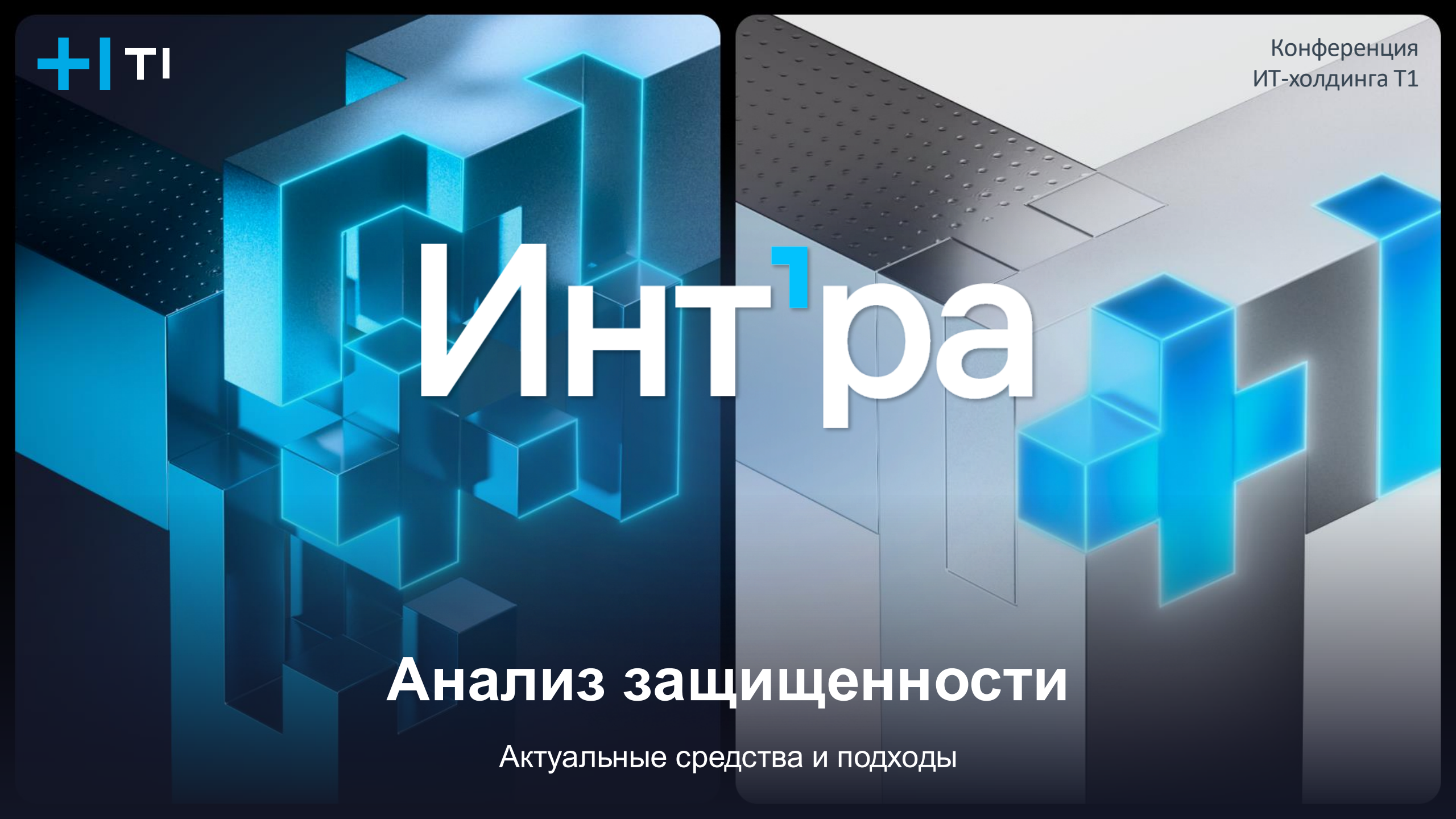
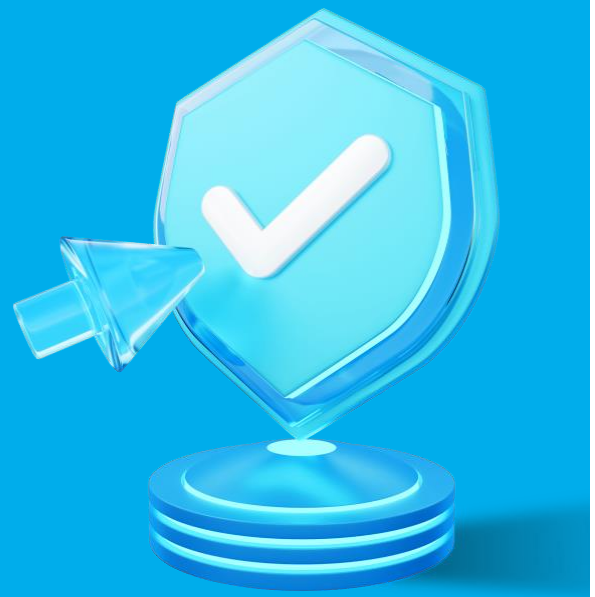

