

АЕГИС

Описание платформы

Задачи, модули, роли и порядок работы с активами и находками.

ПОНЯТЬ УСТРОЙСТВО. ОБСУДИТЬ ПОДКЛЮЧЕНИЕ.

От задачи организации — к рабочему составу продукта.

Содержание

Описание платформы

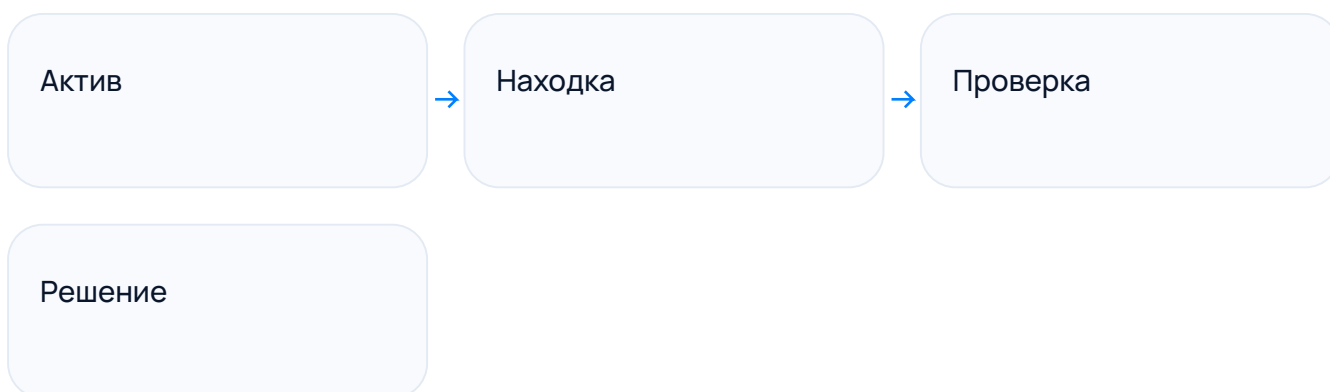
01	Управлять риском, а не списками	3
02	Кому подходит платформа	4
03	Задачи, с которых начинается работа	5
04	Состав платформы и готовность	6
05	ASM: контекст поверхности атаки	7
06	VM: находки с привязкой к активам	8
07	AEV: подтверждение результатов	9
08	SOC-консоль и инциденты	10
09	CA: оценка признаков компрометации	11
10	DLP: контроль передачи данных	12
11	Интеграции и обмен результатами	13
12	Роли и форматы размещения	14
13	Глоссарий и следующий шаг	15
	Контакты и консультация	16

Управлять риском, а не списками

АЕГИС объединяет сведения об активах, находках и результатах проверки в рабочем контексте команды безопасности.

Отдельный результат сканирования ещё не определяет порядок исправлений. Для решения нужны сведения о затронутом активе, доступности, доказательствах и ответственном.

Платформа связывает эти сведения: команда рассматривает находку в контексте актива, уточняет её статус и возвращается к результату после устранения.



- Единый реестр активов и связанный контекст.
- Работа с находками и доказательствами.
- Контроль решений и повторных проверок.

Кому подходит платформа

Для команд безопасности, которым важно согласованно работать с внешним периметром и результатами оценки защищённости.

Руководитель безопасности определяет приоритеты. Аналитик разбирает результаты и уточняет контекст. Специалист по оценке защищённости подтверждает находки. Администратор организует доступ и рабочий контур.

При согласовании учитывают структуру организации, категории активов и способ размещения данных. Рабочие области позволяют разделять контекст разных подразделений.

- Финансовые организации.
- Предприятия с распределённой инфраструктурой.
- Организации с отдельными защищаемыми контурами.

Задачи, с которых начинается работа

Проблемы связаны между собой: неизвестный периметр усложняет проверку, а неподтверждённые результаты усложняют устранение.

Список без приоритета: находки есть, но причины важности неочевидны. Команде нужен контекст и обоснованное решение.

Неизвестный периметр: сведения о доменах, адресах и приложениях распределены между источниками. Устранение без проверки: закрытая задача ещё не подтверждает изменение состояния актива.

Задача	Рабочий результат
Неизвестный периметр	Согласованный реестр активов
Список без приоритета	Находка с контекстом и решением
Устранение без проверки	Результат повторной проверки

Состав платформы и готовность

Состав модулей описывает доступные функции и направления развития.

