Операционная деятельность по безопасности

с использованием ArcSight 2020

Утечки данных

Между январём и июлем 2020 года стали известны

2,037 утечки данных

27,000,000,000 раскрытых записей

Source: Data Breach QuickView 2020 Mid Year Report, Risk Based Security, August 2020

Статистика рынка

80%

клиентов будут избегать бизнеса, если он допустит утечку их информации

Source: IDC Research (as reported by Varonis)

93%

клиентов будут рассматривать возможность судебных действий против бизнеса, если их персональные данные будут украдены в результате утечки данных

Source: Gemalto Survey (as reported by Tech Wire Asia)

$3.86 млн

Средняя общая стоимость утечки данных

Source: Ponemon Institute, 2020

280 дней

среднее время до обнаружения и закрытия утечки данных

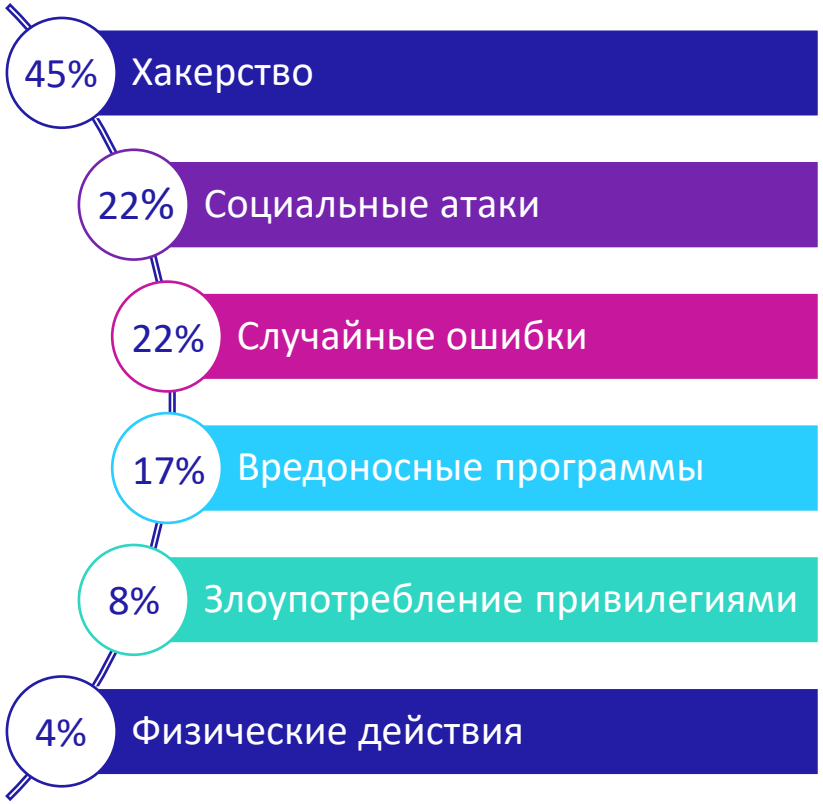
Source: Ponemon Institute, 2020

INTRACOM UKRAINE

MICRO FOCUS

С чем боремся?

Тактики, использованные в 2020



Кибер - криминалитет
Государственные акторы
Зловредные инсайдеры
Небрежные инсайдеры
Партнеры
Контракторы

В РОЗЫСКЕ

Плохие парни извне

Плохие парни изнутри

Глупые парни изнутри

INTRACOM UKRAINE

Source: Verizon Data Breach Investigations Report 2020

MICRO FOCUS

Почему сегодняшний SOC не поспевает?

Почему сегодняшний SOC не поспевает?

70%

Говорят, что их организации сложно справляться с объемом алертов безопасности, генерируемых их инструментами аналитики безопасности.

80%

Говорят, что их аналитики и операторы безопасности до сих пор зависят от многочисленных несвязанных аналитических движков и инструментов выявления.

35 Дней

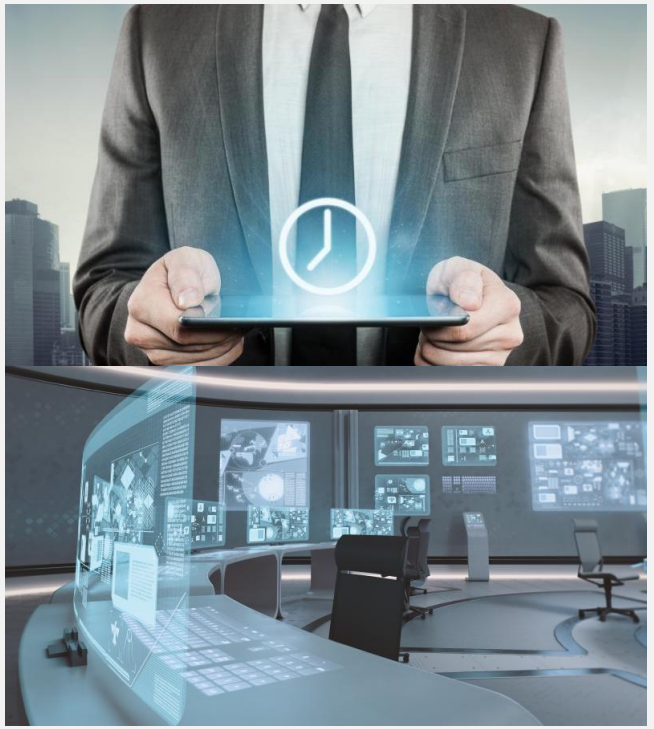
Идентификация и сдерживание зловредных атак занимают на 35 дней больше, чем средний взлом

