CyberRes

ArcSight Platform

Необходимые возможности аналитики в мире современных угроз

Vyacheslav Tupikov
ArcSight Solutions Architect

Содержание

Что такое CyberRes?

CyberRes – это выделенное направление бизнеса компании Micro Focus, занимающееся созданием продуктов и сервисов в области информационной безопасности.

Имя отражает нашу новую глобальную идеологию продуктов для обеспечения киберустойсивости (Cyber Resiliency).

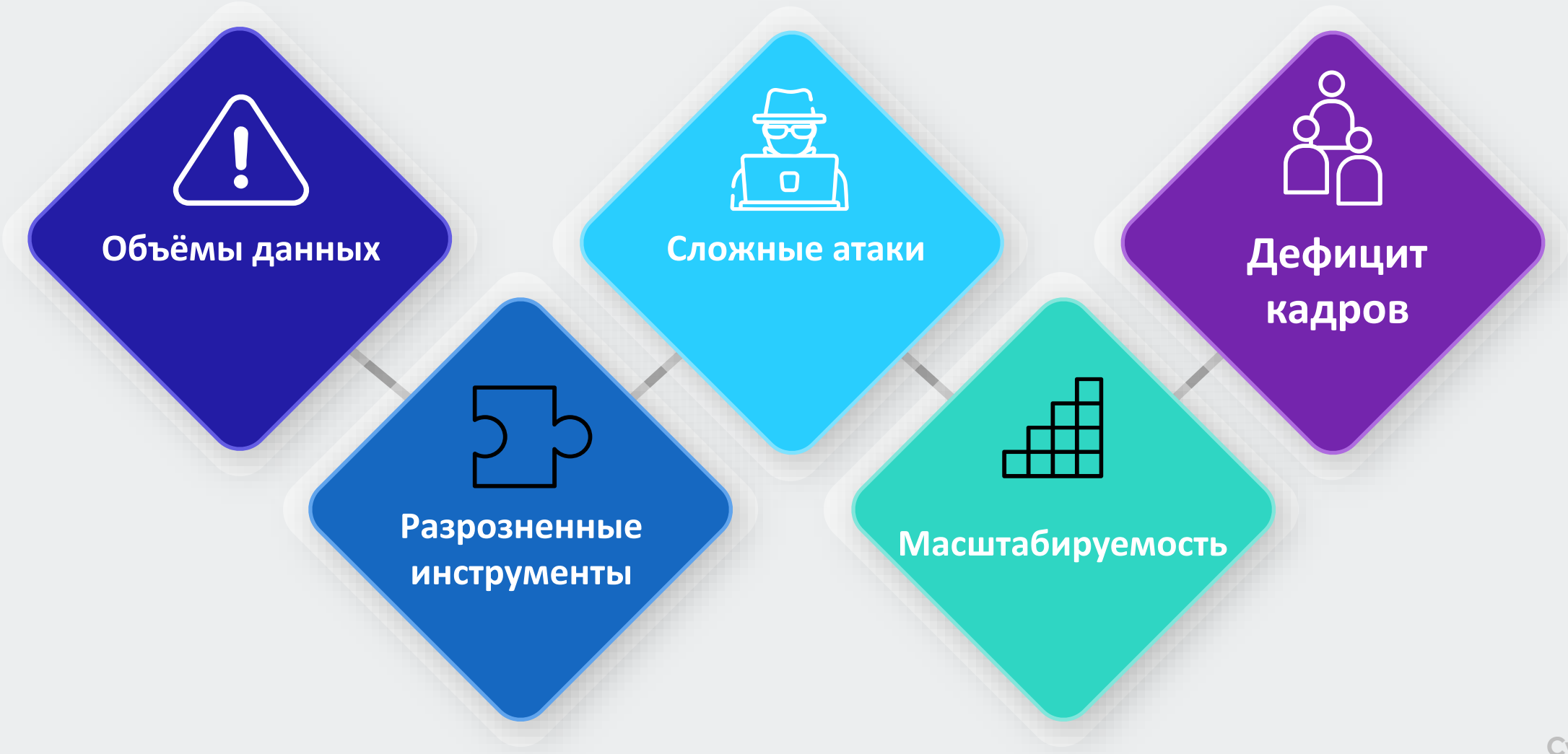
Что такое CyberRes?

