
- Максим Ильяхов.
  Пиши, сокращай: как создавать сильный текст
  (+ блог и другие книги)
- Даниэль Канеман.
  Думай медленно… Решай быстро

Cyber Camp 2023

All your bases are belong to us: актуальные методы, техники и утилиты для захвата AD

Лука Сафонов
Генеральный директор
ООО «Киберполигон»

Ссылки:

- RedTeam brazzers: https://t.me/RedTeambro
- Ralf Hacker Channel: https://t.me/RalfHackerChannel

Cyber Camp 2023

Как администрировать ИТ-инфраструктуру так, чтобы тебя не взломали

Борис Абрамов

Руководитель группы комплексной защиты информации центра информационной безопасности, «Инфосистемы Джет»

Ссылки:

- Securing privileged access: https://learn.microsoft.com/en-us/security/privileged-access-workstations/overview

Анатомия DDoS-атак на базе TCP, TLS и UDP

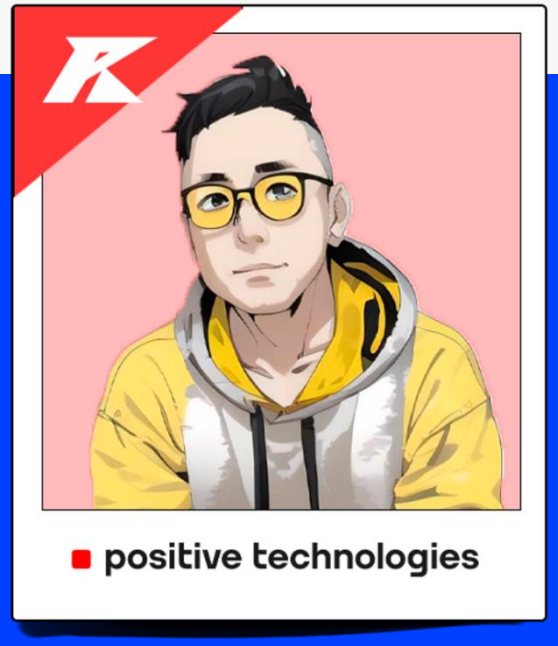
Георгий Тарасов
Менеджер продукта
Qrator.AntiBot, Qrator Labs

Ссылки:

- Панельная дискуссия конференции операторов связи региона Asia-Pacific — APRICOT 2022, обсуждение текущей ситуации с DDoS-атаками: https://youtu.be/NCzuiK5IgoA?si=CWsFC1lV110nOiaZ
- Совместное исследование Yandex и Qrator, посвященное ботнету Meris — источнику крупнейших прикладных DDoS-атак на текущий момент: https://habr.com/ru/companies/yandex/articles/577026/

Cyber Camp 2023

Заработай на чужих ошибках, или как стартовать в багхантинге



Дмитрий Ким
Бизнес-лидер направления Standoff365 Bug Bounty, Positive Technologies

Ссылки:

- Полезная информация и статьи для начинающих и опытных ребят. Контент собираем из своей экспертизы и опыта экспертов багхантинга: https://t.me/standoff_365
- Доклады от оффенсив-экспертов: https://m.youtube.com/@standoff365

Cyber Camp 2023

Не все подрядчики одинаково полезны: управление доверием

Александр Морковчин

Руководитель отдела развития консалтинга ИБ «Инфосистемы Джет»

Ссылки:

- Обзор от ENISA, июнь 2023 года: https://www.enisa.europa.eu/publications/good-practices-for-supply-chain-cybersecurity
- How Top CISOs Are Transforming Third-Party Risk Management, RSAC ESAF 2023 https://www.rsaconference.com/library/blog/rsac-esaf-cisos-transforming-third-party-risk
- Телеграм-канал «ИБ на полшестого»: https://t.me/sesyrity

Защита АСУ ТП: специфика и тенденции

Сергей Крылов
Эксперт центра информационной безопасности, «Инфосистемы Джет»

Ссылки:

- Безопасность АСУ ТП. Вводный курс: https://stepik.org/course/14905/promo
- Энциклопедия АСУ ТП: https://www.reallab.ru/bookasutp/