61%

Оценочный, консолидированный ежегодный рост совокупного всемирного объема данных в период 2019-2025. Ожидается рост от 33 Зеттабайтов до 175 Зеттабайтов.

70%

Говорят, что особо или достаточно сложно найти и нанять персонал SOC.[1]



[1] ESG Research, 2019 [2] Ponemon Institute 2020 [3] IDC Research, 2018

В чём нуждается SOC следующего поколения

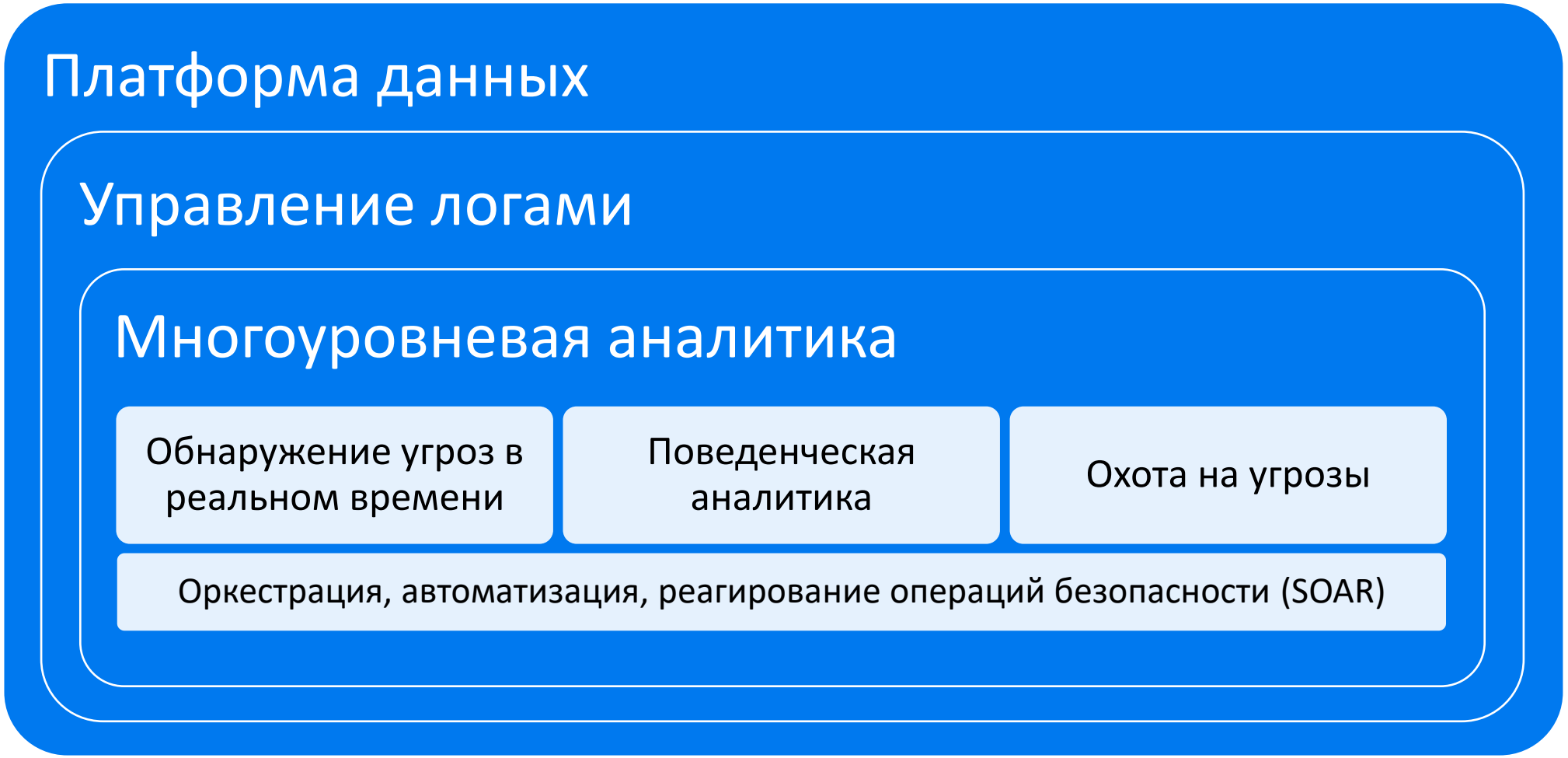
INTRACOM UKRAINE

MICRO FOCUS

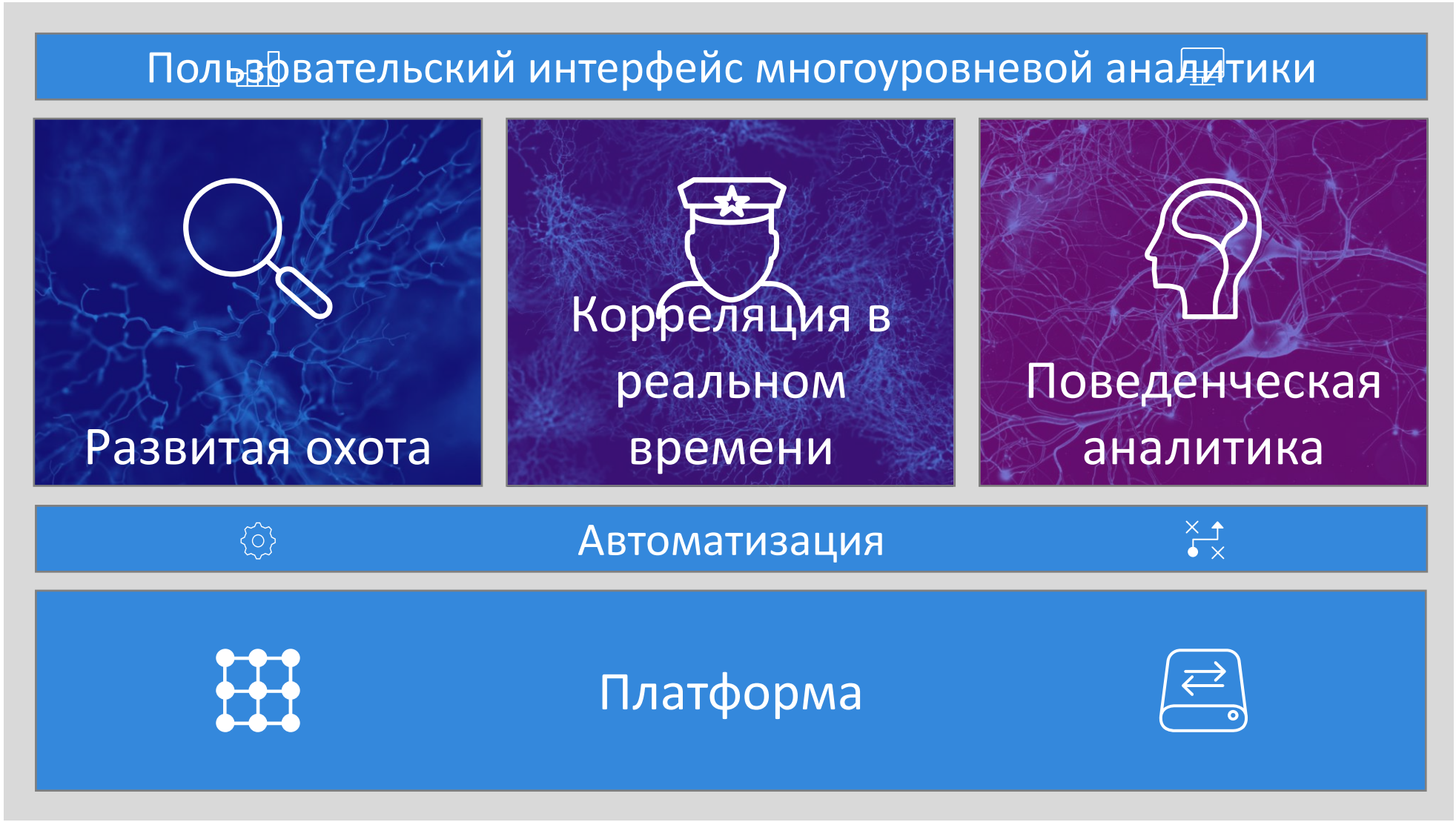
Способности ArcSight 2020

Способность	Что её предоставляет	Бизнес-ценность
Управление информацией и событиями безопасности	Мощная, интеллектуальная СУИБ следующего поколения, основанная на открытой архитектуре и мощной корреляционной машине реального времени	Централизует ваши операции безопасности и определяет «известные» угрозы в реальном времени.
Управление логами и охота на угрозы	Всеобъемлющее управление логами и решение по поиску, которые снижают нагрузки комплаенса и ускоряют расследование инцидентов.	Наполняет централизованное хранилище логов, питающее интеллектуальное расследование и комплаенс.
Платформа данных о безопасности	Собирает, нормализует, обогащает и распределяет данные о событиях из более чем 480 типов источников.	Использует более содержательные и экономически оправданные данные для наработки лучшего видения угроз.
Аналитика поведения пользователей и элементов	Обнаружение аномалий, изучающее нормальное поведение каждого элемента и определяющее наиболее непривычные или подозрительные действия.	Определяет сложные или «неизвестные» угрозы, такие, как угрозы инсайдеров или целевые атаки.
Оркестрация, автоматизация и реагирование операций безопасности	Бесшовная оркестрация технологий и персонала, автоматизация и управление инцидентами.	Повышает эффективность реагирования на кибератаки в операциях безопасности.

