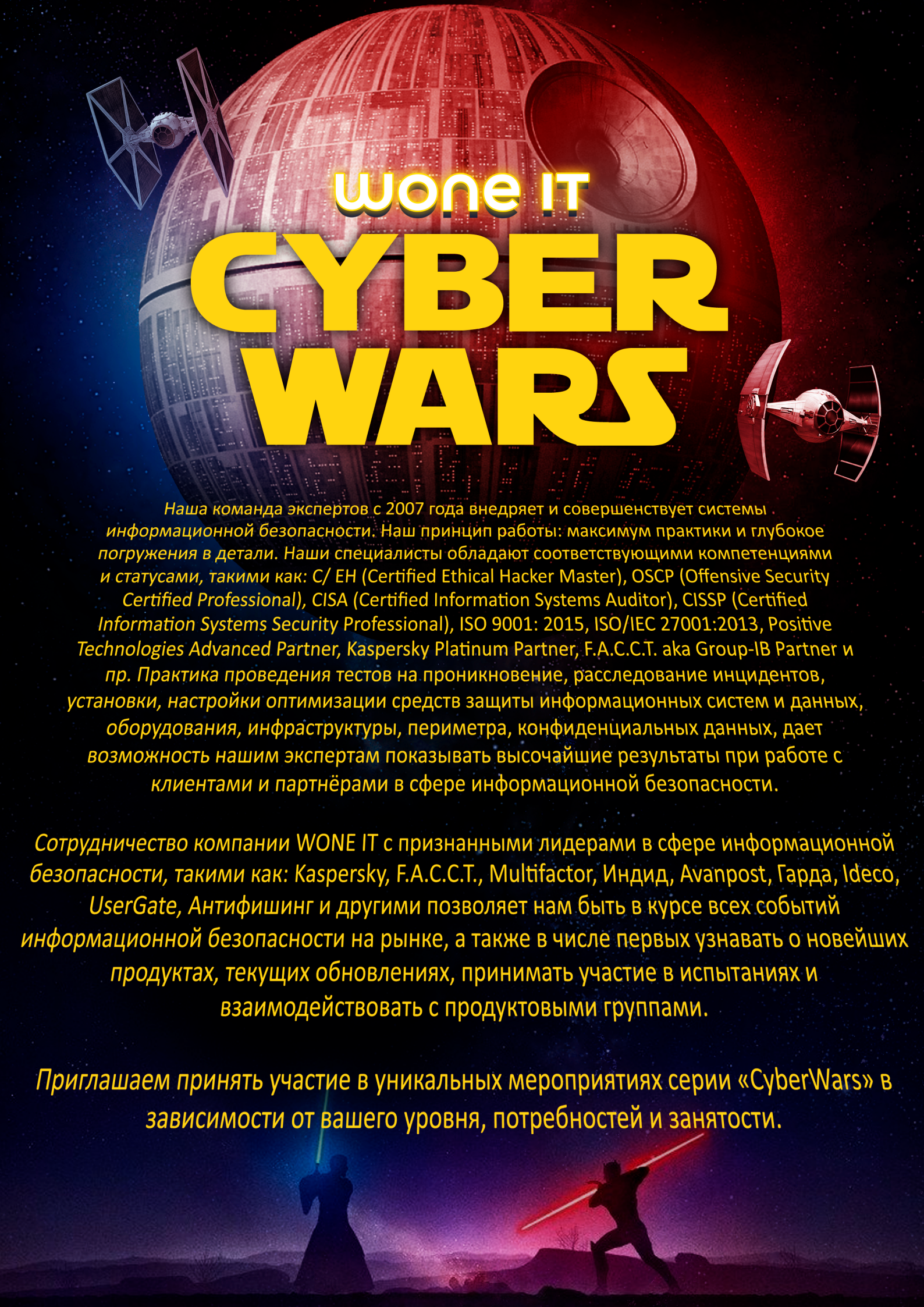

Наша команда экспертов с 2007 года внедряет и совершенствует системы информационной безопасности. Наш принцип работы: максимум практики и глубокое погружения в детали. Наши специалисты обладают соответствующими компетенциями и статусами, такими как: C/ EH (Certified Ethical Hacker Master), OSCP (Offensive Security Certified Professional), CISA (Certified Information Systems Auditor), CISSP (Certified Information Systems Security Professional), ISO 9001: 2015, ISO/IEC 27001:2013, Positive Technologies Advanced Partner, Kaspersky Platinum Partner, F.A.C.C.T. aka Group-IB Partner и пр. Практика проведения тестов на проникновение, расследование инцидентов, установки, настройки оптимизации средств защиты информационных систем и данных, оборудования, инфраструктуры, периметра, конфиденциальных данных, дает возможность нашим экспертам показывать высочайшие результаты при работе с клиентами и партнёрами в сфере информационной безопасности.

