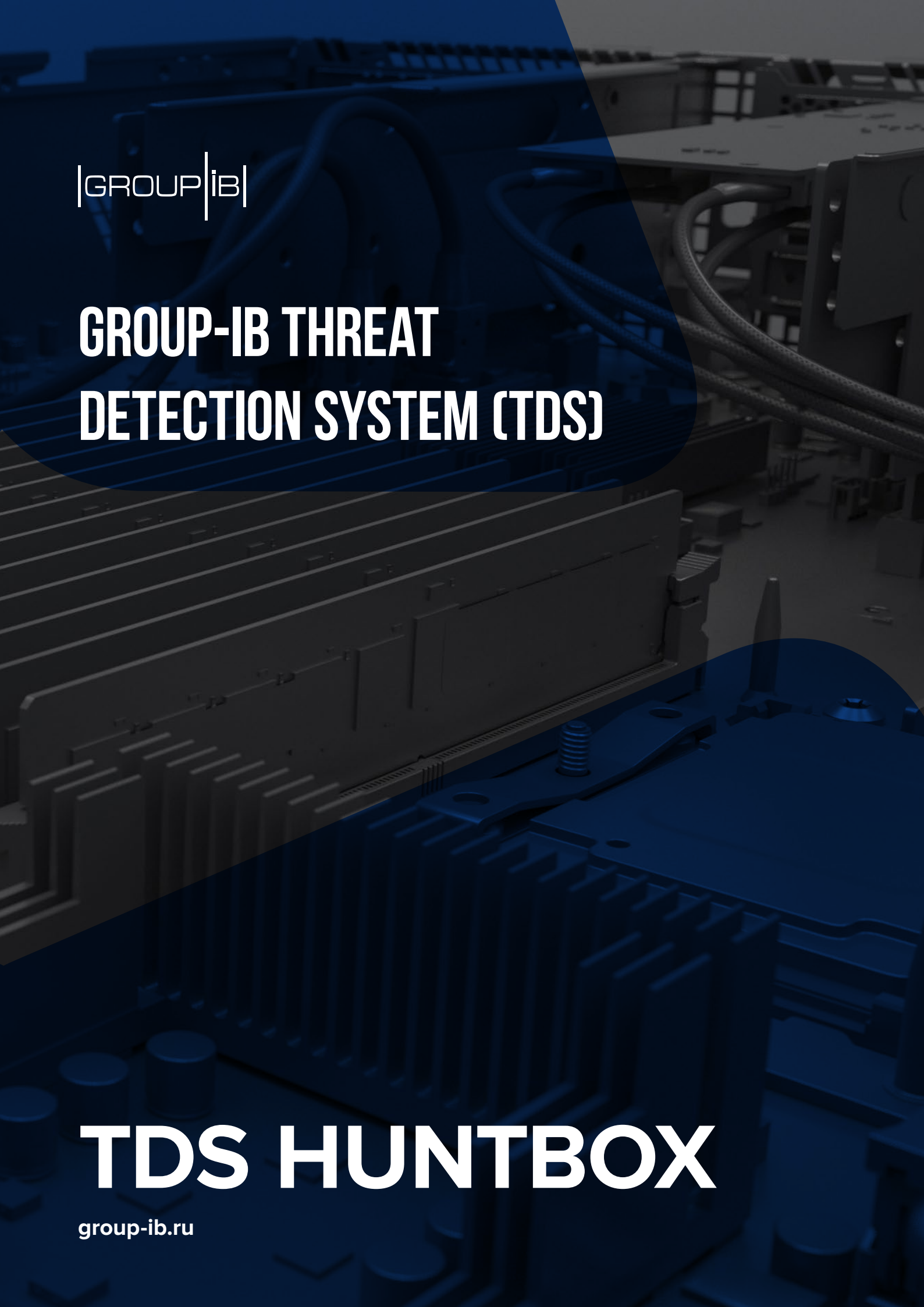

GROUP-IB THREAT DETECTION SYSTEM (TDS)

TDS HUNTBOX

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 HUNTBOX

TDS Huntbox — это набор инструментов, необходимых для команд мониторинга, реагирования на инциденты и проведения компьютерных расследований в защищаемой инфраструктуре. Может служить как дополнительным инструментом SOC, так и его ядром.

ОСНОВНЫЕ ФУНКЦИИ TDS HUNTBOX:

Управление детектирующей инфраструктурой

TDS Huntbox является единой точкой управления всеми детектирующими модулями комплекса: Sensor, Polygon, Endpoint и единой точкой хранения всех событий, алертов и инцидентов, что позволяет осуществлять сквозной поиск по всей базе ретроспективных событий и эффективно коррелировать их между собой.

