ЦИТ
ЦИФРОВЫЕ
ИНДУСТРИАЛЬНЫЕ
ТЕХНОЛОГИИ

ПЛАТФОРМА АВТОМАТИЗАЦИИ ПРОЦЕССОВ ИБ И ИТ

Каталог ИИ-решений

ЕДИНАЯ ПЛАТФОРМА С НАБОРОМ МОДУЛЕЙ

ЦИТ ЦИФРОВЫЕ ИНДУСТРИАЛЬНЫЕ ТЕХНОЛОГИИ

SOAR

Управление инцидентами с динамическими плейбуками, объектно-ориентированным подходом и ИИ-помощниками

UEBA

Поведенческий анализ для поиска аномалий при помощи ML-моделей, статистических методов и корреляции

TIP

Анализ угроз, киберразведка и threat hunting с интеграцией любых источников для ретро и потокового поиска с DGA

CERT

Двусторонние интеграции с центрами реагирования регуляторов ГосСОПКА (НКЦКИ) и FinCERT (ЦБ РФ)

AM

Управление активами и инвентаризацией, поиск, категорирование, скрипты и жизненный цикл ПО и железа

VS

Поиск уязвимостей методами белого и черного ящиков с пентестом для активов, контейнеров и веб-сервисов

VM

Управление уязвимостями с автопатчингом, обогащением, расчетом SLA и поддержкой любых сканеров

SPC

Контроль параметров безопасности с харденингом и автоматизацией обновления политик до эталонных

КИИ

Аудит соответствия 187-ФЗ и сопутствующих подзаконных актов для поддержания критической инфраструктуры

CM

Комплаенс с десятками коробочных стандартов и возможностью загрузки любого набора НМД

RM

Управление рисками с количественными и качественными методиками оценки и тикетинг-системой

ORM

Управление операционными рисками и событиями ОР с мониторингом ключевых индикаторов (КИР) и задачами

BCM

Управление непрерывностью бизнеса с анализом влияния (BIA), планированием (BCP) и GAP-анализом

SA

Управление состоянием ИБ для групп компаний, холдингов и ДЗО с импортом различных стандартов

ЕДИНАЯ ПЛАТФОРМА на базе No- и Low-code

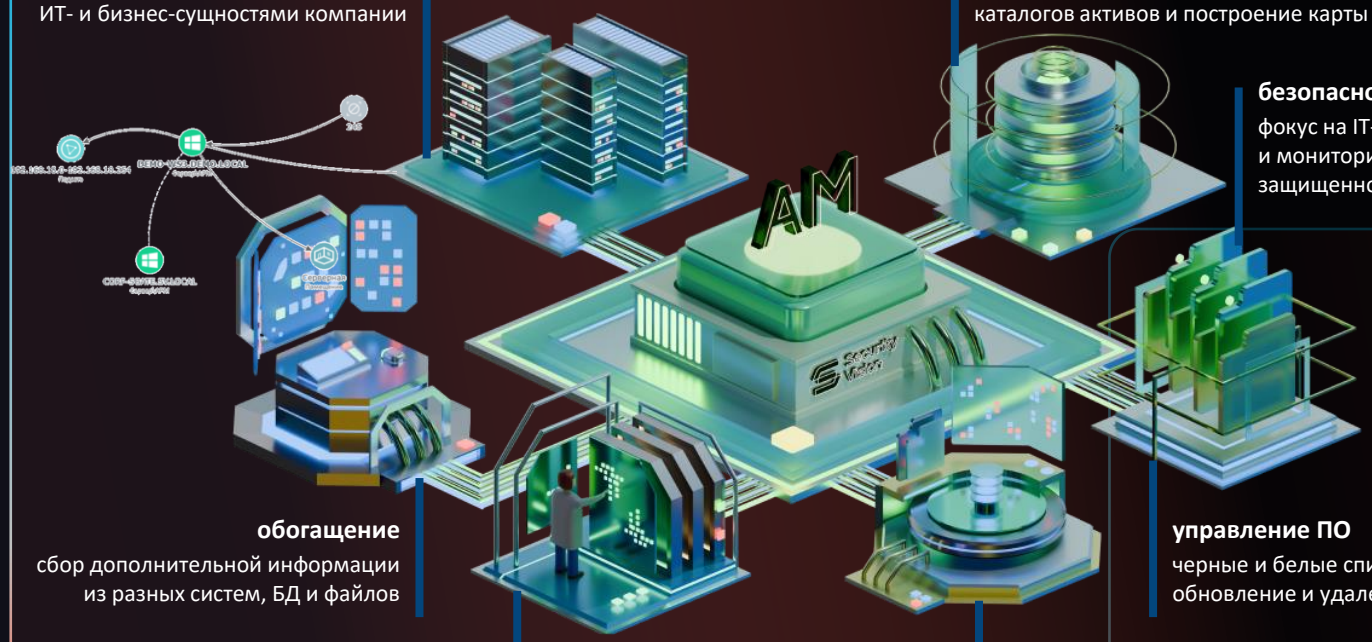
Конструкторы, не требующие навыков программирования для разработки собственных модулей и кастомизации логики работы и внешнего вида: объекты и карточки, коннекторы и интеграции, рабочие процессы, роли и меню, аналитика, дашборды и отчеты

