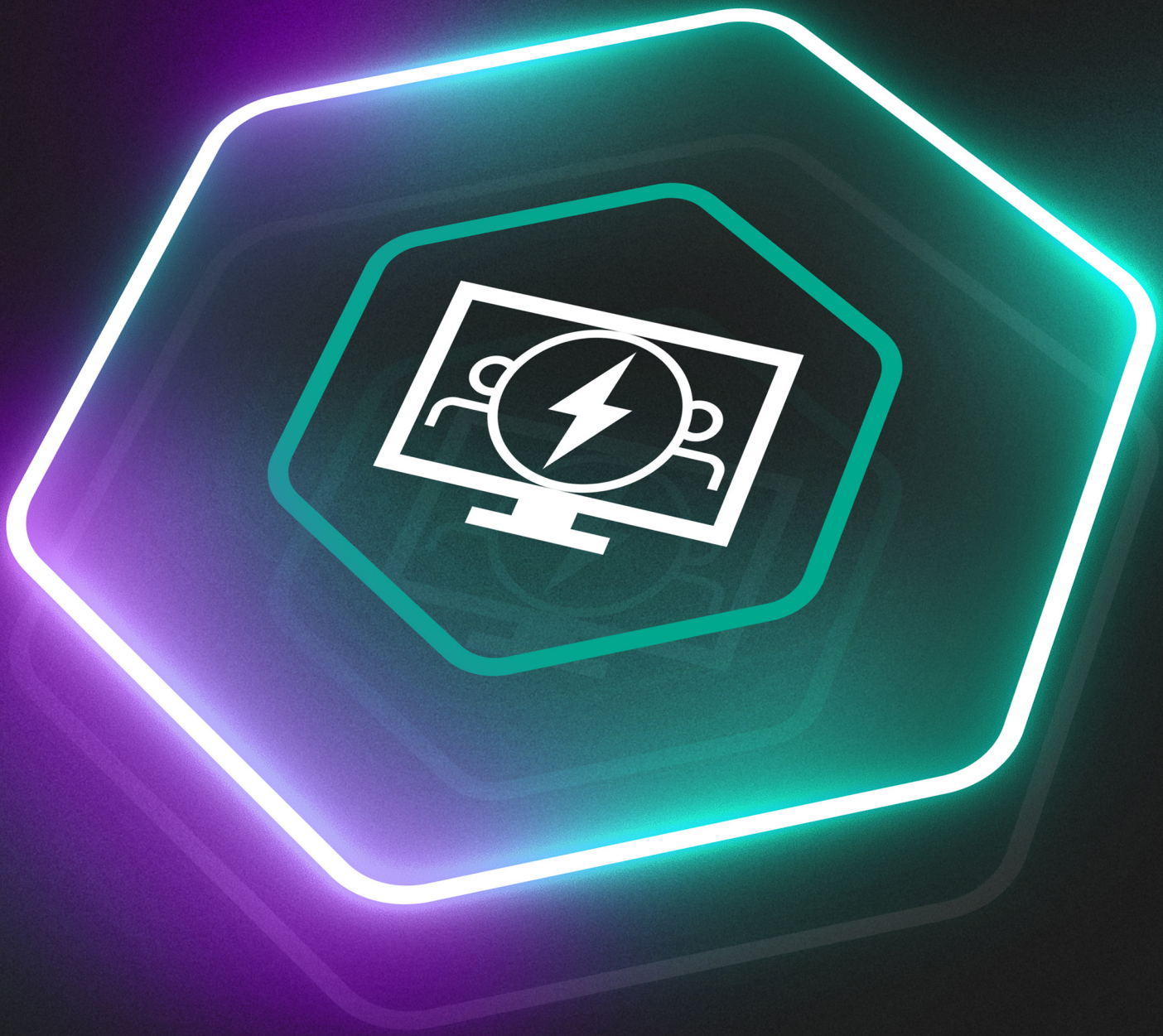

Kaspersky Red Teaming

kaspersky активируй будущее

Kaspersky
Red Teaming

Для чего нужен Red Teaming

Полностью предотвратить компрометацию информационных активов в крупных сетях может быть крайне сложно, а в случае атак с использованием уязвимостей "нулевого дня" и вовсе невозможно.