Конференция
ИТ-холдинга Т1
Инт ра
Анализ защищенности
Актуальные средства и подходы

Анализ защищенности

Интра

Что хотим выявить

+ Ранее неинвентаризированные активы, получить максимально актуальную информацию
+ Неисправленные или неизвестные уязвимости
+ Теневые ИТ и неуправляемые устройства
+ Неправильные настройки СЗИ и политики безопасности
+ Развивающиеся угрозы и методы



Наиболее близкие нормативные документы

+ ГОСТ Р ИСО/МЭК 27004-2021 Мониторинг, оценка защищенности, анализ и оценивание
+ Информационное письмо Банка России от 21 июля 2023 г. № ИН-017-56/48 «О порядке проведения оценки соответствия защиты информации»
+ ГОСТ Р 57580.2-2018 ЗАЩИТА ИНФОРМАЦИИ ФИНАНСОВЫХ ОРГАНИЗАЦИЙ. Методика оценки соответствия
+ Методика оценки показателя состояния технической защиты информации и обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации (утв. ФСТЭК России 2 мая 2024 г.)
+ NIST SP 800-115 Technical Guide to Information Security Testing and Assessment

Концепция Continuous Threat Exposure Management (CTEM)

Инт'ра

Шаг 1

Масштаб (Scope)

Шаг 2

Идентификация (Discovery)