CyberRes объединяет следующие семейства продуктов:

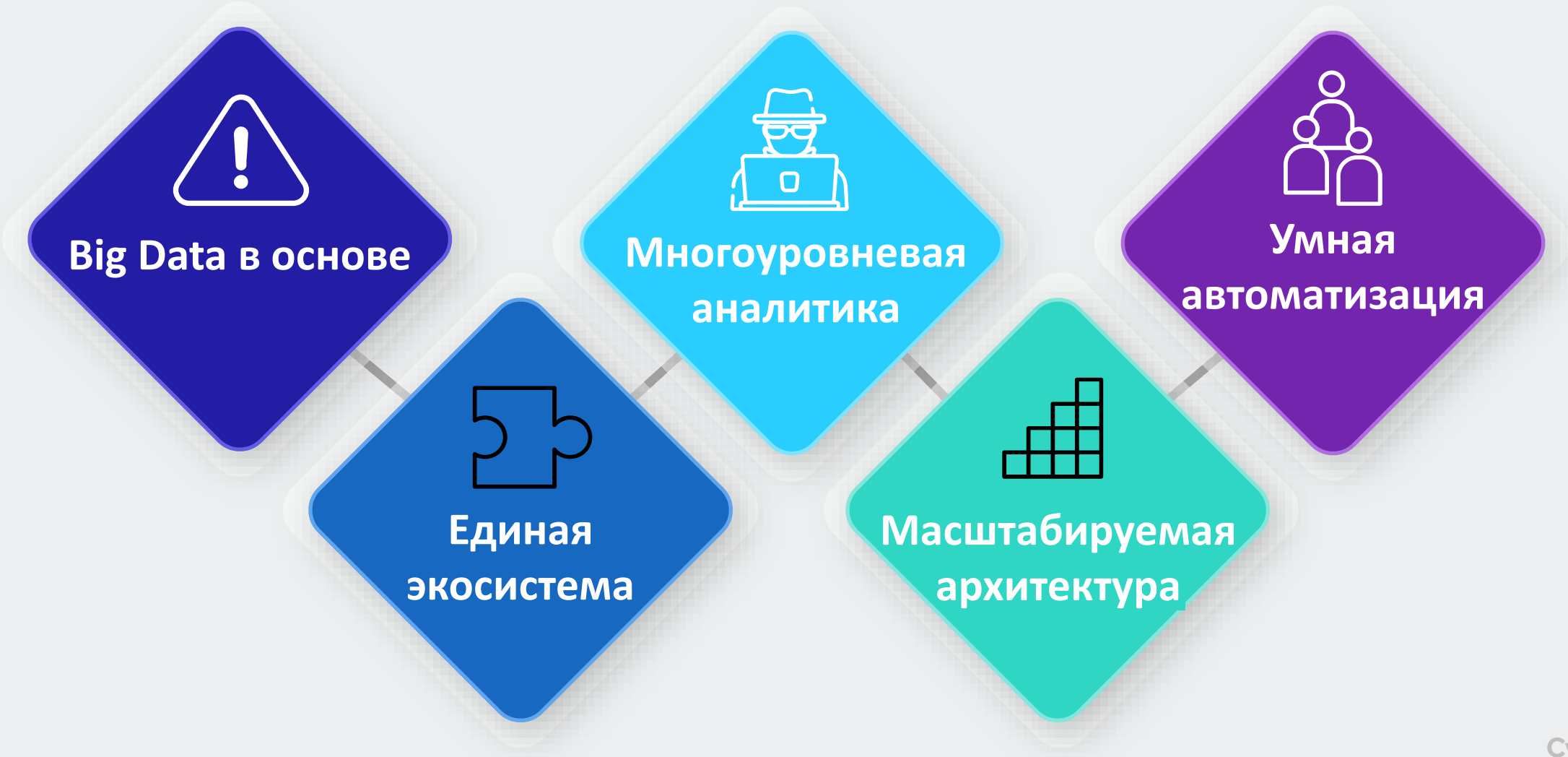
- ArcSight – Security Operations
- Fortify – Application Security
- Interset – Artificial Intelligence
- NetIQ – Identity and Access Management
- Voltage – Data Privacy and Protection