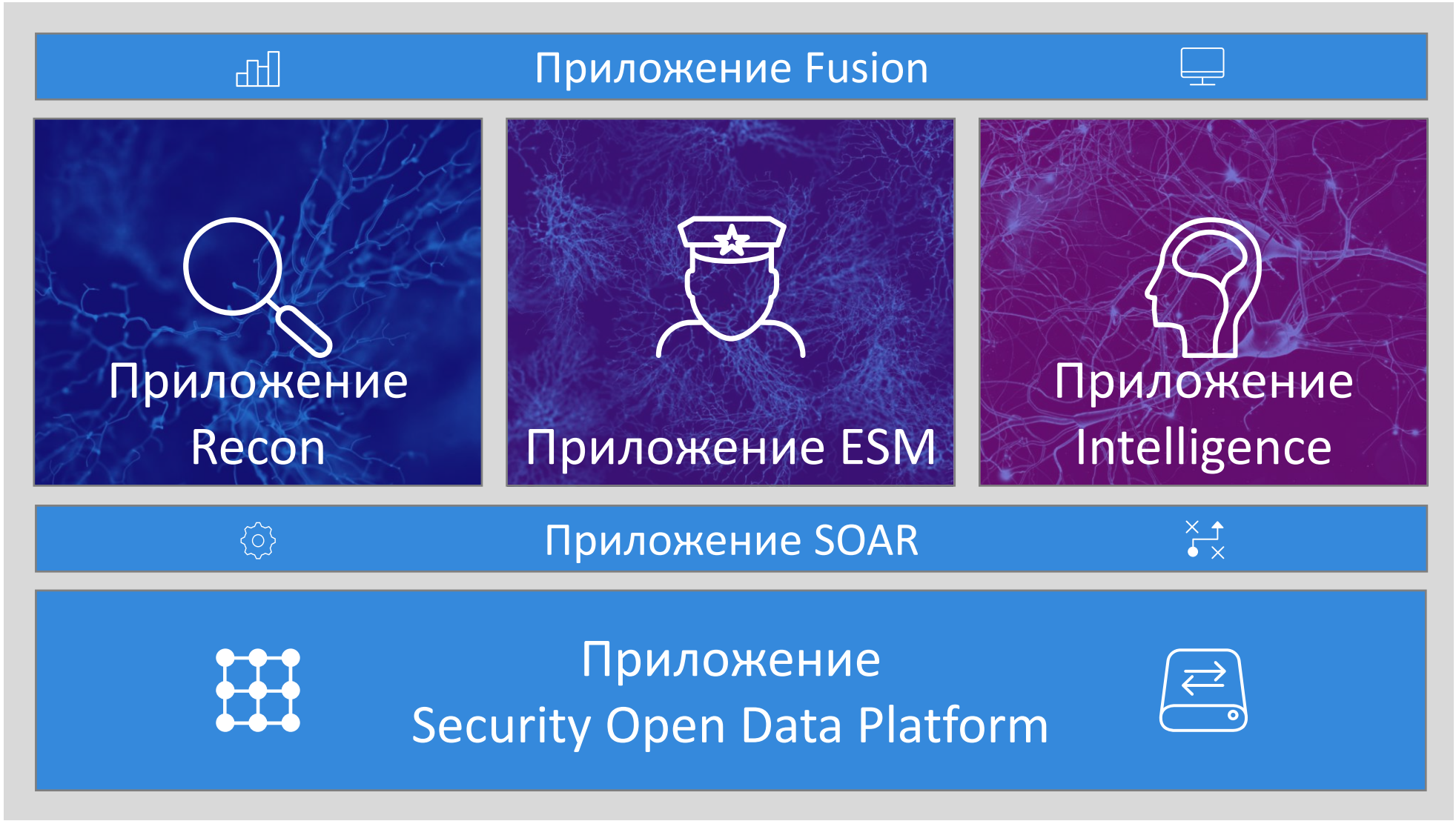
ArcSight упрощенно



Возможности ArcSight 2020



Предложения продуктов ArcSight 2020



INTRACOM UKRAINE

MICRO FOCUS

Что ArcSight 2020 означает для бизнеса

Продвинутые обнаружение угроз и реагирование защищает:

- Ценные IP-адреса
- Критически важные системы
- Клиентские данные, обращение которых регулируется

Обнаружение угроз и реагирование в реальном времени сокращает или ограничивает:

- Прерывание бизнеса
- Судебные тяжбы
- Штрафы регуляторов

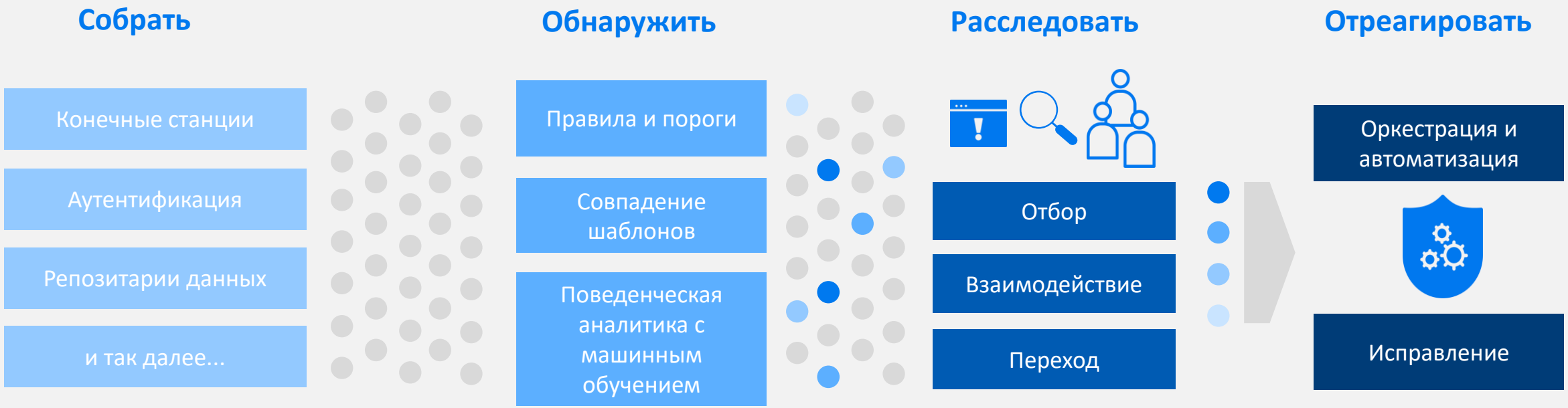
Автоматизация и интуитивное расследование помогают:

- Максимальной производительности SOC
- Сокращению занятости аналитика SOC

Высокая интероперабельность помогает:

- Оптимизировать существующие инвестиции в безопасность
- Избежать подхода «оторви и выброси»