Ядро и АЕВ доступны. Реестр активов и проверка по шаблонам CVE доступны в составе частично реализованных ASM и VM. Остальные направления имеют явные статусы.

Модуль	Готовность
Ядро	Доступно
АЕВ, проверка эксплуатируемости	Доступно
ASM, контроль периметра	Частично
VM, уязвимости	Частично
SOC-консоль и инциденты	В разработке
АЕГИС DLP	Бета
Connect, интеграции	В разработке
СА, оценка компрометации	В планах
Проверка в CI/CD	В планах

ASM: контекст поверхности атаки

Реестр активов формирует основу дальнейшей работы с уязвимостями.

В реестр включают доменные имена, адреса, приложения и сетевые компоненты в согласованных границах. Связи, метки и происхождение сведений помогают разбирать принадлежность актива.

Изменения реестра сохраняют контекст: кто внёс запись, к какой области она относится и каким источником подтверждена. Архивирование отделяет актуальные объекты от записей, исключённых из работы.

АЕГИС

УПРАВЛЕНИЕ УЯЗВИМОСТЯМИ

Рабочая область

Активы

Находки

Проверки

Настройки

Белый Веб

Консоль / Активы

Реестр активов

Принадлежность, тип, источник и состояние объекта

Объект	Тип	Область	Состояние
Шлюз доступа	Сетевой узел	Внешний контур	В работе
Каталог учётных записей	Инфраструктура	Внутренний контур	В работе
Прикладной интерфейс	Веб-приложение	Внешний контур	На проверке
Сервер приложений	Инфраструктура	Внутренний контур	В работе
Рабочая станция	Рабочий узел	Внутренний контур	В работе

АЕГИС - Единый контекст активов и результатов

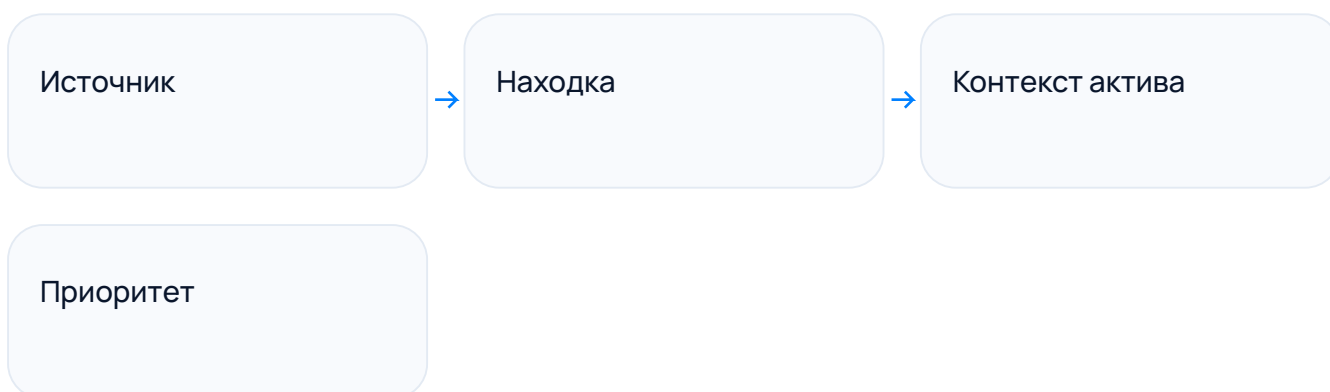
- Тип и идентификатор актива.
- Связи, метки и источник сведений.
- Права на чтение и изменение реестра.

VM: находки с привязкой к активам

Работа с уязвимостями начинается с понятной записи о проблеме и её влиянии.

Находка связывает актив, описание недостатка, источник обнаружения и материалы проверки. Идентификатор уязвимости помогает сопоставить сведения из разных источников.

Приоритизация опирается на контекст: значимость актива, доступность, подтверждение проблемы и возможные последствия. Решение сохраняют вместе с объяснением, чтобы следующий участник понимал основания действий.



- Понятное описание недостатка.
- Обоснование приоритета и связанный актив.
- Рекомендации и история изменения статуса.

AEV: подтверждение результатов

Проверка защищённости помогает отличить потенциальную проблему от подтверждённого риска.