Шаг 3

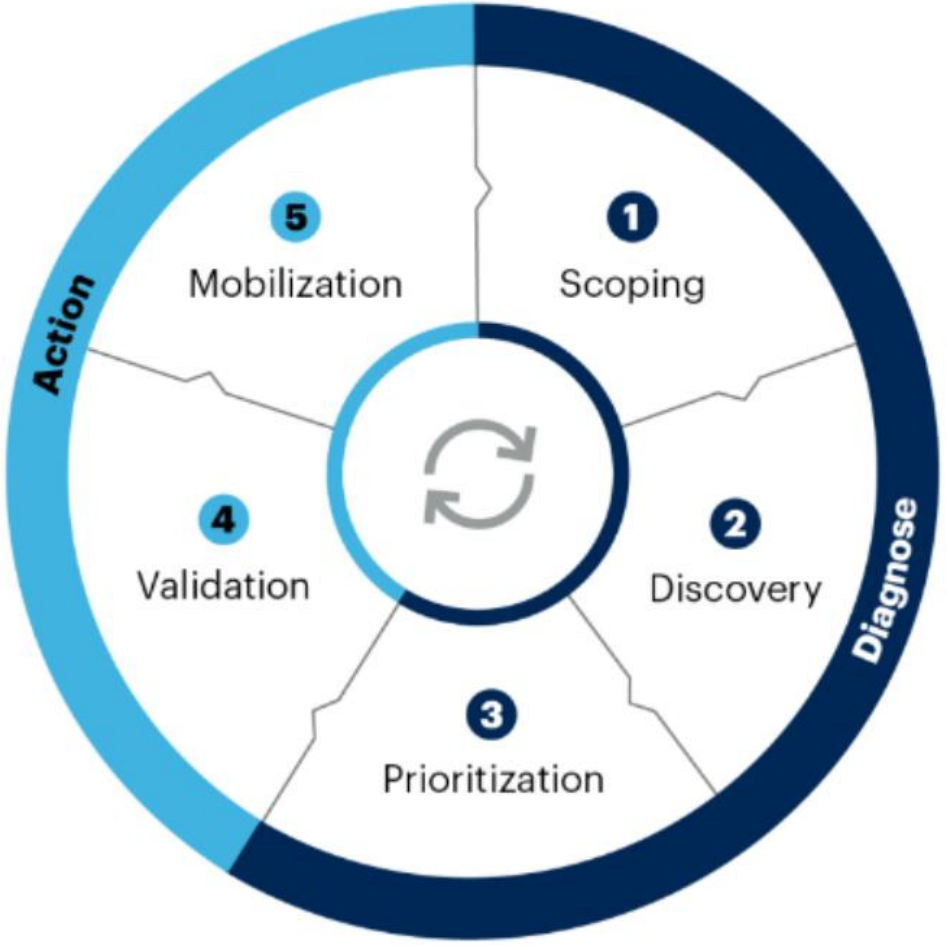
Приоритезация (Prioritization)

Шаг 4

Валидация (Validation)

Шаг 5

Мобилизация (Mobilization)



Стандартные VM, средства для выявления уязвимостей

Инт'ра

Что это — стандартные средства для автоматизации поиска уязвимостей сетевым и/или агентским методом

Для чего — для выявления известных уязвимостей

Недостатки

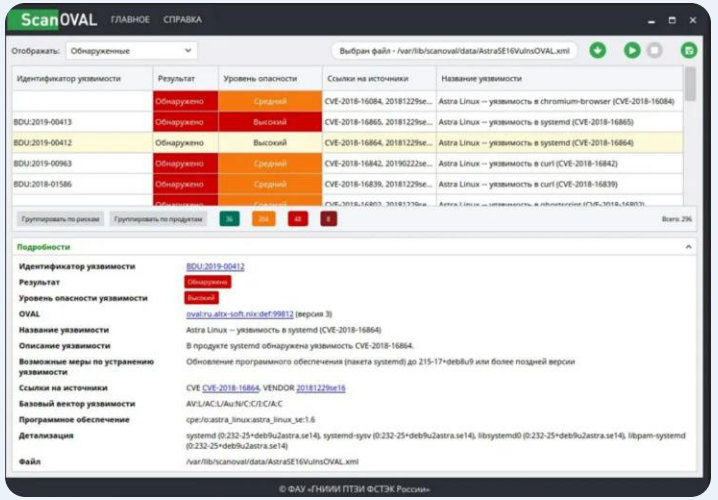
+ Большое количество сработок на достаточно крупной инфраструктуре
+ Большое количество False Positive
+ Необходимость дополнительной приоритезации
+ Нет проверки политик безопасности и учета компенсирующих мер

Одна из самых больших задач — корректно проанализировать результаты сканирования

OVAL/SCAP инструменты

***Для исключения ложных срабатываний при контроле защищенности ИС под управлением ОС Astra Linux, необходимо руководствоваться:**

+ актуальным списком устраненных уязвимостей
+ перечнями устраненных и неактуальных уязвимостей ОС Astra Linux, представленными в формате, используемом средствами анализа защищенности в качестве источника сведений об уязвимостях (OVAL-описания)