УПРАВЛЕНИЕ АКТИВАМИ УЯЗВИМОСТЯМИ СО СКАНЕРОМ

ресурсно-сервисная модель
единая модель данных для связей с ИТ- и бизнес-сущностями компании

поиск объектов
сканирование по расписанию, формирование каталогов активов и построение карты сети

безопасность
фокус на IT-задачах и мониторинге защищенности



обогащение
сбор дополнительной информации из разных систем, БД и файлов

категорирование
фильтрация активов, поиск данных и связей между любыми объектами

жизненный цикл
фиксация изменений атрибутов объектов от их появления до вывода эксплуатации

управление ПО
черные и белые списки, обновление и удаление

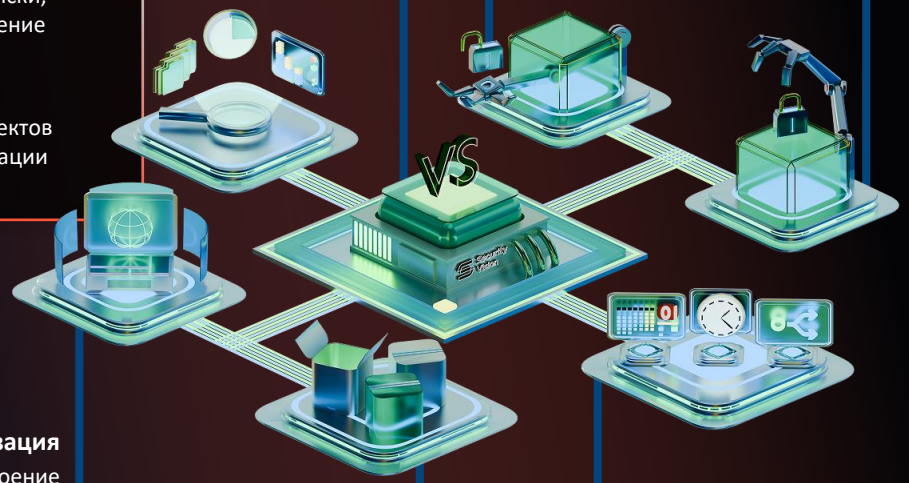
AM

Управление активами и инвентаризацией, поиск, категорирование, скрипты и жизненный цикл ПО и железа

ретро-скан
самый быстрый поиск уязвимостей без подключения

черный ящик
включая «пентест» с перебором паролей и алгоритмов шифрования

белый ящик
аудит и сканирование с полным доступом



инвентаризация
поиск активов и построение ресурсно-сервисной модели

контейнеры
открытые/закрытые контейнеры и их образы

гибкий Мультисканер
подключение любых сторонних средств и гранулярное управление режимами и графиком

