

ЦИТ

ЦИФРОВЫЕ
ИНДУСТРИАЛЬНЫЕ
ТЕХНОЛОГИИ

ПЛАТФОРМА АВТОМАТИЗАЦИИ ПРОЦЕССОВ ИБ И ИТ

Каталог ИИ-решений

ЕДИНАЯ ПЛАТФОРМА С НАБОРОМ МОДУЛЕЙ

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

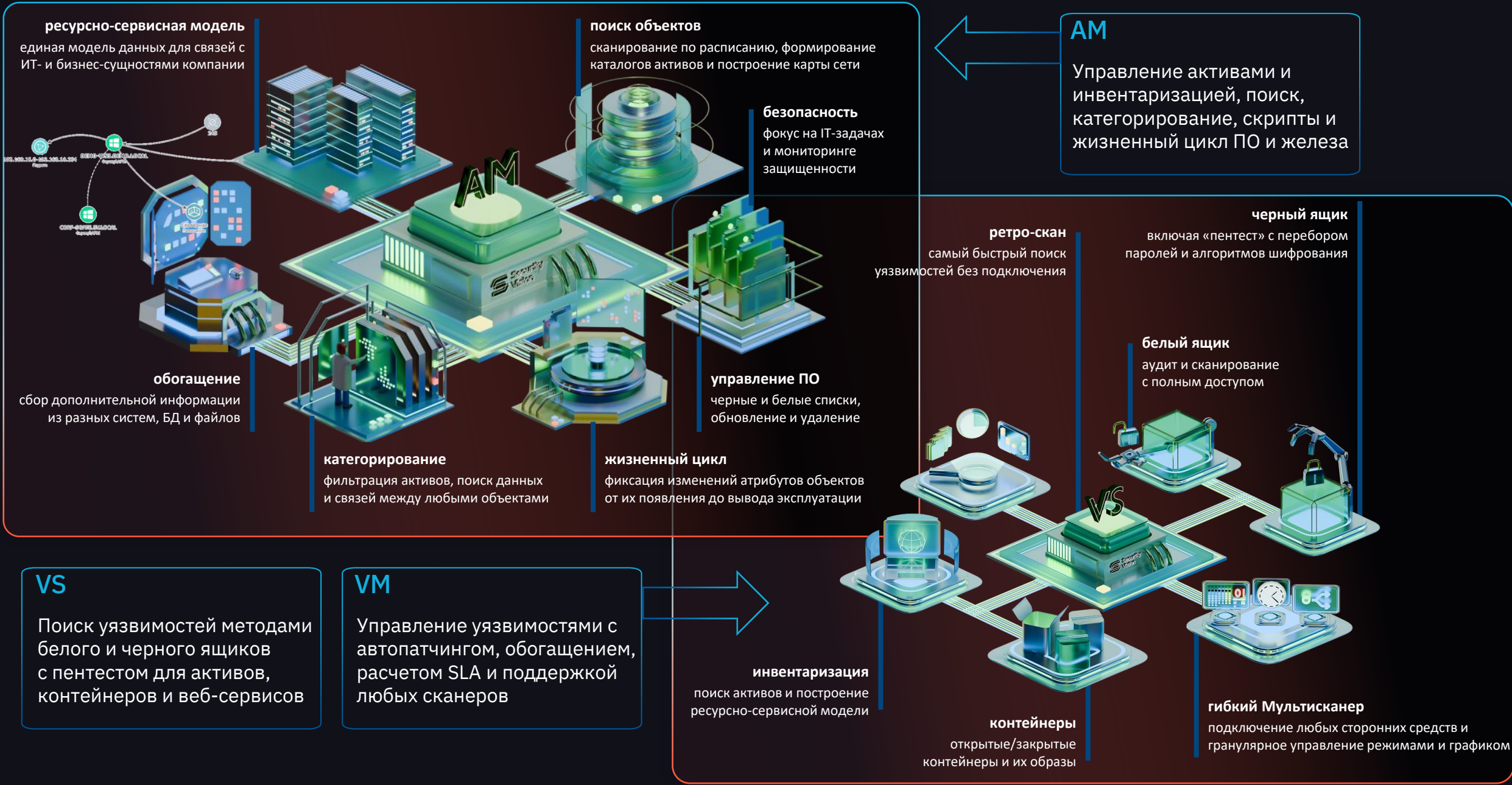
SA

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



ПРИМЕНЕНИЕ ИИ-ИНСТРУМЕНТОВ

Создан	18.03.2024 18:10:37 (Администратор Системы)
Обновлен	29.05.2025 16:42:05 (Администратор Системы)
Ответственный	Администратор Системы
Подразделение	Отдел развития
Организация	ООО «Интеллектуальная Безопасность»
Ответственный за пожарную безопасность	Гайнуллина Катерина

Поиск маршрутов

- IP-адрес источника
- IP-адрес назначения
- Искать порты
- Искать протоколы
- Исключить порты
- Исключить протоколы