* https://wiki.astralinux.ru/pages/viewpage.action?pageId=331355418&ysclid=m7todfz49p421456004

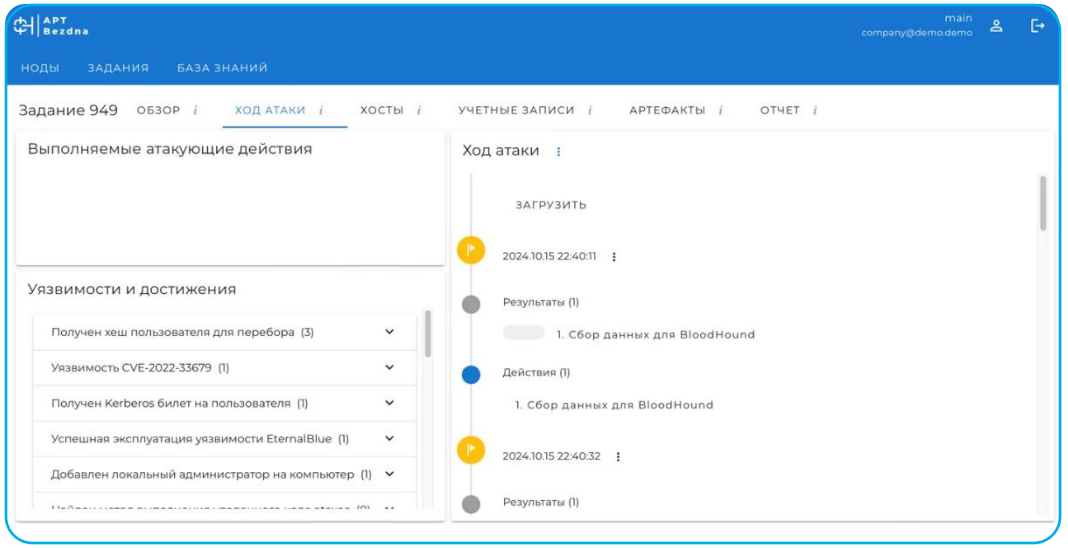
Breach and Attack Simulation (BAS)

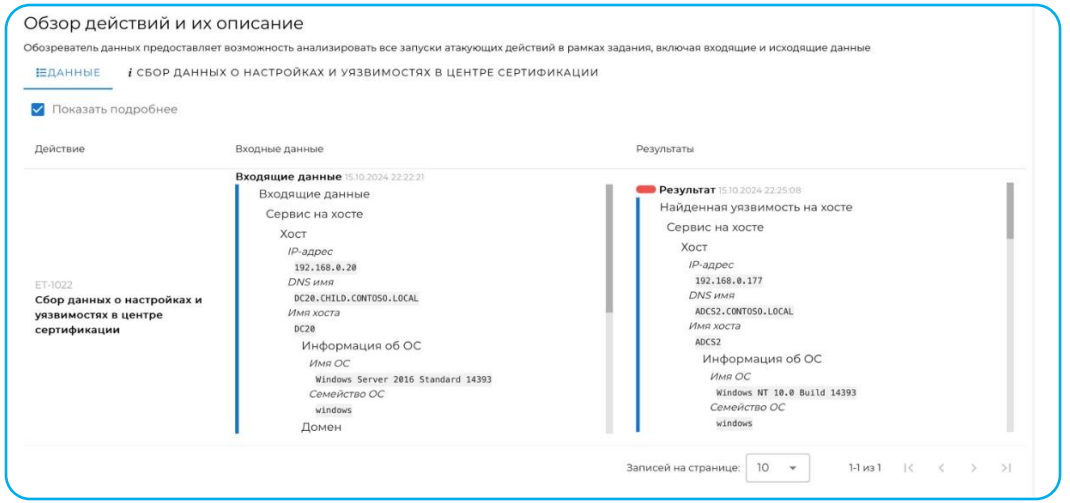
Инт'ра

Что это — средство для непрерывной оценки защищённости ИС, имитирующее действия злоумышленника