VS

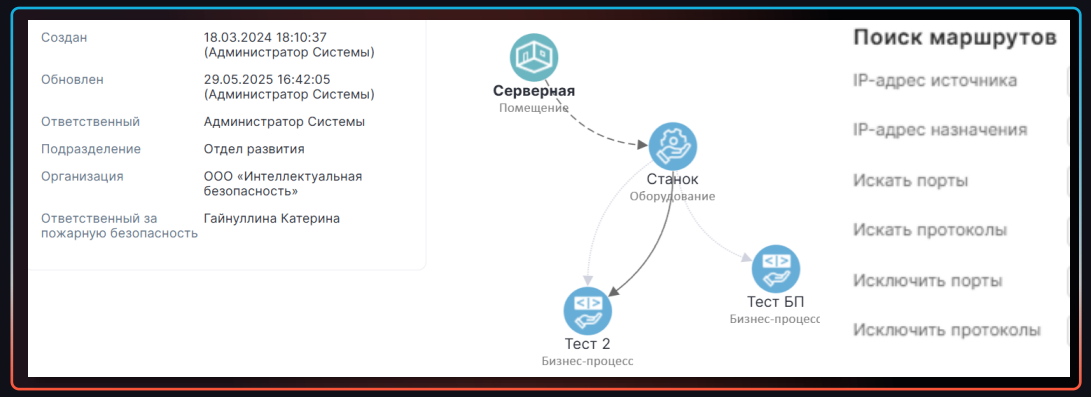
Поиск уязвимостей методами белого и черного ящиков с пентестом для активов, контейнеров и веб-сервисов

VM

Управление уязвимостями с автопатчингом, обогащением, расчетом SLA и поддержкой любых сканеров

ПРИМЕНЕНИЕ ИИ-ИНСТРУМЕНТОВ

ЦИТ ЦИФРОВЫЕ ИНДУСТРИАЛЬНЫЕ ТЕХНОЛОГИИ



поиск активов, которые могут в первую очередь подвергнуться атаке или были скомпрометированы

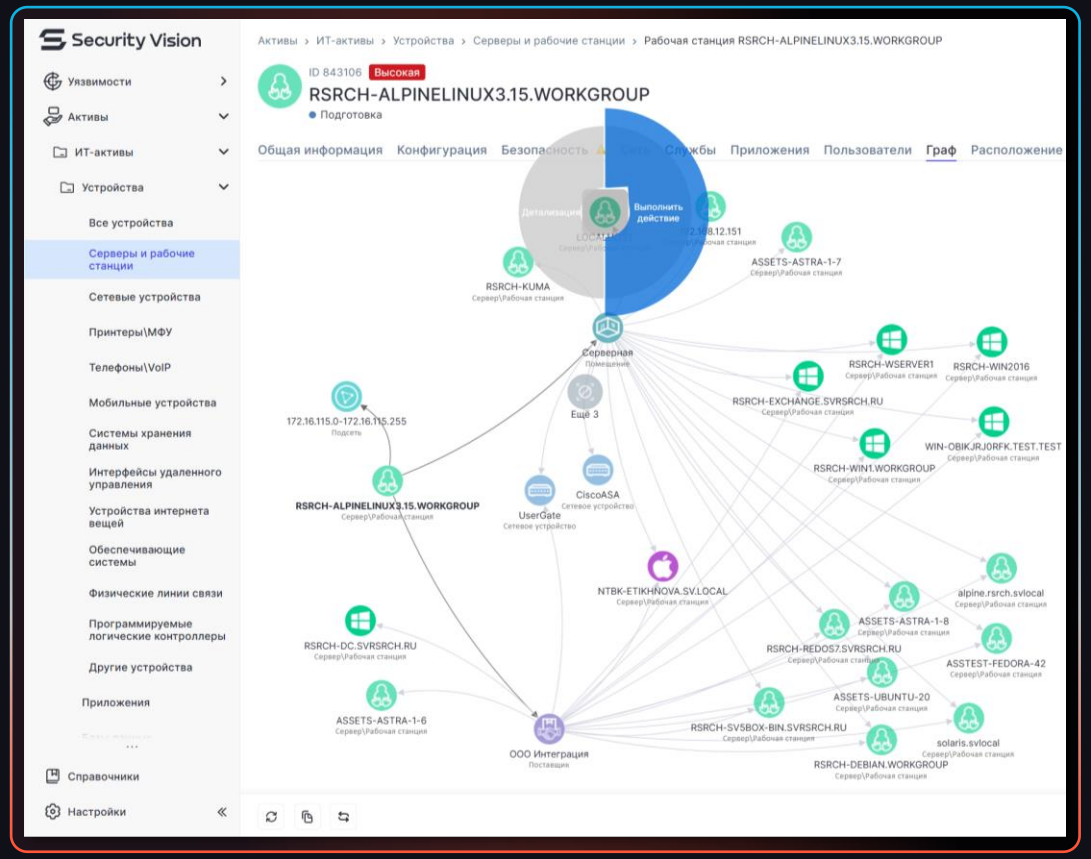
управление ПО и оборудованием через графы и массовые операции

