GROUP-IB THREAT DETECTION SYSTEM (TDS)

TDS POLYGON

group-ib.ru

GROUP-IB THREAT DETECTION SYSTEM (TDS)

TDS — комплексное решение, предназначенное для выявления целенаправленных атак и неизвестных угроз, охоты за угрозами как внутри защищаемого периметра, так и за его пределами, реагирования на инциденты и их расследования.

Применение TDS позволяет определять заражения, которые пропускают стандартные средства защиты: антивирусы, межсетевые экраны, системы предотвращения вторжений.

КЛЮЧЕВЫЕ ПРЕИМУЩЕСТВА:

- Более точное обнаружение неизвестных угроз и самообучение системы за счет обратной связи от каждого отдельного модуля;
- Автоматизация охоты за угрозами, реагирования, расследования инцидентов;
- Комплексное решение, работающее как единое целое, не требующее интеграционных работ и корреляции событий между разными детектирующими компонентами;
- Интегрированные данные от Group-IB Threat Intelligence;
- Включённые услуги по мониторингу, реагированию, охоте за угрозами и расследованию инцидентов от экспертов с многолетним опытом;
- Гибкие варианты развертывания и простота использования;
- Включенная страховка на случай инцидентов от международных страховых компаний.

ТЕХНИЧЕСКИЕ ПОДХОДЫ:

- Глубокий анализ сетевого трафика для выявления аномалий и вредоносного трафика;
- Поведенческий анализ файлов и ссылок в изолированных песочницах;
- Выявление аномалий в поведении пользователей и программ на компьютерах;
- Автоматизированная охота за неизвестными угрозами;
- Проверка индикаторов, полученных от Threat Intelligence;
- Корреляция событий, собираемых комплексом TDS.

ДЕТЕКТИРОВАНИЕ УГРОЗ НА РАЗЛИЧНЫХ ФАЗАХ ATT&CK MATRIX:

- Угрозы нулевого дня;
- Эксплойты, трояны, бэкдоры, вредоносные скрипты под десктопные, серверные и мобильные платформы;
- Скрытые каналы передачи данных;
- Бестелесные угрозы;
- Атаки с использованием легитимных инструментов (living-off-the-land).

ПОЛНОЕ РЕШЕНИЕ THREAT DETECTION SYSTEM (TDS) СОСТОИТ ИЗ ЧЕТЫРЕХ ОСНОВНЫХ МОДУЛЕЙ:

TDS Huntbox

Единая система управления детектирующей инфраструктурой, автоматизированного анализа, корреляции событий и обеспечения процесса охоты за угрозами.

TDS Sensor

Модуль для глубокого анализа сетевого трафика и выявления угроз на сетевом уровне.

TDS Polygon

Модуль для запуска файлов, ссылок и их динамического анализа, для выявления известных и неизвестных угроз в изолированной среде.

TDS Endpoint

Агент для обнаружения угроз на хосте, фиксации полной хронологии событий на системе, блокировки аномального поведения, изоляции хоста, сбора криминалистически значимых данных.

TDS POLYGON

TDS Polygon — модуль продукта Group-IB Threat Detection System (TDS), позволяющий производить поведенческий анализ файлов, извлекаемых из электронных писем, сетевого трафика, файловых хранилищ, персональных компьютеров и автоматизированных систем, посредством интеграции через API или загружаемых вручную. TDS Polygon дополняет функциональность продукта TDS, расширяя возможности по обнаружению вредоносных файлов, нацеленных на защищаемую инфраструктуру.

ОСОБЕННОСТИ СИСТЕМЫ:

- **Покрытие основных каналов распространения угроз** — почта, интернет, заражение официальных сайтов, а также инсайдеры и USB-носители;
- **Постоянно обновляемые базы индикаторов компроментации и классификатора** — исходя из расследований криминалистов и на основе информации из систем Threat Intelligence;
- **Высокий уровень выявления угроз** за счет собственного низкоуровневого монитора и системы сокрытия виртуализации от вредоносного ПО;
- **Выявление социально-инженерного воздействия** — обнаружение попыток обхода средств anti-APT решений вредоносным файлом в процессе поведенческого анализа;
- **Мультиверсионный анализ** — Windows XP, Windows 7, Windows 10 в двух вариантах разрядности – x32/x64, а также с использованием двух языков системы — русский/английский;
- **Обнаружение отложенных атак** — использование ретроспективного анализа при интеграции с различными системами защищаемой инфраструктуры;
- **Обнаружение вредоносного ПО** в почтовых сообщениях, файловых хранилищах, а также при скачивании из сети Интернет с возможностью блокировки*;
- **Полная конфиденциальность анализа файлов** — обработка и анализ файлов осуществляется внутри контура безопасности заказчика, непосредственно на устройстве TDS Polygon;
- **Интерфейс с тикет-системой** в SOC Group-IB (опционально);
- **Внутренний классификатор угроз;**
- **Различные варианты развертывания SW/HW/Cloud**;

* Необходимо взаимодействие с TDS Sensor и интеграция его в соответствующие системы защищаемой инфраструктуры.

