СИСТЕМА РАННЕГО ПРЕДУПРЕЖДЕНИЯ КИБЕРУГРОЗ

TDS

ОБНАРУЖЕНИЕ ЦЕЛЕВЫХ АТАК

Используя данные киберразведки и технологии машинного обучения, комплекс TDS позволяет выявить все формы вредоносного кода, распространяющегося или уже работающего в вашей сети:

- целевые угрозы и 0-day атаки
- вредоносные документы
- банковские трояны
- шпионское ПО
- мобильные трояны
- инструменты удаленного доступа
- бекдоры
- и другие угрозы

Комплекс обнаружения целевых атак состоит из трех модулей:

TDS Sensor

Анализ входящих и исходящих пакетов данных с использованием сигнатур и правил, основанных на эксклюзивных данных об угрозах.

TDS Polygon

Анализ поведения подозрительных объектов в безопасной среде, позволяющий предотвратить заражения в результате

- фишинговых рассылок
- атак на браузер
- атак с использованием ранее неизвестных вредоносных программ и инструментов

Вердикт о степени опасности объекта выносится на основании классификатора, формируемого системой машинного анализа.

Машинный интеллект на страже вашей безопасности

С помощью передовых технологий машинного обучения мы обработали данные, накопленные за 12 лет расследований и экспертиз. Результаты легли в основу классификатора, который обновляется по мере появления новых данных.

Обучение машин проходит под контролем опытных аналитиков, что сводит к минимуму количество ложных срабатываний.

1,8 МИЛЛИАРДА РУБЛЕЙ

за 7 месяцев похитила из российских банков преступная группа Buhtrap

Корректно работающие антивирусы и межсетевые экраны не смогли выявить активность вредоносного ПО, которое группа распространяла через фишинговые письма.

Мы отслеживали активность Buhtrap и эволюцию ее трояна с момента появления, задолго до начала целевых атак. Благодаря своевременному обновлению сигнатур, банки, в которых был установлен сенсор TDS, не пострадали.

Узнайте больше о тактике Buhtrap на group-ib.ru/reports

SOC GROUP-IB

Ручной анализ логов, выделение критически важных инцидентов и поддержка реагирования специалистами CERT-GIB в режиме 24/7/365.

- Уведомления о критических заражениях и попытках эксплуатации уязвимостей по телефону и e-mail.
- Возможность выезда на место инцидента, в том числе для сбора цифровых доказательств;

УНИКАЛЬНЫЕ ИСТОЧНИКИ ДАННЫХ ОБ УГРОЗАХ

Высокотехнологичная инфраструктура сбора данных об активности киберпреступников дает нам возможность быстро и точно обновлять маркеры вредоносной активности для выявления критических событий.

КИБЕРРАЗВЕДКА

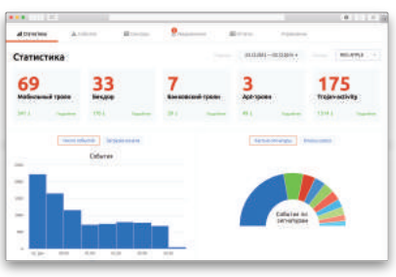
Эксклюзивные данные threat intelligence о новых вредоносных программах и изменениях в известных вирусах, смене тактик атак и адресов C&C-серверов.

КРИМИНАЛИСТИКА

Индикаторы компрометации и другие сведения об актуальных целевых атаках от Лаборатории компьютерной криминалистики и исследования вредоносного кода Group-IB, участвующей в их расследовании.

МАШИННЫЙ ИНТЕЛЛЕКТ

Выявление неизвестного вредоносного кода и моделирование новых тактик атак с использованием передовых алгоритмов машинного обучения.



Все данные о выявленных угрозах доступны в облачном веб-интерфейсе. Вы увидите все активные заражения сразу после подключения сенсора TDS.