1. расчет критичности уязвимостей **с учетом параметров активов** и данных о самой уязвимости

2. **черные/белые** списки ПО, **автопатчинг** и управление **обновлением/удалением** программ

3. **мультисканер** с поддержкой решений от **любых** производителей **в дополнение к собственному**

4. **черные/белые** списки ПО, **автопатчинг** и управление **обновлением/удалением** программ



УПРАВЛЕНИЕ ИНЦИДЕНТАМИ И АНАЛИЗ УГРОЗ

сбор алертов и подозрений на инциденты
интеграция СЗИ, макро-корреляция, группировка и дедупликация событий

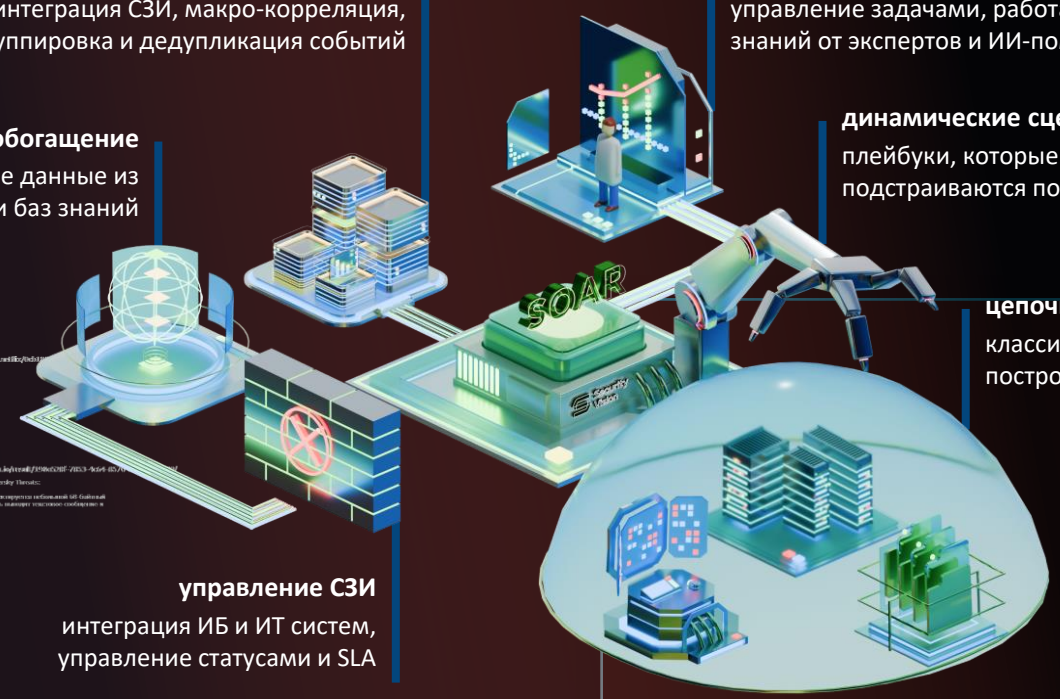
рекомендации для аналитиков
управление задачами, работа в группе, база знаний от экспертов и ИИ-помощники

обогащение
аналитические данные из внешних систем и баз знаний

динамические сценарии
плейбуки, которые автоматически подстраиваются под окружение