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

ИИ-РЕКОМЕНДАЦИИ И ПОИСК ПОХОЖИХ

SOAR > Инциденты > Инцидент ID 15100578

ID 15100578 **Высокая**

Подозрение на обнаружение активности C2 ¹⁹

В работе | Сдерживание | Руслан Рутенко

Общая информация | **Расследование** | Достижимость | Источники | MITRE ATT&CK | БДУ ФСТЭК | Коммуникация | Заметки | История

Результаты действий 7

Действия

- 15.05.2025 15:43:40 (Система)
Получить вердикт по IP на VirusTotal (88.119.167.239)
Статус: **Выполнено**
Адрес 88.119.167.239 является вредоносным. 10/94 поставщиков систем безопасности отметили этот IP-адрес как вредоносный
- 15.05.2025 15:43:33 (Система)
Получить информацию об IP из Shodan (88.119.167.239)
Статус: **Ошибка**
Ошибка: 401 (Unauthorized). API-key недействителен
- 15.05.2025 15:43:29 (Система)
Получение информации о текущих сессиях пользователей (Windows) (WIN-OBIKJRJORKF.TEST.TEST)
Статус: **Выполнено**
Текущие сессии пользователей: petrov
- 15.05.2025 15:43:25 (Система)
Получить список служб (Windows) (WIN-OBIKJRJORKF.TEST.TEST)
Статус: **Запланировано**
- 15.05.2025 15:43:21 (Система)
Получение данных о сетевых соединениях (Windows) (WIN-OBIKJRJORKF.TEST.TEST)
Статус: **Запущено**

Показывать 5 из 9

Чат

Рекомендации 4 3

Действия по похожим инцидентам

- Обладание хоста из системы сканирования
- Получить данные об УЗ в CMDB
- Запрос информации по IP из аналитических скриптов

TA0003 Persistence - T1098 Account Manipulation

Первичный анализ инцидента

- Выясните, является ли выявленная активность легитимной для пользователя и хоста
- Если установлена легитимность, настройте корреляционное правило SIEM, исключающее срабатывание False Positive

Первичное реагирование на инцидент

- Если активность нелегитимна, проведите полную антивирусную проверку узла, задействованного в инциденте
- Проанализируйте alerty IDS/IPS для данного узла
- При обнаружении критичных alertov проведите блокировку узлов из инцидента на МЭ

Расширенное сдерживание инцидента

- Проанализируйте события аутентификации с данного узла, а также под текущей учетной записью в окрестности инцидента. В случае обнаружения подозрительных/массовых попыток аутентификации на другие узлы рекомендуется **заблокировать IP данных узлов на МЭ**, а также **текущую учетную запись**
- Удалите добавленную учетную запись из целевой группы

TA0003 Persistence, TA0001 Initial Access, TA0005 Defense Evasion, TA0004 Privilege Escalation - T1078 Valid Accounts

Первичный анализ инцидента

- Выясните, является ли выявленная активность легитимной для пользователя и хоста
- Если установлена легитимность, настройте корреляционное правило SIEM, исключающее срабатывание False Positive

Первичное реагирование на инцидент

- Если активность нелегитимна, проведите полную антивирусную проверку узла, задействованного в инциденте
- Проанализируйте alerty IDS/IPS для данного узла
- При обнаружении критичных alertov проведите блокировку узлов из инцидента на МЭ

Расширенное сдерживание инцидента

- Проанализируйте события аутентификации с данного узла, а также под текущей учетной записью в окрестности инцидента. В случае обнаружения подозрительных/массовых попыток аутентификации на другие узлы рекомендуется **заблокировать IP данных узлов на МЭ**, а также **текущую учетную запись**

ID	Время	Наименование	Критичность	Источник
000005	22.02.2024 12:49:12	Подозрение на обнаружение активности C2	Высокая	UserGate
000051	22.02.2024 12:50:12	Подозрение на обнаружение активности C2	Высокая	UserGate
000531	22.02.2024 12:58:13	Подозрение на обнаружение активности C2	Высокая	UserGate
000532	22.02.2024 12:58:13	Подозрение на обнаружение активности C2	Высокая	UserGate
000533	22.02.2024 12:58:13	Подозрение на обнаружение активности C2	Высокая	UserGate

Показывать 5 из 19

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

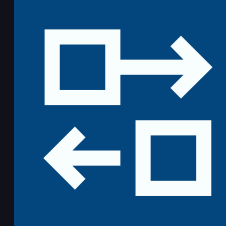
скоринг False Positive и поиск похожих анализ вердиктов инцидентов с оценкой

графы достижимости с маршрутами нарушителей и ACL алгоритмами



АНАЛИЗ ВЕРДИКТОВ И ЛПС

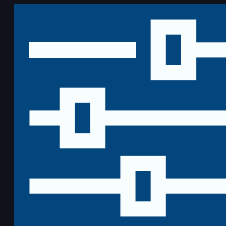
The screenshot shows a SOAR interface for incident ID 15100578. The main content area is divided into several sections: 'Основные данные' (Basic info), 'Реагирование' (Response), 'Действия' (Actions), 'Хосты' (Hosts), and 'Учётные записи' (Credentials). A chat window is open, displaying a message from 'Анненков Максим' with the text: '=== 1. Identification === Objective: Detect the incident, determine scope, and involve stakeholders.' Below the chat window, there are buttons for 'ML-помощь', 'ML-рекомендации', and 'Чат с GPT'. A white tooltip box is overlaid on the chat window, containing the text: 'Написать в ChatGPT', 'Написать в YandexGPT', and 'Написать в DeepSeek'. The 'Действия' section shows a donut chart with 5 total actions, where 2 are completed (40%), 2 are in progress (40%), and 1 is planned (20%). The 'Хосты' section shows a table with columns for Name, IP, Type, OS, Criticality, and Owner. The 'Учётные записи' section shows a table with columns for Name, IP, Type, OS, Criticality, and Owner.