Cyber Camp 2023

Как безопасно презентовать безопасность

Кирилл Анастасин

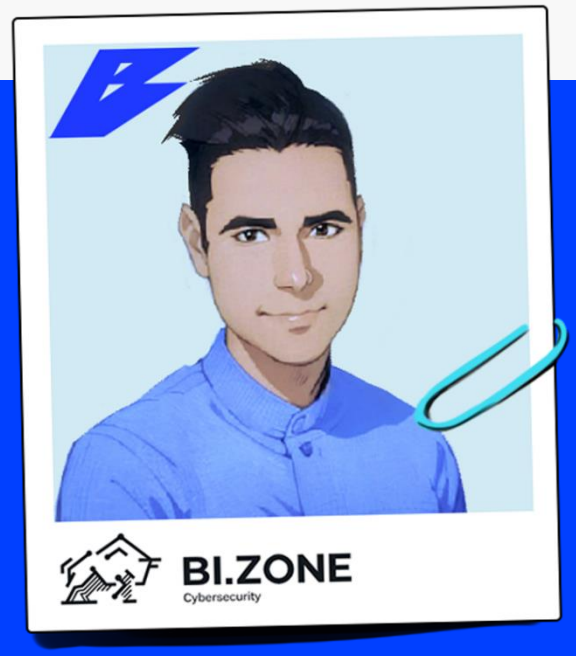
Дизайнер, художник, продюсер презентаций, автор проекта «Комикаки»

Книги:

- Крис Восс.
  Договориться не проблема.
  Как добиваться своего без конфликтов
  и ненужных уступок

Cyber Camp 2023

Бой с тенью: как кибербразведка помогает сократить время реагирования на инцидент



Олег Скулкин

Руководитель управления кибербразведки, BI.ZONE

Книги:

- Threat Intelligence and Me: A Book for Children and Analysts: https://www.amazon.com/Threat-Intelligence-Me-Children-Analysts/dp/1541148819

Ссылки:

- FOR578: Cyber Threat Intelligence: https://www.sans.org/cyber-security-courses/cyber-threat-intelligence/
- Operationalizing Threat Intelligence: A guide to developing and operationalizing cyber threat intelligence programs: https://www.amazon.com/Operationalizing-Threat-Intelligence-operationalizing-intelligence/dp/1801814686
- Practical Threat Intelligence and Data-Driven Threat Hunting: A hands-on guide to threat hunting with the ATT&CK™ Framework and open source tools: https://www.amazon.com/Practical-Threat-Hunting/dp/1838556370
- Intelligence-Driven Incident Response: Outwitting the Adversary 2nd Edition: https://www.amazon.com/Intelligence-Driven-Incident-Response-Outwitting-Adversary/dp/109812068X

Cyber Camp 2023

Чертоги оперативной памяти: как проанализировать то, что пока не забыто

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

Книги:

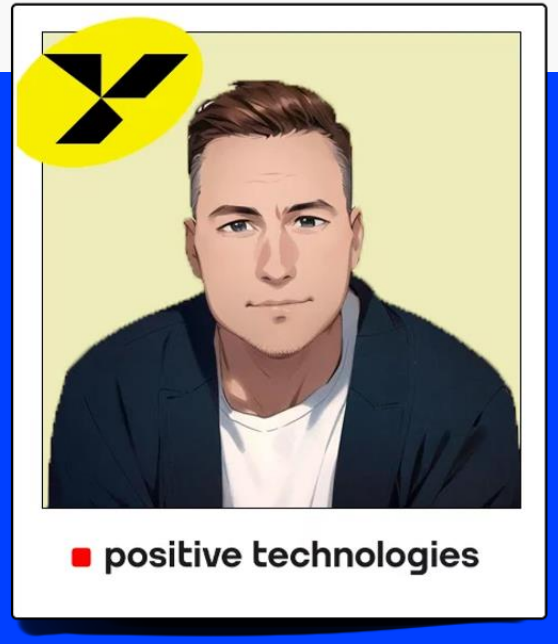
- Andrew Case, Aaron Walters, Jamie Levy, Michael Hale Ligh.
  The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory
- Svetlana Ostrovskaya, Oleg Skulkin.
  Practical Memory Forensics: Jumpstart effective forensic analysis of volatile memory (есть перевод на русский язык)

Ссылки:

- Задания по анализу образов памяти: https://cyberdefenders.org/

Cyber Camp 2023

Плагины IDE для безопасной разработки



Лев Новоженин
Инженер внедрения
и пилотирования продуктов
AppSec, Positive Technologies