цепочки атак
классификация и построение kill-chain

управление СЗИ
интеграция ИБ и ИТ систем, управление статусами и SLA



SOAR

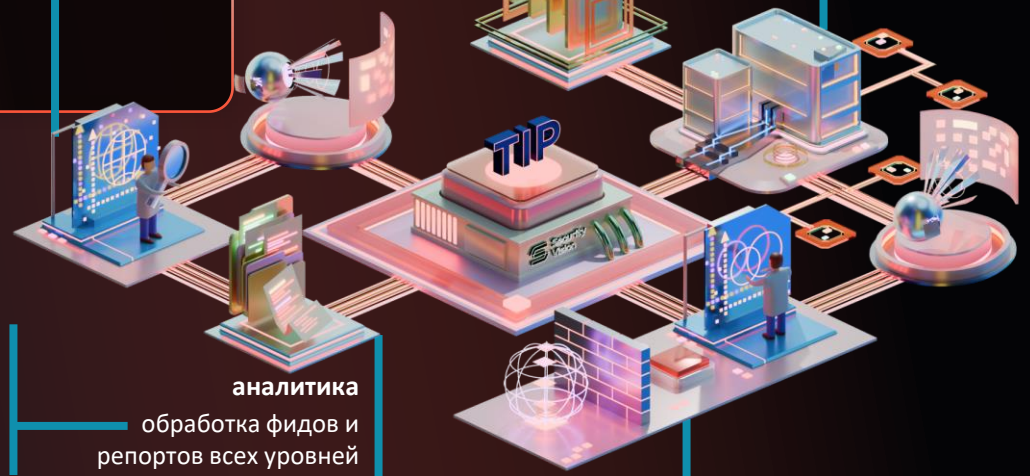
Управление инцидентами с динамическими плейбуками, объектно-ориентированным подходом и ИИ-помощниками

match «на лету»
обнаружение совпадений на трафике с DGA-алгоритмами

ретро-поиск
обнаружение совпадений по историческим данным