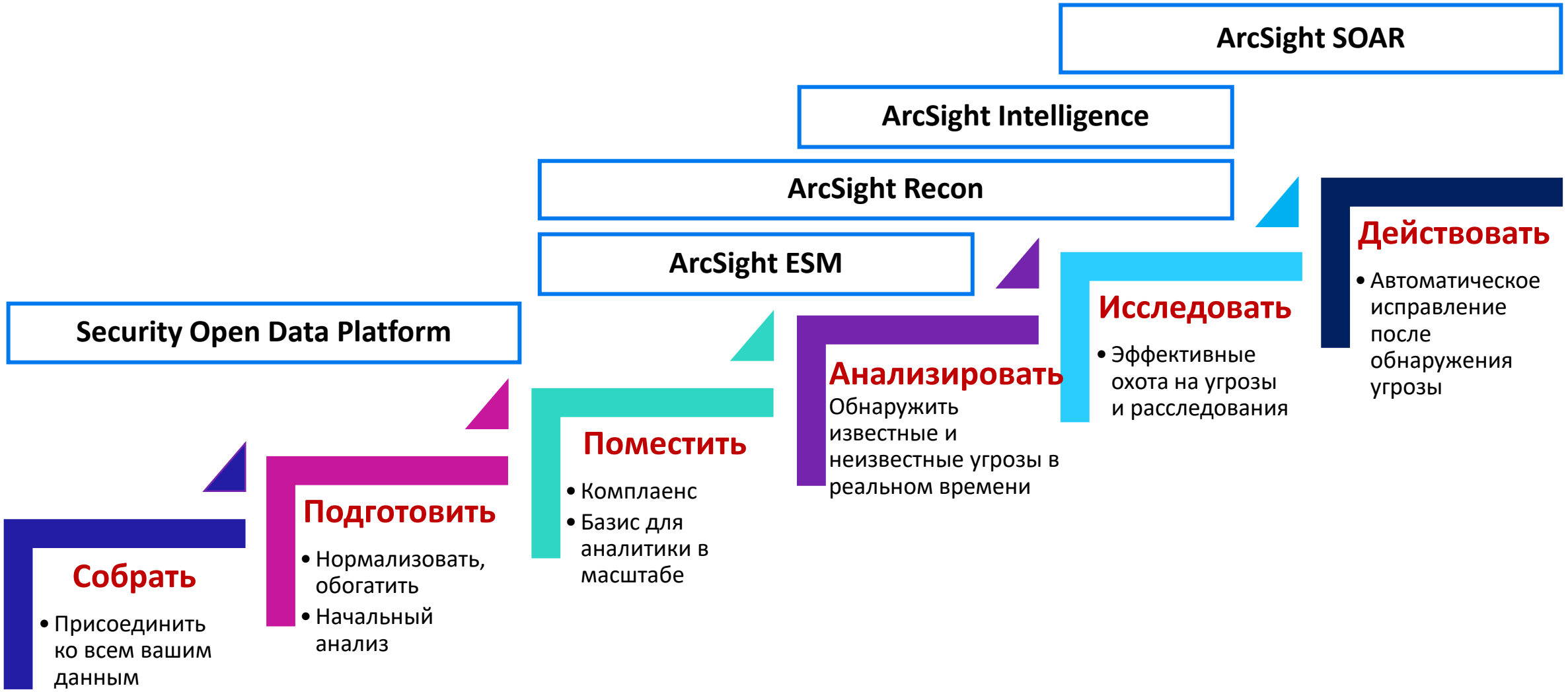
Внутри SOC следующего поколения



INTRACOM UKRAINE

MICRO FOCUS

Micro Focus ArcSight 2020



INTRACOM UKRAINE

MICRO FOCUS

Архитектура ArcSight

КОНСОЛЬ WEB
Управление доступным мониторингом и платформой

СОДЕРЖИМОЕ
MITRE ATT&CK® | Комплаенс | Отчеты и дашборды

ARCSIGHT RECON
Соответствие | Поиск | Удержание | Охота | Расследование

ARCSIGHT ENTERPRISE SECURITY MANAGER (ESM)
Мониторинг | Корреляция в реальном времени