КАК РАБОТАЕТ СИСТЕМА ОБНАРУЖЕНИЯ АТАК TDS

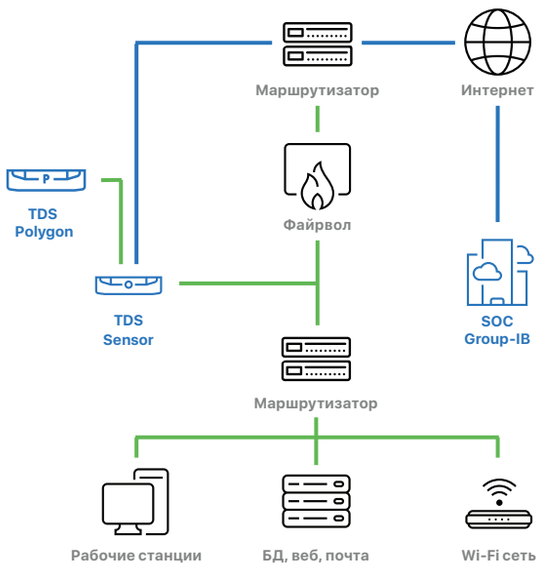
СЕНСОР TDS

Выявляет зараженные узлы, устанавливая их взаимодействия с командными центрами.

Детектирует сетевые аномалии, генерируемые вредоносными программами, при помощи алгоритмов машинного анализа.

Интегрируется с системой поведенческого анализа Polygon для выявления ранее неизвестного вредоносного кода.

Передает информацию о выявленных инцидентах в SOC Group-IB или внутреннюю систему учета логов.



SOC GROUP-IB

Данные, полученные от сенсора, классифицируются и коррелируются в Центре обработки данных.

События анализируются квалифицированными специалистами Group-IB вручную.

Анализ данных ведется круглосуточно, без выходных.

Эксперты SOC уведомят ваших специалистов о критичных угрозах по телефону и e-mail, а детальные результаты анализа будут доступны в удобном web-интерфейсе.

TDS POLYGON

Polygon запускает файлы, полученные от TDS, в изолированной среде, анализирует их поведение на низком уровне и выносит объективное заключение о степени опасности объектов.

Обработка и анализ файлов производится внутри вашего контура безопасности, обеспечивая полную конфиденциальность.

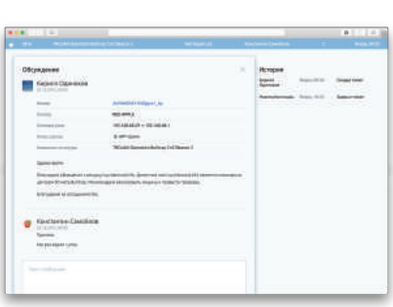
Вы можете привлечь специалистов Group-IB для дальнейшего исследования и реагирования на выявленные угрозы.

Приобретая TDS, вы бесплатно получаете страховой полис от AIG, распространяющийся на риски утечки корпоративных или персональных данных и нарушения безопасности компьютерной системы, вызванной заражением или повреждением информации.

Ведь в отдельных случаях киберпреступники могут использовать не только вредоносное ПО, но и социальную инженерию, обман, подкуп сотрудников. Клиенты Group-IB защищены и от таких сложных атак.

GIB + AIG

МАКСИМАЛЬНОЕ УДОБСТВО ИСПОЛЬЗОВАНИЯ



Интерфейс тикет-системы позволяет упорядочить процесс реагирования и обмен знаниями между его участниками.

Облачный интерфейс

Вся информация о выявленных угрозах доступна в веб-интерфейсе, через который удобно отслеживать уведомления в течение дня.

Эффективная поддержка

Удобная тикет-система, которая может быть организована и на базе локального веб-интерфейса, гарантирует, что ни один вопрос не останется без ответа.

Наглядные отчеты

Визуализированная статистика по периодам и по типам событий позволяет отслеживать изменения в динамике и характере атак.

Интеграция с SIEM

Поток событий, фиксируемых сенсором TDS, может быть автоматически направлен в любую SIEM или систему хранения логов.

СВЯЖИТЕСЬ С НАМИ
чтобы провести тест-драйв TDS
+7 (495) 984 33 64
tds@group-ib.ru

УЗНАЙТЕ БОЛЬШЕ
о возможностях предотвращения целевых атак с помощью TDS
tds.group-ib.ru

ПОЗНАКОМЬТЕСЬ С GROUP-IB
– одним из 7 лучших поставщиков данных кибер разведки (threat intelligence) в мире по версии Gartner
www.group-ib.ru