Работу выполняют в согласованных границах. Материалы проверки связывают с целью, сценарием и результатом; специалист формирует заключение на основании собранных доказательств.

Повторная проверка возвращает команду к той же находке после изменений. Это сохраняет связь между первоначальным выводом, исправлением и результатом контроля.

АЕГИС УПРАВЛЕНИЕ УЯЗВИМОСТЯМИ Рабочая область Активы Находки Проверки Настройки Белый Веб	Консоль / Находки		
	Работа с находками		
	Контекст, основания решения и материалы проверки		
	Объект	Статус	Основание
	Доступ к интерфейсу управления	Подтверждена	Проверка
	Права учётной записи	Принятый риск	Решение
	Защищённый обмен	На проверке	Материалы
	Изменение конфигурации	Подтверждена	Контекст
	Повторная проверка	В работе	Результат
АЕГИС · Единый контекст активов и результатов			

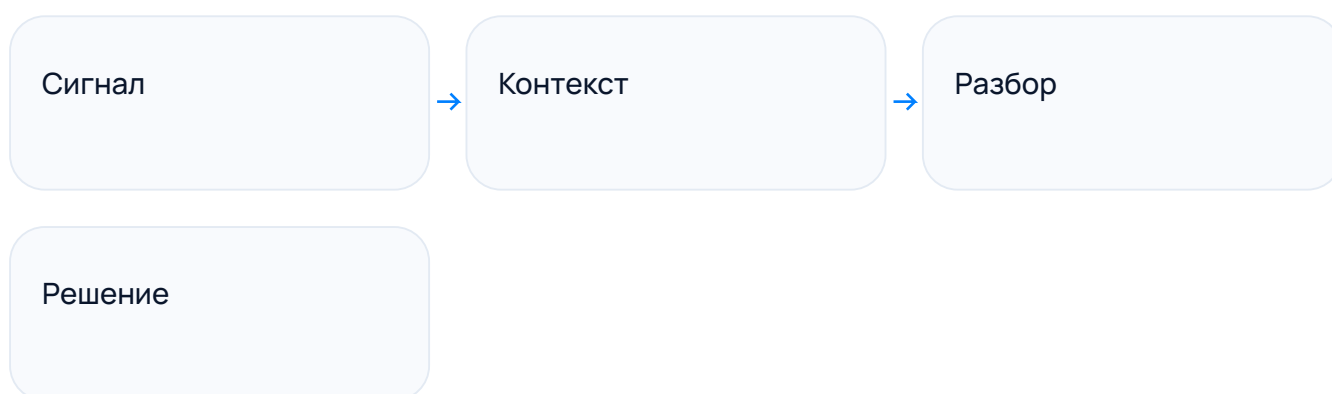
- Согласованные цели и ограничения.
- Материалы и заключение специалиста.
- Повторная проверка после исправления.

SOC-консоль и инциденты

SOC-консоль и инциденты находятся в разработке.

Аналитический сценарий объединяет карточку события, связанные активы, комментарии и материалы расследования. Ответственный уточняет влияние и согласует дальнейшие действия.

Реагирование не должно терять связь с исходным основанием. В рабочем процессе фиксируют причину решения, выполненные действия и материалы для последующего разбора. Подключение такого сценария определяется составом поставки.



- Связанные активы и события.
- Ответственный и история обсуждения.
- Результат расследования и дальнейшие действия.

СА: оценка признаков компрометации

Оценка компрометации СА запланирована; направление пока не доступно.

Работу начинают с цели оценки и перечня допустимых источников. Артефакты сопоставляют с правилами обнаружения и контекстом инфраструктуры.

Заключение строится на проверенных признаках, а не только на автоматическом совпадении. В материалах отделяют наблюдение от вывода специалиста и от рекомендации. Объём и состав этого направления согласуют отдельно.