ARCSIGHT INTELLIGENCE
Угрозы инсайдеров| Поведенческая аналитика

ARCSIGHT SOAR
Управление сценариями| Оркестрация |Реагирование

SECURITY OPEN DATA PLATFORM

MANAGEMENT CENTER
Администрирование и управление пакетом

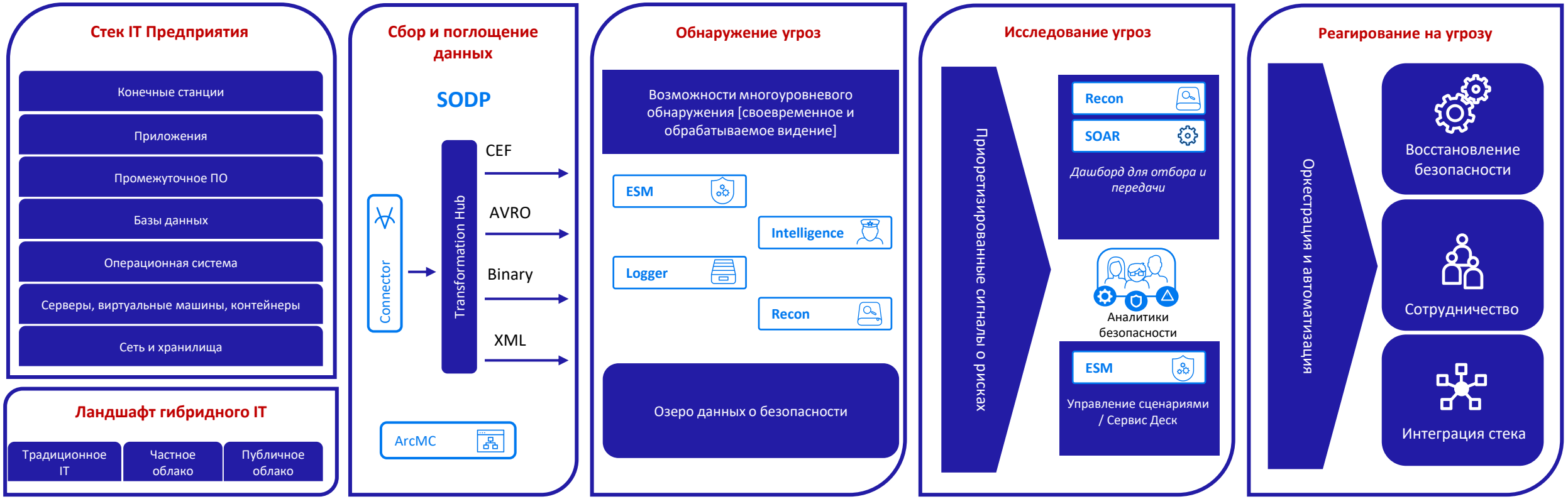
TRANSFORMATION HUB
Доставка информации

SMART/FLEX CONNECTORS
Сбор, обогащение и нормализация данных

INTRACOM UKRAINE

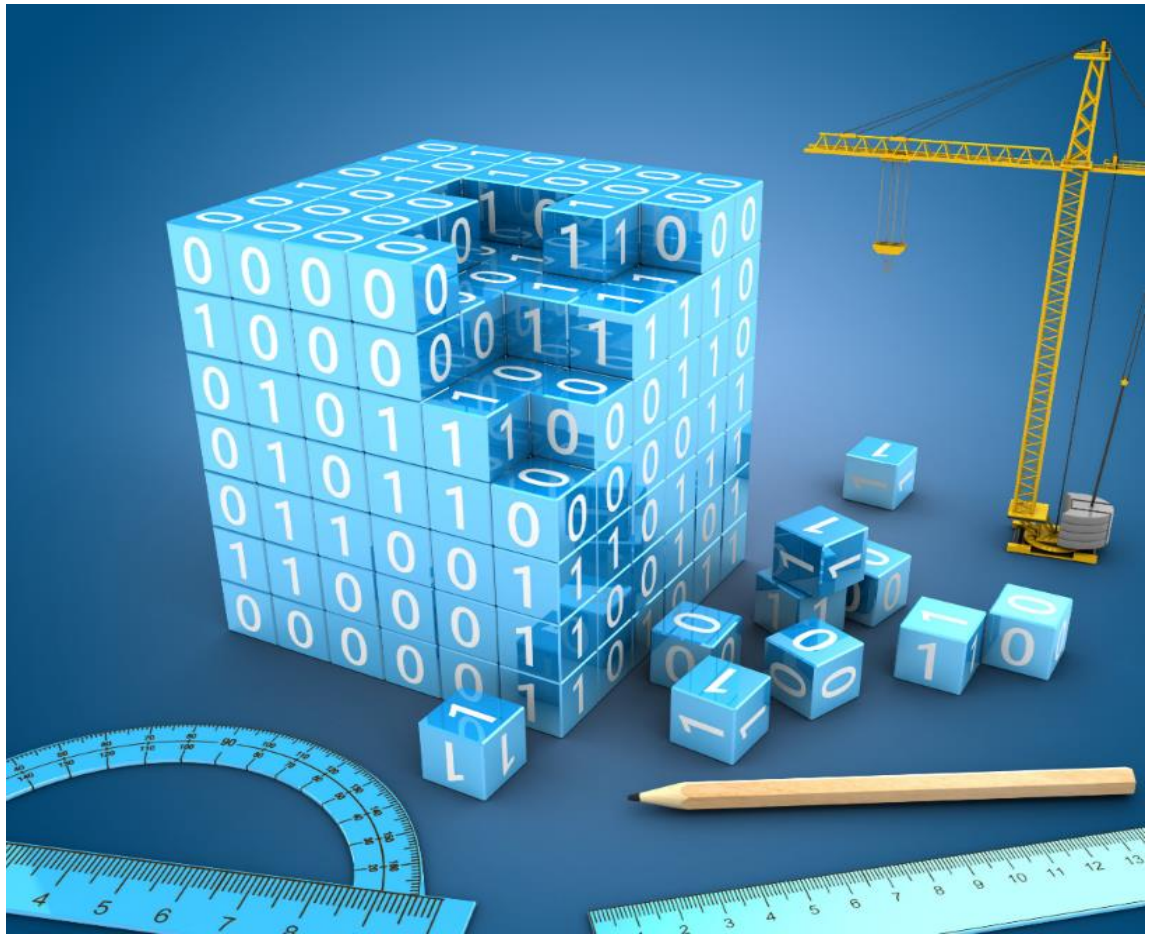
MICRO FOCUS

Архитектура ArcSight 2020



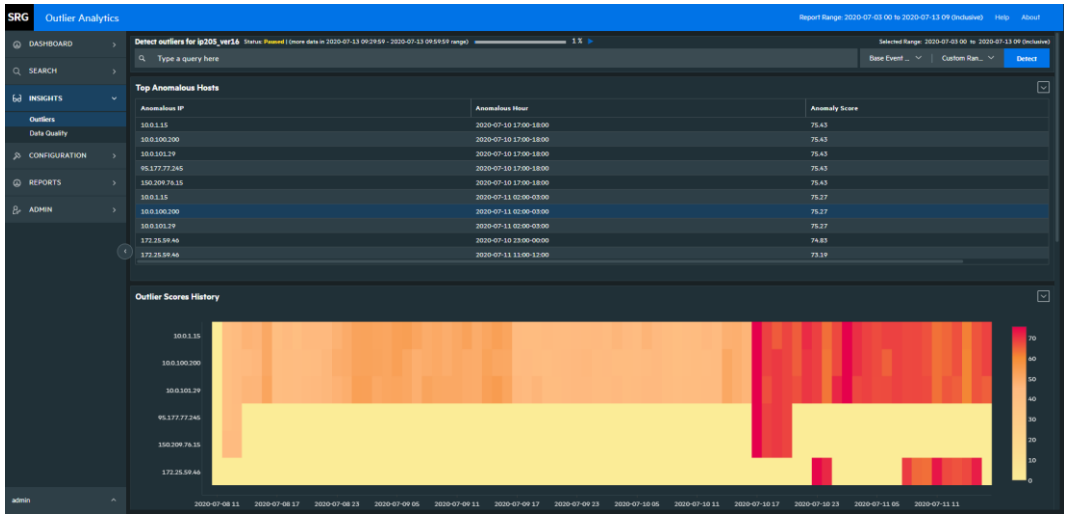
Security Open Data Platform

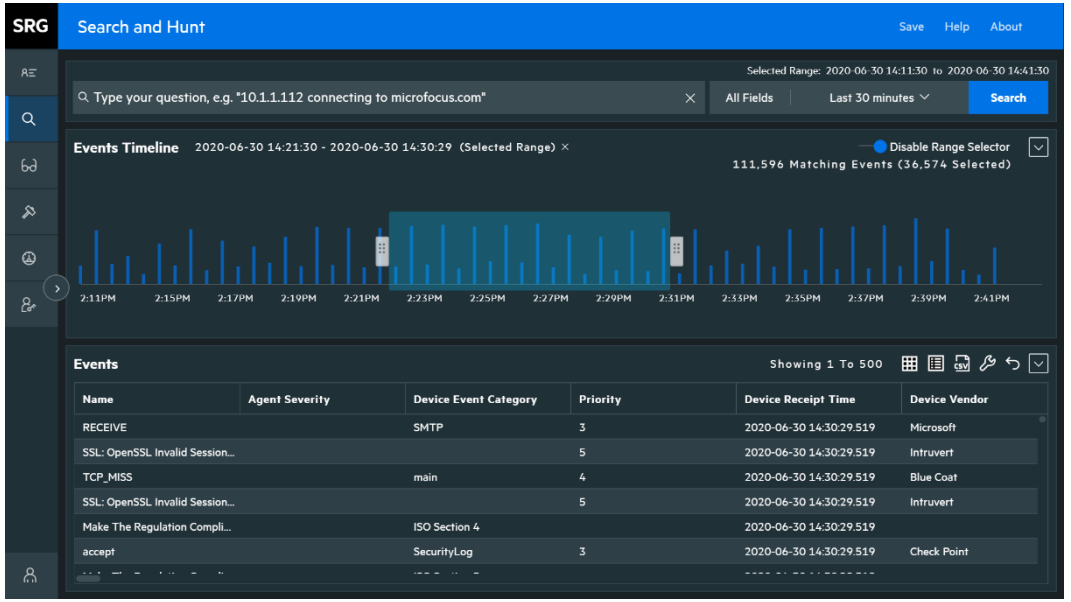