Обнаружение атак, корреляция и обогащение

Обнаружение атак происходит только в доверенных средах, что позволяет исключить вмешательство атакующего в обнаружение его активности. Независимо от того, как произошел детект, запускается процесс корреляции событий со всех модулей TDS. После того, как все связанные события были обнаружены, их индикаторы проходят процесс обогащения во внутренних источниках и данных Threat Intelligence — процессы корреляции и обогащения запускаются снова, что позволяет мгновенно получать полную картину атаки в графовом и табличном виде.

Визуализация инцидента

Наглядная визуализация взаимосвязей процессов, файлов, мьютексов, ключей реестра, участвующих в инциденте — информация необходимая для оперативного расследования любого инцидента.

Охота за угрозами

Для охоты за угрозами во внутренней инфраструктуре предоставляется возможность сквозного поиска по всем событиям, зафиксированным на хостах, в сетевом трафике, динамическом анализе в песочнице с максимально глубоким контекстом — от процесса и параметров его запуска, до технических заголовков электронных писем.

Графовый анализ

Для охоты за пределами инфраструктуры клиента предоставляется отдельный инструмент — Граф. Group-IB фиксирует слепки состояния сети Интернет, выделяет характерные признаки, строит между ними связи, коррелирует эту инфраструктуру с конкретными инструментами и атакующими. Граф предоставляет возможность искать по IP-адресам, доменам, адресам электронной почты, номерам телефонов, SSL сертификатам или отпечаткам SSH, хэш - суммам файлов в ручном режиме, а также автоматически получать скрытую инфраструктуру атакующих для последующей проверки этих данных внутри защищаемого периметра.

Реагирование на инцидент

Для обеспечения совместной работы между разными экспертами в процессе реагирования на инцидент используется встроенная система обмена сообщениями. Интерфейс TDS Huntbox реализует следующие варианты реагирования на хостах:

- Завершение вредоносных процессов;
- Запрет запуска файлов, вовлеченных в инцидент;
- Изолирование компьютера от сети;
- Запуск сбора криминалистических данных, например, дамп ОЗУ, список установленных обновлений, файлы реестра, сбор журналов ОС и т.п.

	TDS Huntbox Standard	TDS Huntbox Enterprise	TDS Huntbox Storage
Количество подключенных Endpoint, шт.	<1000	1000-2000	*
Емкость накопителя	2x 960 GB(SSD) + 4x 1,2 TB(HDD)	2x 960 GB(SSD) + 4x 1,2 TB(HDD)	2x 960 GB(SSD) + 2x 1,2 TB(HDD)
Сетевые интерфейсы	4x 1000 BASE-T	4x 1000 BASE-T	4x 1000 BASE-T
Форм-фактор	1U	1U	1U
Порт IPMI (задняя панель)	1	1	1
Порты USB (задняя панель)	2	2	2
Последовательный порт (задняя панель)	1	1	1
Порт VGA	1	1	1
Блок питания переменного тока (Вт)	2x 750	2x 750	2x 550
Максимальная потребляемая мощность (Вт)	705	705	517
Размеры (ВхШхГ), мм	43 x 434 x 755	43 x 434 x 755	43 x 434 x 755
Вес устройства в отдельности / в фунтах (кг)	22	24	19,9
Heat dissipation (max)	2x 2891 BTU/h	2x 2891 BTU/h	2x 2107 BTU/h
Сертификаты соответствия	ТР ТС 004/2011; ТР ТС 020/2011	ТР ТС 004/2011; ТР ТС 020/2011	ТР ТС 004/2011; ТР ТС 020/2011
Соответствие нормативам	RoHS, WEEE	RoHS, WEEE	RoHS, WEEE
Рабочая Температура	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	10°C to 35°C (50°F to 95°F) with no direct sunlight on the equipment
Рабочая относительная влажность	10% to 80% relative humidity with 29°C (84.2°F) maximum dew point	10% to 80% relative humidity with 29°C (84.2°F) maximum dew point	10% to 80% relative humidity with 29°C (84.2°F) maximum dew point

* HB Storage используется при увеличении объема и длительности хранения информации. HB Storage используется совместно с HB Standard/ Enterprise.

Варианты развертывания:

Существует три варианта поставки TDS Huntbox: SW/HW/Virtual. В зависимости от требования TDS Huntbox может быть развернут следующим образом:

- **on-prem** – изолированное решение, при котором все данные остаются внутри периметра клиента;
- **on-cloud** – развертывание TDS Huntbox в инфраструктуре Group-IB, что позволяет оперативно наращивать мощности и осуществлять мониторинг, расследование и реагирование;
- **гибридное** – смешанная установка модулей TDS между защищаемой инфраструктурой и инфраструктурой Group-IB для решения индивидуальных задач клиента.