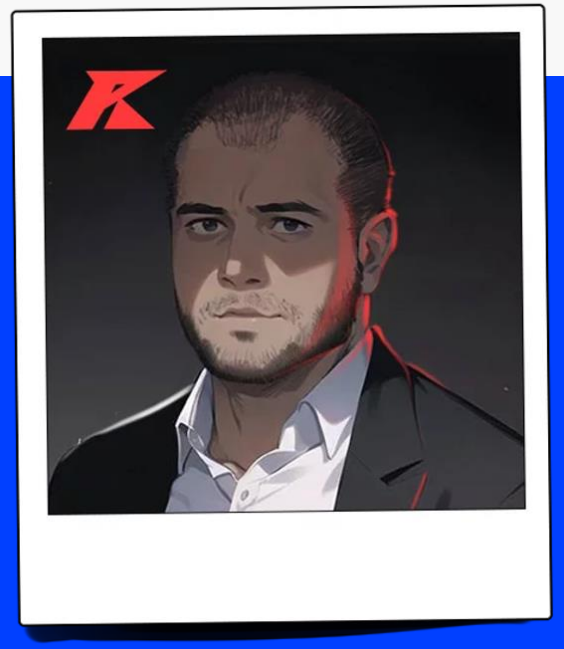
Книги:

- Таня Янка. Безопасность веб-приложений. Исчерпывающий гид для начинающих разработчиков
- Michal Zalewski. The Tangled Web: A Guide to Securing Modern Web Applications 1st Edition
- Майкл Ховард, Дэвид Лебланк. Защищенный код
- Dafydd Stuttard, Marcus Pinto. The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws 2nd Edition
- Дэн Берг Джонсон, Дэниел Савано, Дэниел Деоган. Безопасно by Design
- Брюс Шнайер, Нильс Фергюсон. Практическая криптография

Ссылки:

- Positive Development Community: https://t.me/POSIdev

Пентест: по ту сторону баррикад



Саид Эфендиев
Независимый эксперт

Ссылки:

- Dered: https://t.me/dered_team
- RedTeam brazzers: https://t.me/RedTeambro
- Ralf Hacker Channel: https://t.me/RalfHackerChannel
- Offensive Twitter: https://t.me/OffensiveTwitter
- xakep.ru
- mdsec.co.uk
- mgeek.tech

Безопасность в облаке не за миллион долларов

Александр Матвиенко
Руководитель группы защиты от утечек информации центра информационной безопасности, «Инфосистемы Джет»

Книги:

- Кевин Митник.
  Искусство обмана. Искусство вторжения. Искусство быть невидимым.

Ссылки:

- Телеграм-канал SecAtor:
  https://t.me/true_secator

Counter-OSINT при проведении пентеста

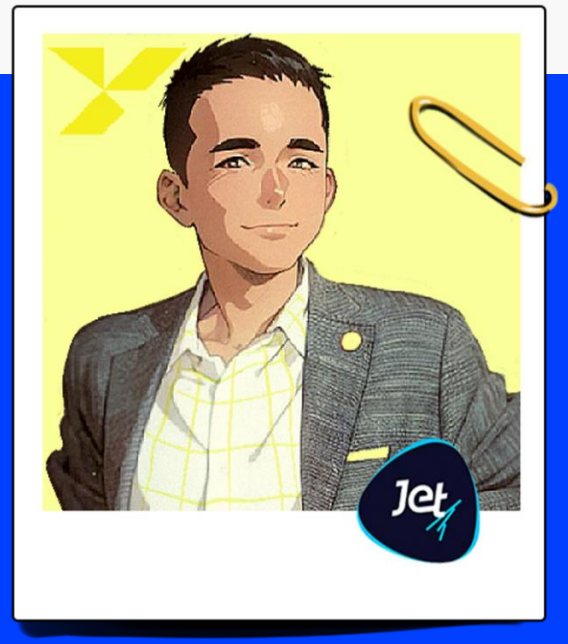
Dukera
Сообщество OSINT Mindset

Ссылки:

- Counter-OSINT: руководство по приватности и защите своих данных в Сети: https://github.com/soxoj/counter-osint-guide-ru/tree/main
- Автостопом по анонимности в Интернете: https://whiteprime.github.io/thgtoa/

Cyber Camp 2023

Экскурсия по Software Supply Chain Security



Антон Гаврилов

Руководитель направления DevSecOps центра информационной безопасности, «Инфосистемы Джет»

Ссылки:

- Телеграм-канал об актуальном в мире DevSecOps: https://t.me/devsecops_weekly
- CI/CD Security — то, без чего DevSecOps не имеет смысла / Денис Якимов (Альфа-Банк) https://www.youtube.com/watch?v=UK9DXSeA7E4&t=1s
- Безопасность CI/CD / Алексей Федулаев (Bimeister), Андрей Моисеев (ИнфоТеКС) https://www.youtube.com/watch?v=7owmOSg-mHA

Cyber Camp 2023

Телеграм-канал CyberCamp:
https://t.me/CYBERCAMP_ONLINE