Для чего

+ непрерывный анализ защищённости/пентест
+ проверка функционирования внедрённых СЗИ (корректность настройки, проверка на уязвимости)
+ проверка работы службы реагирования на инциденты
+ проверка корректности настройки сегментирования сети и сетевых правил при симуляции реальной атаки
+ помощь в выявлении в SOC и SIEM того, насколько хорошо инфраструктура охвачена сбором событий





Network Security policy manager (NSPM)

Интра

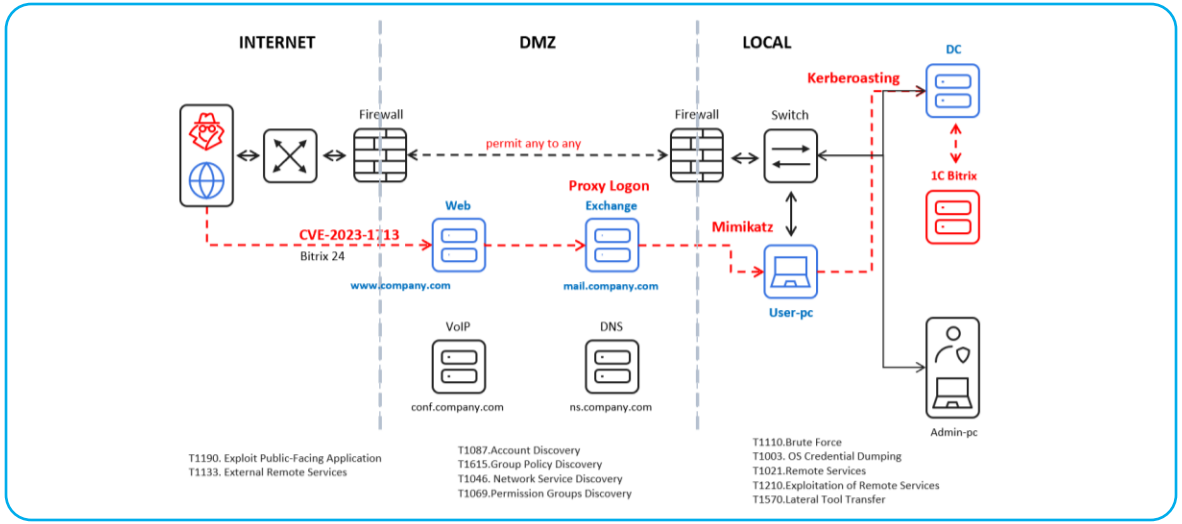
Что это — средства проверки политик безопасности сетевых устройств