Именно поэтому очень важно сделать все возможное, чтобы инциденты информационной безопасности были обнаружены как можно раньше. Зрелые организации с хорошо отлаженными процессами оценки безопасности, управления уязвимостями и обнаружения инцидентов информационной безопасности должны проводить учения формата Red Teaming.

Эти учения определяют, насколько хорошо инфраструктура защищена от высококвалифицированных злоумышленников, действующих максимально скрытно, и помогают обучить команду ИТ-безопасности выявлять атаки и реагировать на них в реальных условиях.

Как работает Kaspersky Red Teaming?

Threat Intelligence

Сервис начинается с обсуждения известных заказчику угроз и опыта «синей» команды (Blue Team) компании. Цель - выявить наиболее критичные бизнес-активы и понять, как результаты проекта могут быть адаптированы к TTP, используемым в системах защиты компании.

Однако во время этих обсуждений эксперты «Лаборатории Касперского» не запрашивают никакой информации о целевых активах, поскольку «красная» команда (Red Team) будет проводить самостоятельный сбор информации, как это делали бы реальные противники.

Этап сбора информации включает в себя как анализ общедоступной информации (разведка из открытых источников), так и анализ данных, доступных в подпольных сообществах.

Имитация атаки

Этот этап начинается с подготовки сценариев и инструментов атак на основе результатов этапа анализа угроз.

Подготовка может включать в себя глубокое исследование систем, используемых в среде клиента, с целью выявления новых уязвимостей, разработку специальных инструментов для обхода систем безопасности клиента или подготовку атак методом spear-phishing. По завершении подготовки эксперты переходят к активной фазе моделирования противника.

Тесты проводятся по сценариям заказчика с использованием специальных техник, позволяющих избежать обнаружения «синей» командой.

После того как «красная» команда выполнит свои задачи, проводятся мероприятия по обнаружению и реагированию на инциденты, чтобы вовлечь в учения «синюю» команду.

Тесты по моделированию противника могут включать в себя:

- Пассивный сбор информации
- Активный сбор информации (обнаружение сети), включая сканирование портов, определение доступных служб и ручные запросы к определенным службам (DNS, почта)
- Сканирование и анализ внешних уязвимостей
- Безопасность веб-приложений (с использованием как автоматизированных, так и ручных подходов) для выявления различных типов уязвимостей
- Ручной анализ уязвимостей, включая выявление ресурсов без аутентификации, важной общедоступной информации, недостаточного контроля доступа
- Угадывание учетных данных
- Тесты социальной инженерии
- Эксплуатация одной или нескольких найденных уязвимостей и повышение привилегий (если возможно)
- Разработка атаки с использованием полученных привилегий и перечисленных выше методов до тех пор, пока поставщик услуг не сможет получить доступ к локальной сети или критическим сетевым ресурсам (например, контроллерам домена Active Directory, бизнес-системам, СУБД и т. д.) или пока не будут исчерпаны все методы атаки, доступные в ходе тестирования.

Подготовка отчета

На этом этапе команда «Лаборатории Касперского» проанализирует результаты симуляции противника, подготовит отчет с подробным описанием атак (включая временные метки и индикаторы компрометации) и предоставит рекомендации.

Обзор результатов учений

После оценки можно организовать семинар с «голубой» командой компании, чтобы обсудить результаты проекта, причины любых необнаруженных или непредусмотренных проблем, а также возможные улучшения в защите.