Потребности SecOps сегодня

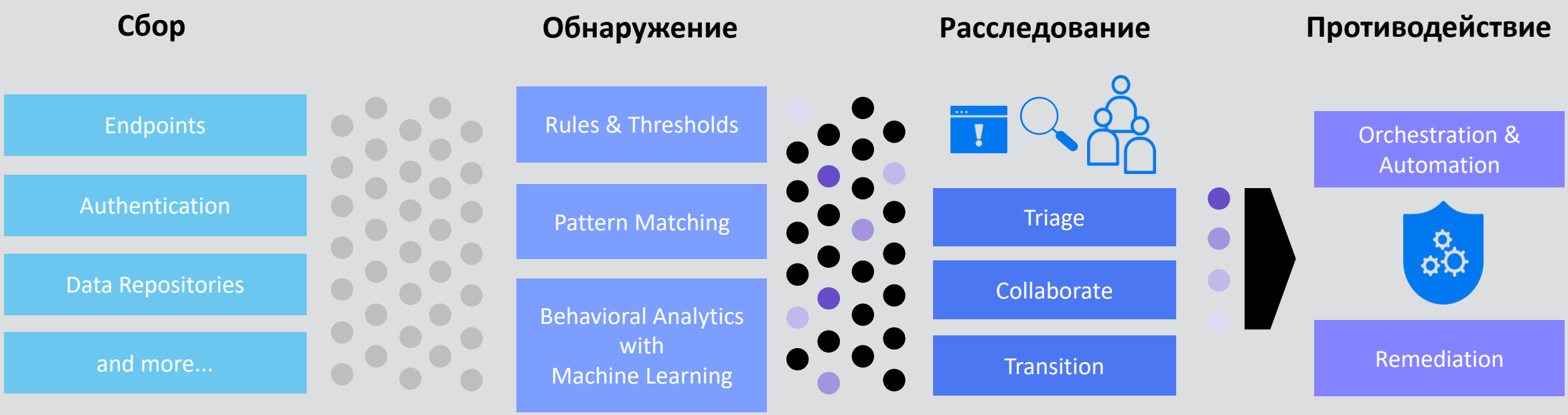
Потребности SecOps сегодня



Потребности SecOps сегодня



Необходимые возможности



ArcSight Platform – коллаборация наших лучших технологий

Стек наших лучших технологий

- Современная архитектура – ITOM CDF (Container Deployment Foundation)