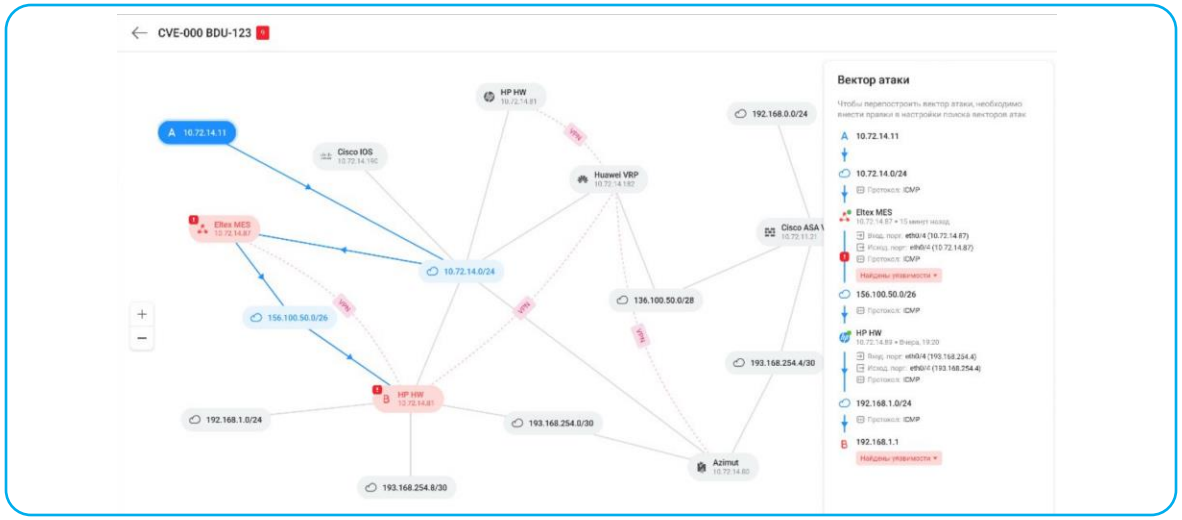
Для чего

+ Поиск уязвимостей на сетевых устройствах (МЭ, NGFW, маршрутизаторы, коммутаторы)
+ Построение векторов атак с учетом известных уязвимостей и существующей инфраструктуры защиты
+ Оценка исполнения требований по настройке сетевых политик, автоматизированных аудит политик

Преимущества

+ Позволяет строить вектора атак с учетом всех политик СЗИ
+ Позволяет проверять корректность настройки политик
+ Позволяет проверять исполнение требований безопасности





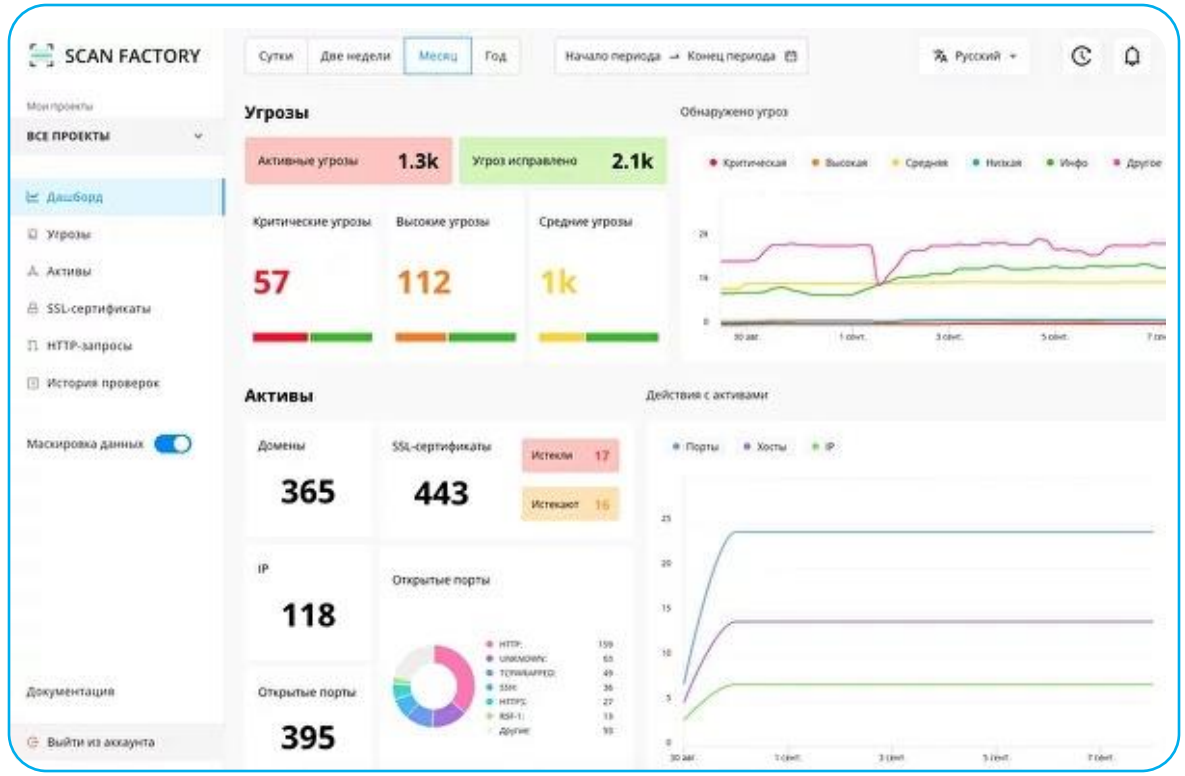
External Attack Surface Management (EASM)