сбор фидов
интеграция с любыми данными и аналитическими центрами

поиск событий в периметре
интеграция с источниками «сырых» событий



TIP

Анализ угроз, киберразведка и threat hunting с интеграцией любых источников для ретро и потокового поиска с DGA

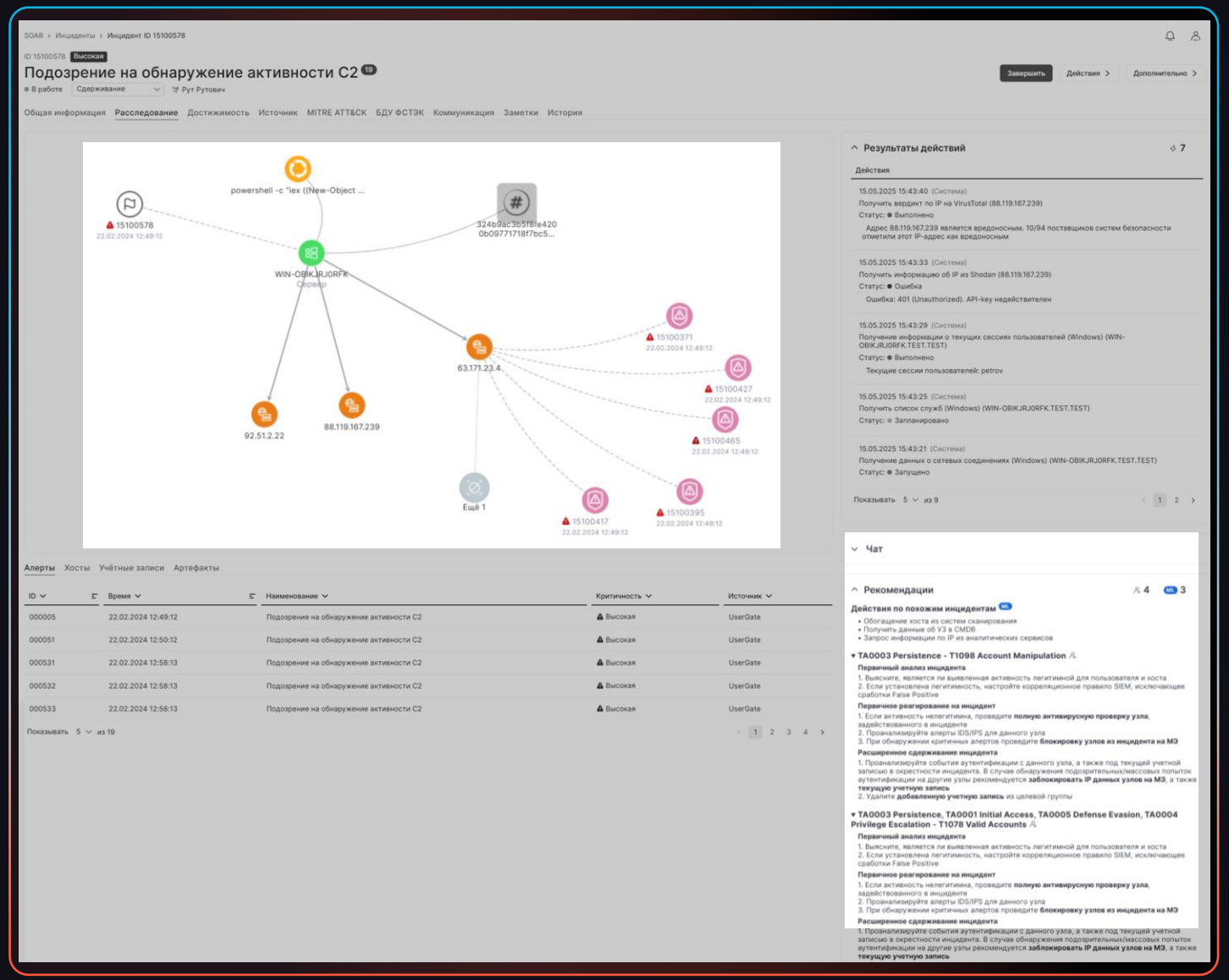
злоумышленники
ВПО
угрозы
уязвимости
IoA
домены
URL, Email
хэши
IP