Методология Kaspersky Red Teaming

Можно использовать следующие инструменты оценки

- Средства сбора информации (Maltego, theHarvester и другие)
- Различные универсальные и специализированные сканеры (NMap, MaxPatrol, Nessus, AcuneticsWVS, nbtscan и другие)
- Комплексные решения для оценки безопасности (KaliLinux)
- Инструменты для угадывания учетных данных (Hydra, ncrack, Bruter и другие)
- Специализированные решения для оценки безопасности веб-приложений (OWASPdirbuster, BurpSuite, ProxyStrike, различные плагины для Mozilla Firefox)
- Анализаторы сетевого трафика (Wireshark, Cain and Abel)
- Инструменты для извлечения и управления учетными данными (Mimikatz, WCE, pwdump и другие)
- Специализированные инструменты для различных типов атак (Yersinia, Loki, Responder, SIPVicious и другие)
- Инструменты для дизассемблирования и отладки (IDA Pro, OllyDbg)
- И другие, включая эксплойты ограниченного доступа и пользовательские средства эксплуатации, разработанные «Лабораторией Касперского».

Red Teaming схож с реальной хакерской атакой и позволяет оценить меры защиты на практике. Однако, в отличие от хакерской атаки, этот сервис выполняется опытными экспертами по безопасности из «Лаборатории Касперского», которые уделяют первостепенное внимание конфиденциальности, целостности и доступности системы, строго придерживаясь международных стандартов и лучших практик, таких как:

1. Стандарт выполнения тестов на проникновение (PTES)
2. Специальная публикация NIST 800-115 "Техническое руководство по тестированию и оценке информационной безопасности"
3. Руководство по методологии тестирования безопасности с открытым исходным кодом (OSSTMM)
4. Основы оценки безопасности информационных систем (Information Systems Security Assessment Framework, ISSAF)
5. Консорциум по безопасности веб-приложений (WASC)
6. Классификация угроз Open Web Application Security Project (OWASP)
7. Руководство по тестированию Common Vulnerability Scoring System (CVSS)
8. и другие применимые стандарты в зависимости от сферы деятельности и местоположения вашей организации

Для обеспечения законности и безопасности Kaspersky Red Teaming заказчик должен предоставить официального сотрудника в качестве контактного лица для всех коммуникаций по проекту, включая переговоры о масштабах, решение вопросов доступа и подтверждение активных работ. Представитель должен иметь адрес электронной почты, принадлежащий доменному имени заказчика, и не являться сторонним посредником.

Результаты Kaspersky Red Teaming

Резюме	После оказания услуги заказчик получит отчет, содержащий выводы высокого уровня по выявленным защитным возможностям и рекомендации по их улучшению.
Подробное описание уязвимостей	Кроме того, в отчет включено подробное описание найденных уязвимостей, в том числе уровень серьезности, сложность эксплуатации, потенциальное воздействие на уязвимую систему и доказательства существования уязвимостей (по возможности).
Подробное описание проведенных действий	Подробное описание действий, включая временные метки и индикаторы компрометации, предоставляется для анализа и улучшения работы защитной команды.
Рекомендации	Рекомендации по устранению уязвимостей, улучшению процессов реагирования на инциденты и смягчению выявленных проблем предотвращения и обнаружения.

Преимущества Kaspersky Red Teaming

Безопасность работ

Наш главный приоритет — обеспечение конфиденциальности, целостности и доступности ваших ресурсов. Эксперты «Лаборатории Касперского» примут все необходимые меры предосторожности, чтобы не допустить нанесения ущерба вашей среде.

Защищенность данных

Мы будем хранить и передавать всю конфиденциальную техническую информацию, связанную с проектом, включая важные данные, учетные данные и результаты оценки, используя надежное шифрование. По желанию заказчика эта информация может быть удалена после завершения проекта.

Признанные эксперты

Наша команда экспертов по оценке безопасности — это опытные специалисты, обладающие глубокими знаниями в данной области. Они постоянно развивают и оттачивают свои навыки. Их исследования в области безопасности были отмечены такими лидерами отрасли, как Oracle, Google, Apple, Microsoft, Facebook, PayPal, Siemens, SAP и другими.

Узнать подробнее о Kaspersky Red Teaming

services@kaspersky.com

#kaspersky
#активируйбудущее