Инт'ра

Что это — система для управление внешними поверхностями атак — механизм, который в режиме реального времени позволяет отслеживать уязвимости в распределенных цифровых активах компании

Для чего

+ Разведка по открытым источникам и выявление «теневых» ресурсов
+ Обнаружение фишинговых сайтов
+ Обнаружение ресурсов, доступные из сети Интернет
+ Поиск упоминаний в утечках информации на хакерских форумах
  - Подготовка атак
  - Мониторинг утечек учётных записей в открытых источниках



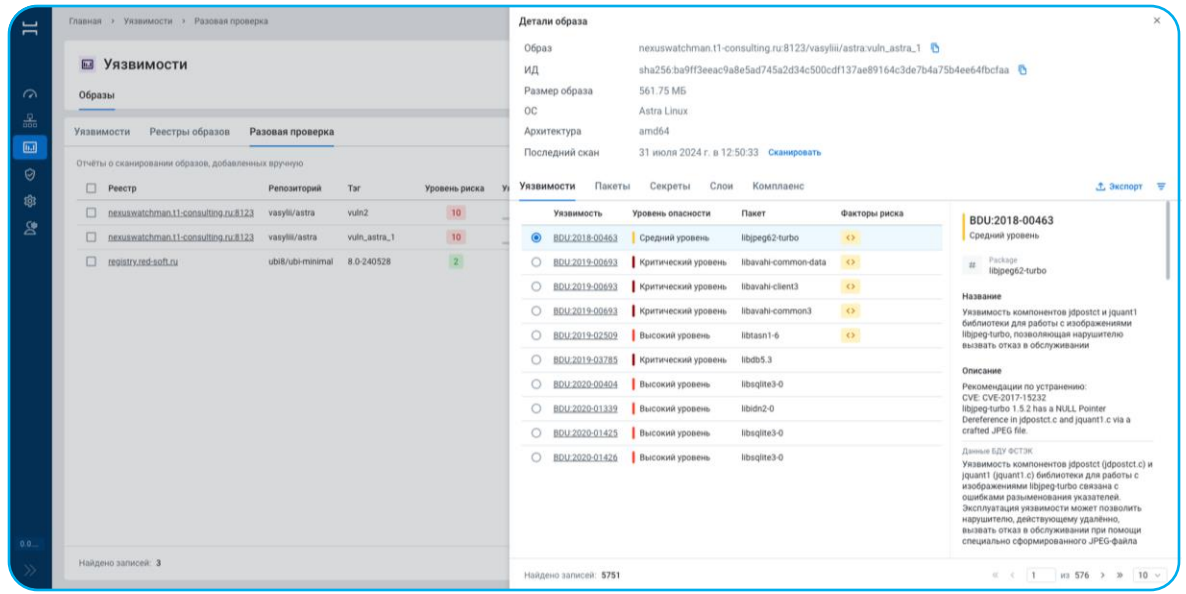
Container security (CS)

Инт¹ра

Что это — система для анализа защищенности контейнерных сред

Для чего

+ Сканирование на уязвимости образов и ПО внутри образов, классификация, приоритезация
+ Поиск вредоносного ПО внутри образов
+ Подпись и проверка целостности образов
+ Проверка требований в части настроек политик безопасности (Compliance)



Что ещё

Что не рассмотрели

1

Continuous Penetration Testing (CPT)

2

DAP — Database audit and protection

3

DCAP — Data-Centric Audit and Protection

4

CASB — Cloud Access Security Broker

5

Cloud Native Application Protection Platform (CNAPP)