стратегический
операционный
тактический
технический

аналитика
обработка фидов и репортов всех уровней

встроенное реагирование
вероятности реализации угроз и эффективность мер защиты

ИИ-РЕКОМЕНДАЦИИ И ПОИСК ПОХОЖИХ



сбор **алертов** и **инцидентов** с динамическими сценариями, **подстраивающимися под окружение**

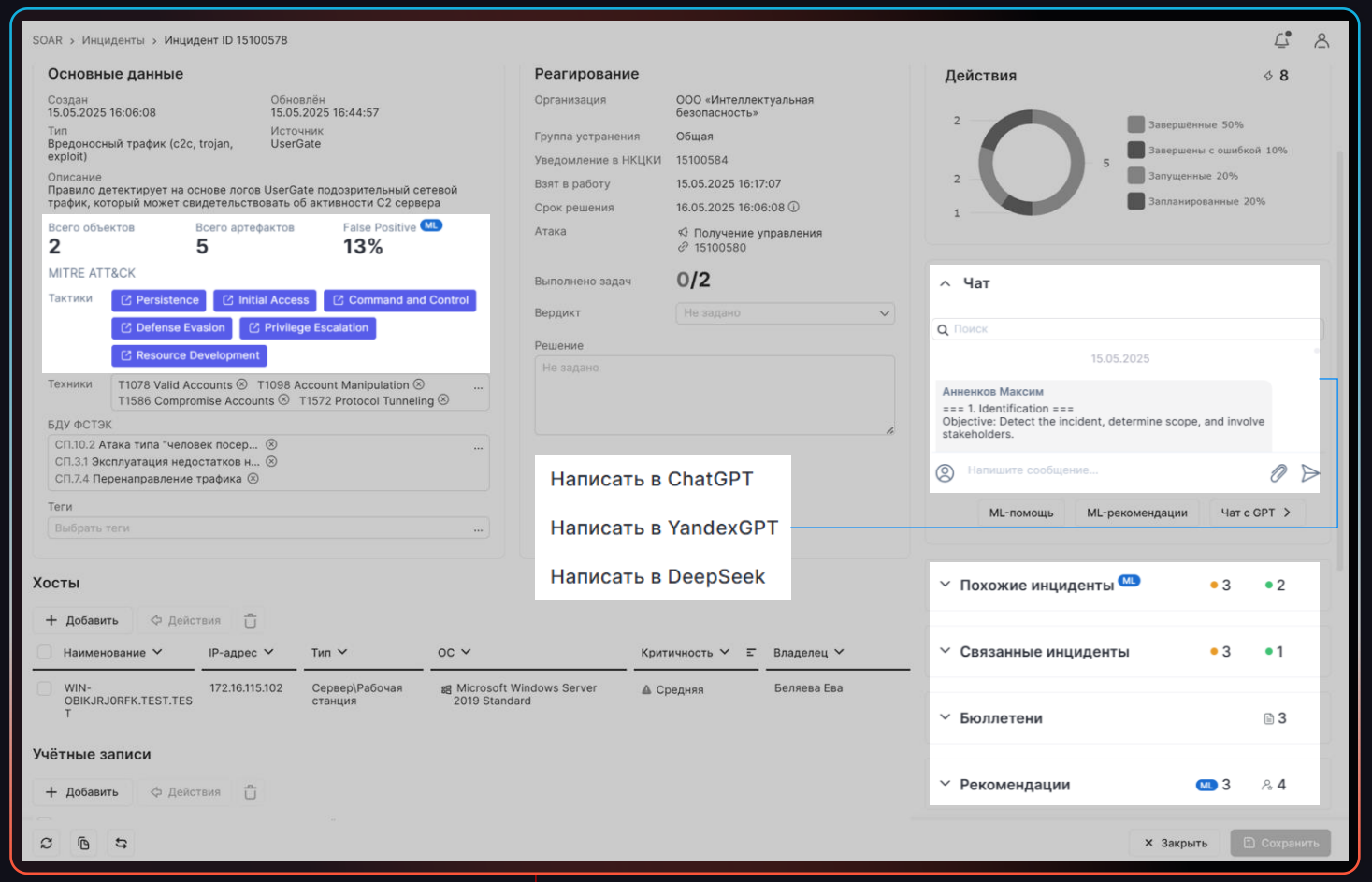
DGA-алгоритмы, анализ IoC и бюллетеней **Random, wordlist, phishing**

анализ **базы знаний** и **истории действий** с объектами для **помощи аналитикам**

скоринг False Positive и поиск похожих **анализ вердиктов инцидентов с оценкой**

графы достижимости с маршрутами нарушителей и ACL алгоритмами

АНАЛИЗ ВЕРДИКТОВ И ЛПС



интеграция с внешними сервисами

ChatGPT, YandexGPT, DeepSeek, и др.

обработка бюллетеней и индикаторов

Анализ угроз и киберразведка

помощь с документацией

вопрос по продукту прямо в чате

Модель обучается на вердиктах проставляемых инцидентам при закрытии, чем больше конкретный инцидент похож на ранее закрытые с вердиктом False Positive, тем выше данный показатель

ПОВЕДЕНЧЕСКИЙ АНАЛИЗ И ПОИСК АНОМАЛИЙ

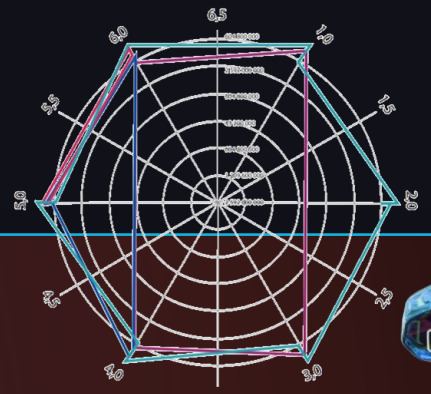
UEBA

Поведенческий анализ для поиска аномалий при помощи ML-моделей, статистических методов и корреляции