Сотрудничество компании WONE IT с признанными лидерами в сфере информационной безопасности, такими как: Kaspersky, F.A.C.C.T., Multifactor, Индид, Avanpost, Гарда, Ideco, UserGate, Антифишинг и другими позволяет нам быть в курсе всех событий информационной безопасности на рынке, а также в числе первых узнавать о новейших продуктах, текущих обновлениях, принимать участие в испытаниях и взаимодействовать с продуктовыми группами.

Приглашаем принять участие в уникальных мероприятиях серии «CyberWars» в зависимости от вашего уровня, потребностей и занятости.

В ХОДЕ МЕРОПРИЯТИЙ ВЫ ПОЗНАКОМИТЕСЬ С РЕАЛЬНЫМИ ИНСТРУМЕНТАМИ ХАКЕРОВ, ТАКТИКАМИ И ПОДХОДАМИ ИХ ПРИМЕНЕНИЯ И ИСПОЛЬЗОВАНИЯ.

Вы познакомитесь с такими тактиками атаки как:

- Spoofing TCP/IP & UDP;
- IP spoofing;
- ARP spoofing;
- DNS Cache Poisoning;
- NetBIOS/NBNS spoofing;
- Referrer spoofing;
- Poisoning of file-sharing networks;
- Caller ID spoofing;
- E-mail address spoofing;
- GPS Spoofing;
- Voice Mail spoofing;
- SMS spoofing;
- Sniffing;
- Extension Spoofing;
- File Name Spoofing;
- Status bar / Link spoof;
- URL Bar Spoofing;
- Source Code Spoofing;
- IDN Clones;
- DDoS;
- ICMP-флуд;
- SYN-флуд;
- UDP-флуд;
- HTTP-флуд;
- MITM.

и иными, современными типами атак, включающими методы социальной инженерии и OSINT.

ВЫ ПОЗНАКОМИТЕСЬ С ТАКИМИ ИНСТРУМЕНТАМИ КАК:

- Nmap
- Fg Power DDOSER
- Shell Booters
- WildDDOS
- Intercepter-NG
- THC Hydra
- Wifi Crusher
- Sherlock
- Mimikatz
- NoSQLMap
- Python CMC Бомбер
- HashCat
- Metasploit

Вы узнаете о вирусологии, каким образом, кто и какие вирусы может доставить на Ваши устройства и корпоративные сети: Вирусы, Loaders, Stillers, Miners, Coinhive, MAAS, XSS, Clippers, RAT, HVNC, Keyloggers, Ransomware и другие популярнейшие инструменты и устройства, применяемые в реальных атаках.

Вы узнаете о вирусологии, кто и каким образом, может доставить вирусы на ваши устройства и корпоративные сети: Вирусы, Loaders, Stillers, Miners, Coinhive, MAAS, XSS, Clippers, RAT, HVNC, Keyloggers, Ransomware и другие популярнейшие инструменты и устройства, применяемые в реальных атаках.

STAGE 1: ТЕОРИЯ

Средний уровень. Для начинающих и действующих экспертов в сфере ИБ.
Мы рассмотрим основные инструменты и типы атак на инфраструктуры, средства и инструменты злоумышленников, разберем принципы и механизмы работы с ними, обсудим как выявлять и противостоять таким инструментам и атакам. Рассмотрим лучшие продукты на рынке в сфере ИБ и обсудим их ключевые преимущества и недостатки. А на сессии Q&A ответим на ваши вопросы.

STAGE 2: ВОРКШОП

Продвинутый уровень. Для действующих специалистов по информационной безопасности.
Мы детально рассмотрим инструменты злоумышленников, в том числе физические устройства, разберём современные и наиболее популярные методы и тактики атак на организации и конечных пользователей, проведём демонстрацию атак на инфраструктуру и пользователей внутри периметра и из вне, разберём инструменты и сервисы (предложенные нами или на ваш выбор по используемому стеку), с помощью которых можно обезопасить внешний и внутренний периметры. В завершении мы проведем лабораторную работу, в ходе которой вы самостоятельно расследуете инциденты, произошедшие на «Звезде смерти», выявите точки входа, вектора атаки, задействованное ПО, устраните последствия атак, а так же не допустите повторения случившегося.

STAGE 3: СРАЖЕНИЕ

Практический уровень. Для опытных, действующих специалистов по ИБ, занимающих позиции в SOC, отделах аналитики ИБ, реверсеров, DevSecOps-инженеров, архитекторов ИТ систем, CTO, DPO, CISO, BISO.
В ходе мероприятия в ограниченный срок, вы развернете и настроите системы безопасности, после чего на вас начнётся масштабная кибератака в реальном времени. Ваша задача защищаться, идентифицировать инциденты по уровню критичности, отфильтровать ложные, научиться распределять задачи, взаимодействовать в команде при возникновении стрессовой ситуации. Нужно не дать команде атакующих воспроизвести недопустимые события в системах и предоставить аналитический отчёт расследования по результатам мероприятия.

wtc@wone-it.ru

Москва, 105066
ул. Нижняя Красносельская
д. 40/12, корп. 2
этаж 3, офис № 323
+7 499 322 05 45

ООО "Ван Ай Ти Трейд"
ИНН: 5044057860
КПП: 770101001
www.wone-it.ru