6

Средства DevSecOps

7

BugBounty

Приоритезация уязвимостей

Инт¹ра

Большинство компаний не принимали во внимание уровень опасности уязвимости (76%), ее трендовость и наличие публичного эксплойта (59%)*

Системы приоритезации

Иностранные методы

+ CVSS 4.0
+ Exploit Prediction Scoring System (EPSS)
+ SSVC (Stakeholder-Specific Vulnerability Categorization)
+ Vulners AI Score
+ VISS (Vulnerability Impact Scoring System)
+ SSPP (Stakeholder-Specific Patching Prioritization)

Российские методы

+ Методика оценки уровня опасностей уязвимостей ФСТЭК
+ Подход НКЦКИ по решению для обновления ПО

Инструменты для приоритезации

CISA KEV | CVEShield | CVE Crowd | CVE Prioritizer

* https://www.ptsecurity.com/ru-ru/research/analytics/problems-in-vulnerability-management-and-how-to-solve-them/

Приоритезация уязвимостей

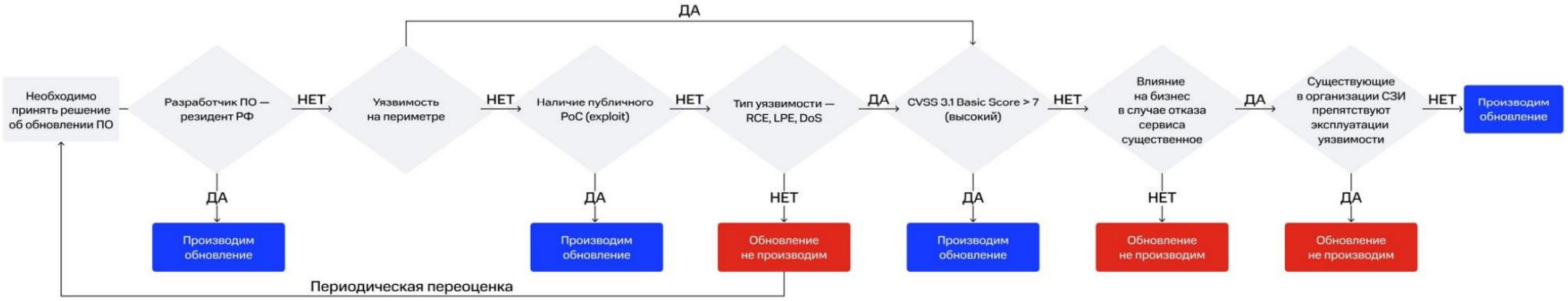
Интра

Stakeholder-Specific Vulnerability Categorization (SSVC)

+ **(State of) exploitation** — возможность эксплуатации уязвимости («нет», «есть публичный POC» или «активно эксплуатируется»)
+ **Technical impact** — уровень воздействия на систему (полное воздействие или частичное)
+ **Automatable** — автоматизированы ли шаги 1–4 цепочки атаки (kill chain); да или нет
+ **Mission prevalence** — на какие системы (с точки зрения опасности для жизнедеятельности организации) влияет уязвимость
+ **Public well-being impact** — какой ущерб (физический, психологический, социальный или эмоциональный) может быть нанесен человеку в случае использования уязвимости

SSVC 2.0

+ **Utility** — преимущества, которые получает злоумышленник от эксплуатации уязвимости
+ **Value density** — какие ресурсы получит злоумышленник в случае эксплуатации уязвимости
+ **Public safety impact, situated safety impact, human impact** — расширяют понятие public well-being impact из первой версии SSVC
+ **System exposure** — доступность системы для атаки



Конференция
ИТ-холдинга Т1

Инт'ра

Игорь Душа
Директор портфеля решений экосистемы в области информационной безопасности НОТА КУПОЛ

idusha@nota.tech

Спасибо за внимание!