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 предоставляемых 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



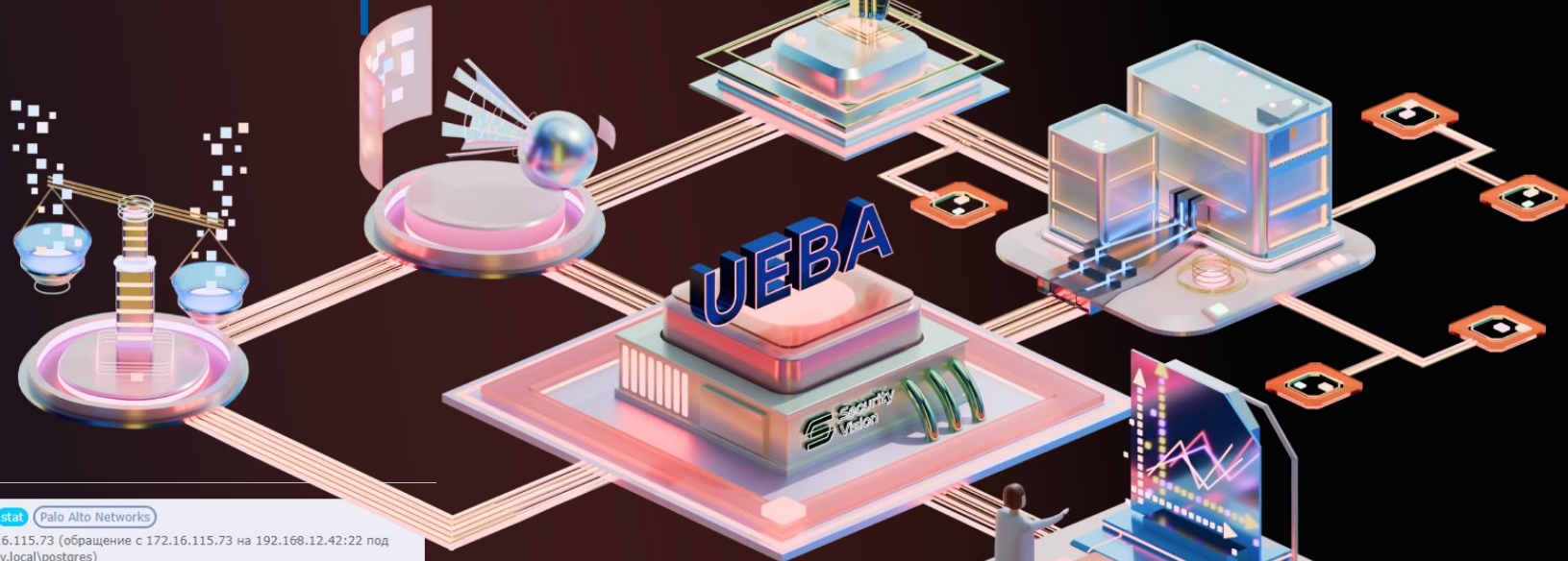
Комбинирование
технологий



Анализ
неочевидного

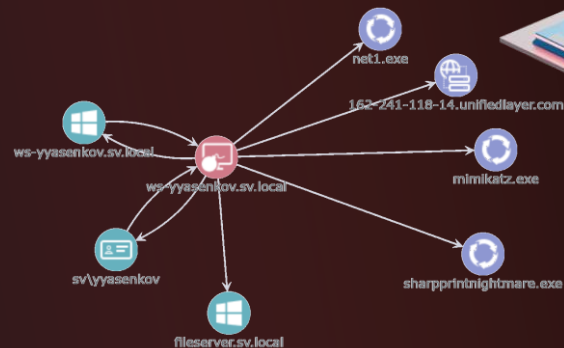
правила корреляции

специальные правила, разработанные для поиска аномалий



белые списки для исключений

критичные списки для генерации инцидентов без учёта объёмных показателей



машинное обучение

предобученные модели и обучение на текущем трафике

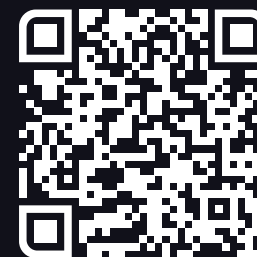
встроенное реагирование

базовые возможности для управления инцидентами

ЦИТ

ЦИФРОВЫЕ
ИНДУСТРИАЛЬНЫЕ
ТЕХНОЛОГИИ

СПАСИБО ЗА ВНИМАНИЕ!



cit.gov.ru