Полная управляемость

Комбинирование технологий

Анализ неочевидного

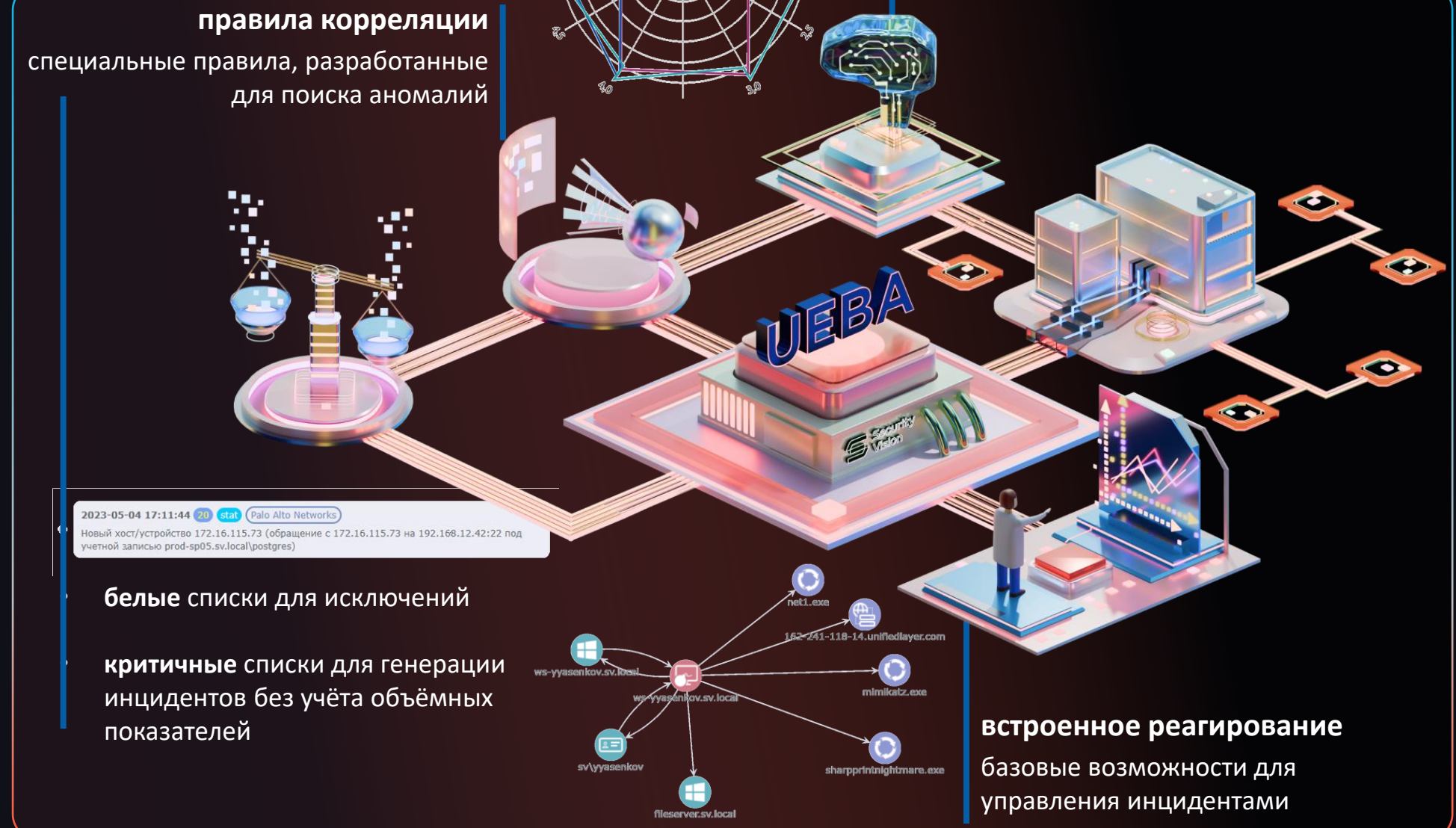


машинное обучение

предобученные модели и обучение на текущем трафике

правила корреляции

специальные правила, разработанные для поиска аномалий



белые списки для исключений

критичные списки для генерации инцидентов без учёта объёмных показателей

встроенное реагирование

базовые возможности для управления инцидентами

ЦИТ
ЦИФРОВЫЕ
ИНДУСТРИАЛЬНЫЕ
ТЕХНОЛОГИИ

СПАСИБО ЗА ВНИМАНИЕ!

cit.gov.ru