ЦЕНТРАЛИЗОВАННОЕ УПРАВЛЕНИЕ

TDS Huntbox предоставляет графический интерфейс управления установленных в защищаемой инфраструктуре модулей TDS, является единой точкой хранения данных об инцидентах, позволяет осуществлять сквозной поиск по всем индикаторам во всех событиях и алертах системы, а также предоставляет функционал:

1. **Threat hunting;**
2. **Реагирование на инциденты;**
3. **Корреляция событий и удаленная форензика.**

TDS POLYGON

ОСНОВНЫЕ ФУНКЦИИ TDS POLYGON:

Запуск файлов в изолированной среде

Тип и правила запуска файла определяются по его заголовкам. Если файл не запустился в выбранной среде, осуществляется его перезапуск в новой среде. Использование различных методов сокрытия факта виртуализации.

Фиксация активности после запуска анализируемого файла

Реализует полное логирование всех изменений в изолированной среде, произошедших после запуска файла, включая видеозапись экрана.

Имитация действий пользователя

После помещения анализируемого объекта в выбранную виртуальную среду реализуется большой спектр возможных действий реального пользователя ОС – от движения мыши и нажатия клавиш до перехода по ссылкам, скачивания и открытия/запуска файлов.

Социально-технические методы

Анализируемые специалистами Group-IB социально-технические методы обхода систем защиты, используемые злоумышленниками, встраиваются в систему TDS Polygon.

Система умеет работать с запароленными архивами, учитывая слова из письма, а также из приложенных офисных документов. Доступно несколько различных режимов работы со ссылками, включая интеллектуальный анализ типов ссылок, ссылок с перенаправлениями различных видов, а также работа с файловыми хранилищами.

Ретроспективный анализ

Продукт TDS использует незадействованные мощности модуля TDS Polygon для проведения повторного поведенческого анализа объектов, первоначальный анализ которых не выявил вредоносных признаков, выявляя тем самым отложенные атаки на защищаемую инфраструктуру.

Подробность отчетов

Опыт криминалистов по сбору и структуризации данных о поведении вредоносного ПО, воплощен в подсистеме отчетности TDS Polygon. В отчеты попадают:

- оценка вредоносности;
- атрибуция объекта;
- видео исполнения файла;
- файловая структура объекта;
- поведенческие маркеры;
- информация о сетевой активности объекта;
- дерево процессов;
- информация о затрагиваемых объектом системных данных;
- дополнительные артефакты анализа.

Более 200 поддерживаемых форматов анализируемых объектов.

	TDS Polygon Cloud	TDS Polygon Standard	TDS Polygon Enterprise
Пиковая производительность, Файлов/день	любая	9000	19000
Сетевые порты (LAN)	—	4x 10/100/1000 BASE-T	4x 10/100/1000 BASE-T
Порт IPMI (задняя панель)	—	1	1
Форм-фактор	Cloud	1U	1U
Емкость накопителя	—	2x 480GB SSD	2x 480GB SSD
Порты USB (задняя панель)	—	2	2
Порты USB (передняя панель)	—	2	2
Последовательный порт (задняя панель)	—	1	1
Порт VGA	—	1	1
Блок питания переменного тока (Вт)	—	2 x 550	2 x 550
Максимальная потребляемая мощность (Вт)	—	517	517
Размеры (ВхШхГ), мм	—	43 x 434 x 678	43 x 434 x 678
Вес устройства в отдельности (кг)	—	16	16
Heat Dissipation(max)	—	2x 2107 BTU/h	2x 2107 BTU/h
Сертификаты соответствия	—	TP TC 004/2011 TP TC 020/2011	TP TC 004/2011 TP TC 020/2011
Соответствие нормативам	—	RoHS, WEEE	RoHS, WEEE
Рабочая Температура	—	RoHS, WEEE	RoHS, WEEE
Рабочая относительная влажность	—	10°C to 35°C (50°F to 95°F) with no direct sunlight on the equipment	10°C to 35°C (50°F to 95°F) with no direct sunlight on the equipment
Рабочая относительная влажность	—	0% to 80% Relative Humidity with 29°C (84.2°F) maximum dew point	0% to 80% Relative Humidity with 29°C (84.2°F) maximum dew point