VERTICA

- Единое озеро данных – Vertica

MICRO FOCUS ArcSight

- Лучший корреляционный движок – ArcSight ESM

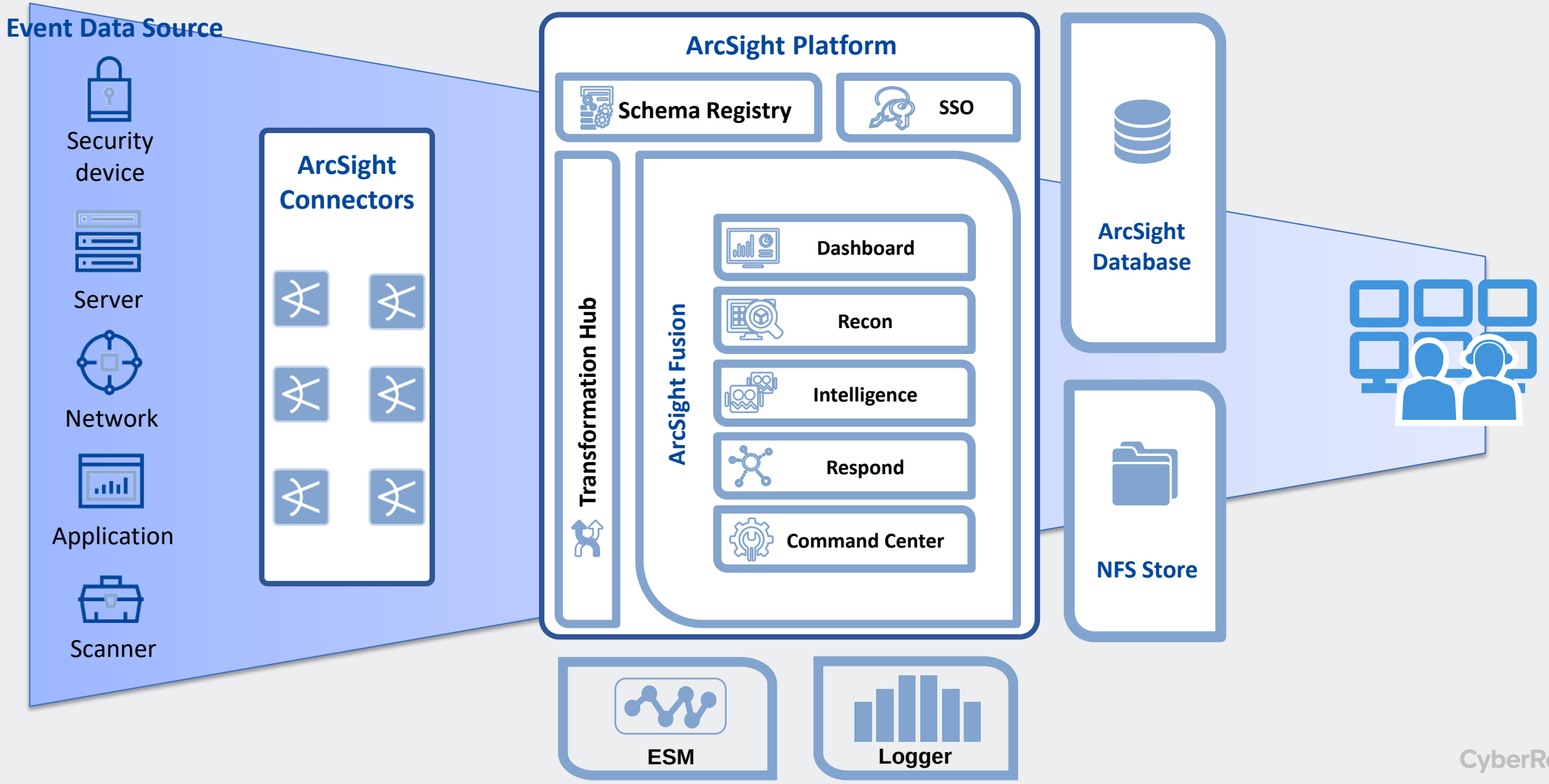
INTERSET

- Аналитические алгоритмы ML – Interset

atarlabs

- Возможности SOAR – Atar Labs

Архитектура платформы

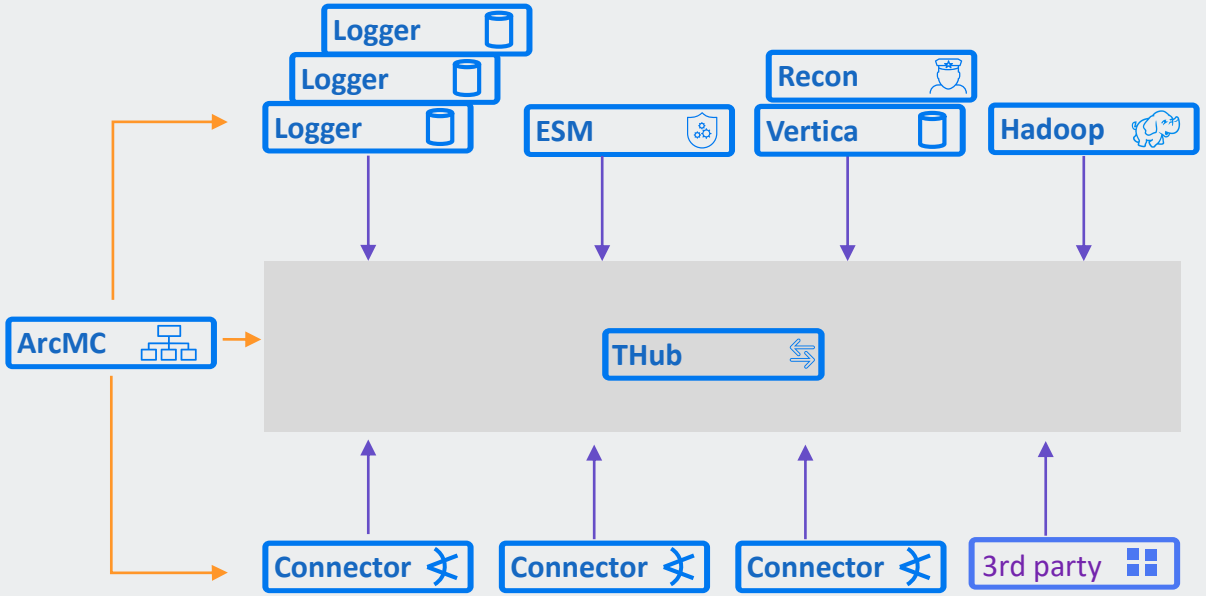


CyberRes

Transformation Hub

Универсальная шина данных для многоуровневой аналитики SecOps

- Основан на Apache Kafka для открытости и производительности
- Масштабируемость и отказоустойчивость за счёт применения контейнеризации
- Нативная интеграция со всеми продуктами семейства ArcSight
- Настраиваемая маршрутизация и фильтрация событий
- Обогащение событий (2021)