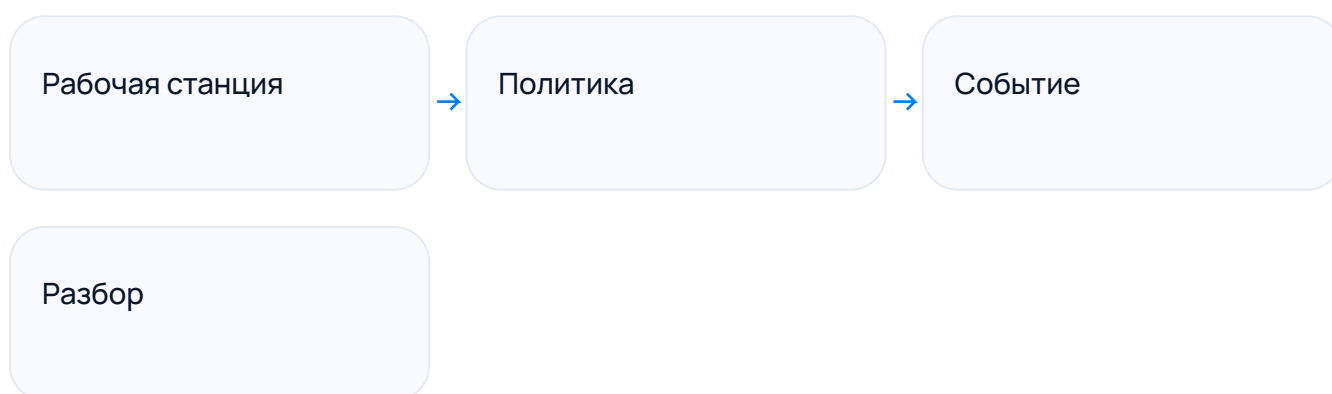
- Границы и источники исследования.
- Артефакты и проверка признаков.
- Заключение с основаниями и рекомендациями.

DLP: контроль передачи данных

АЕГИС DLP — модуль защиты от утечек информации в бета-стадии.

Политики связывают категории информации с каналами её передачи. События от рабочих станций формируют контекст для разбора, а карантин отделяет подозрительные файлы от обычного обращения.

При согласовании определяют защищаемые данные, рабочие станции, допустимые действия и правила доступа к материалам инцидента. Возможность объединения с общим рабочим контекстом АЕГИС рассматривают в составе поставки.



Интеграции и обмен результатами

Направление Connect и интеграции находятся в разработке.

На входе нужны источники сведений об активах, находках и событиях. На выходе — согласованные задачи, уведомления и материалы для ответственных.

При подключении фиксируют направление обмена, состав полей, владельца данных и правила доступа. API и уведомления по событиям обсуждают вместе с требованиями к окружению.

Категория	Назначение
Системы мониторинга	Контекст событий и результатов
Системы задач	Передача рекомендаций и статусов
Каналы уведомлений	Доставка согласованных сообщений

Роли и форматы размещения

Работа организуется вокруг ответственности и границ доступа.

Для руководителя важны основания решений; для аналитика — материалы; для специалиста по оценке защищённости — цели и результаты; для администратора — доступ и настройки.

Облачный формат, установка в контуре организации и изолированное размещение рассматриваются при выборе конфигурации. Требования к ресурсам, обмену данными и обновлениям определяют при согласовании.

Роль	Основная задача
Руководитель ИБ	Приоритеты и принятие решений
Аналитик	Контекст и разбор результатов
Специалист по оценке	Проверки и доказательства
Администратор	Доступ и рабочий контур

Глоссарий и следующий шаг

Общий язык помогает согласовать ожидаемый результат до подключения платформы.

Актив — объект инфраструктуры в границах работы. Находка — запись о выявленной проблеме. Доказательство — материал, на котором основано заключение. Повторная проверка — контроль состояния после изменения.

Для консультации подготовьте категории активов, описание действующего процесса и требования к размещению. Это позволит обсудить состав платформы и последовательность подключения.

Термин	Значение
ASM	Управление контекстом поверхности атаки
VM	Работа с уязвимостями и приоритетами
AEV	Проверка и подтверждение результатов
RBAC	Разграничение доступа по ролям
RLS	Изоляция записей между рабочими областями

Обсудим вашу задачу

Запросить консультацию

Подготовьте описание защищаемого контура, действующие процессы и ожидаемый результат. Состав продукта и параметры подключения определяются при согласовании.

info@whitevweb-security.ru

+7 (993) 405-09-02

whitevweb-security.ru/products/aegis

ООО «Белый Веб» / White Web LLC

ИНН 1685022692 · ОГРН 1251600038084

420132, г. Казань, ул. Фатыха Амирхана, д. 18а, помещ. 1000

Белый Веб — продукты информационной безопасности

v1.0 · 12 октября 2026