Recon

Аналитика базовых событий на технологиях больших данных

Поиск

- Удобный пользовательский web-интерфейс: диаграмма распределения событий по времени, подсказки по поисковому синтаксису, управление глубиной поиска, подсветка синтаксиса
- Просмотр RAW-событий
- Выделенная панель информации по событию
- Единая схема событий и единое хранилище данных

Производительность

- Высокая степень сжатия данных
- Уменьшенные требования к ресурсам для индексирования
- Скорость поиска значительно превосходит Logger

Отчётность

- Полноценный модуль отчётности
- Встроенные отчёты MITRE, OWASP, Cloud и др.

Аналитика

- Data Quality Dashboard для контроля входящего потока событий на предмет ошибок конфигурации даты/времени
- Базовый функционал профилирования (выявления отклонений)

Варианты инсталляции

- All in One – для работы на одном сервере (небольшие инсталляции, пилот)
- Распределённый кластер (на основе Transformation Hub)

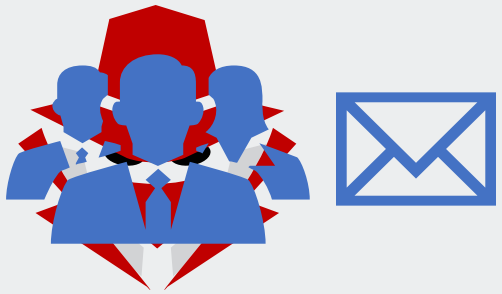
SOAR

Автоматизация расследования и противодействия

- Часть ArcSight Platform
- Полное и полуавтоматическое создание кейсов, приоритизация, расследование, противодействие
- Готовый набор сценариев (playbooks) с возможностью кастомизации
- Средства совместной работы аналитиков
- Настраиваемый кейс-менеджмент с классификацией
- Более 110 интеграций с продуктами крупнейших вендоров
- Делегация задач внутри команды с разграничением уровней доступа
- Детальная история работы по инциденту
- Мониторинг различных метрик эффективности SOC
- Без дополнительной платы для пользователей ESM и Recon!

CyberRes

Технологии в жизни



T1566.001 | Подготовленное письмо

T1204.002 | Запуск вложения

T1547.001 | Закрепиться в системе

T1027.002/T1564.001 | Скрыть присутствие

T1057/T1518 | Анализ окружения

T1071.001 | Отправка данных

T1574.001 | Подмена библиотек

T1219 | Удалённое управление

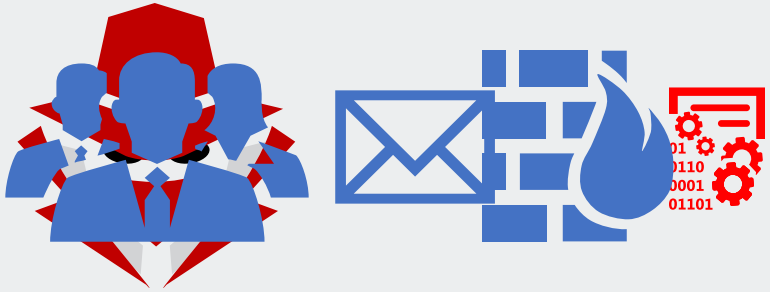
T1003.001 | Дамп учётных данных

T1021.001 | Распространение

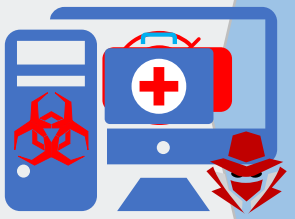
T1020/T1565.001 | Утечка данных

CyberRes

Блокировка компрометированных аккаунтов



Отправка обнаруженных IOC



T1566.001

T1204.002

T1547.001

T1027.002/T1564.001

T1057/T1518

T1071.001

T1574.001

T1219

T1003.001

T1021.001

MICRO FOCUS ArcSight

ArcSight Intelligence

Аномальный отправитель

Аномальный процесс

Модификация реестра

Системные пути

Аномалии процесса

Аномалия трафика

DLL Hijacking

Аномальный инициатор

Mimikatz

Распространение

ArcSight Detect

ArcSight SOAR

Корреляционные события хоста

Аномалии хоста

Репутация и обогащение

Расследование и противодействие

ArcSight Recon

CyberRes

Вопросы?

CyberRes

A Micro Focus line of business