- **Собрать** отовсюду
- **Использовать** везде
- Чистые, обогащенные данные позволяют **лучшее видение**
- Структурированные данные **экономически эффективнее**



ArcSight Recon

- Унифицирует **хранение, отчетность, расследования** и **анализ** трудно обнаруживаемых неизвестных угроз
- **Экономически эффективное** долговременное **хранение** данных
- Непрерывный **комплаенс** безопасности
- Поглощение и поиск среди **миллиардов событий** за секунды
- **Встроенная аналитика** и рекомендации
- Включает **ArcSight SOAR**



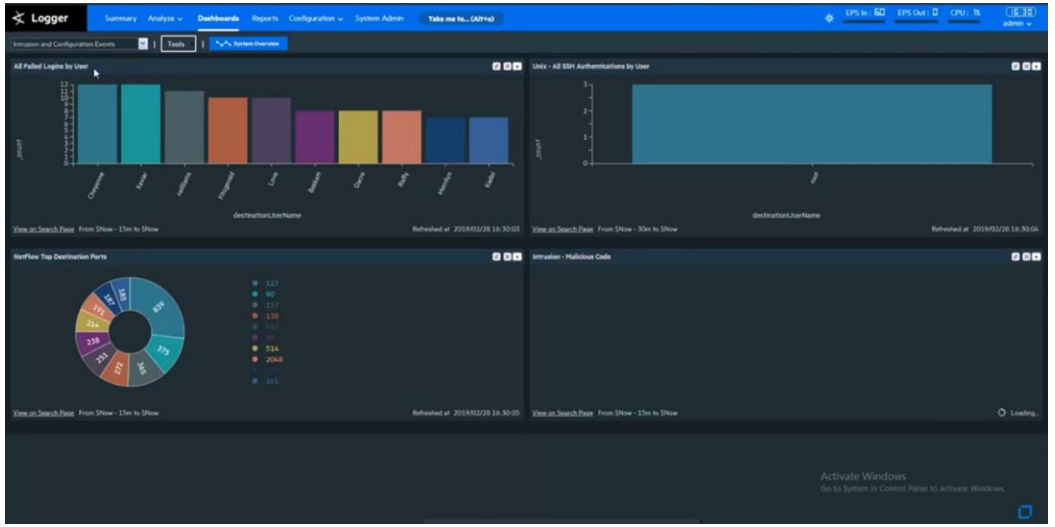


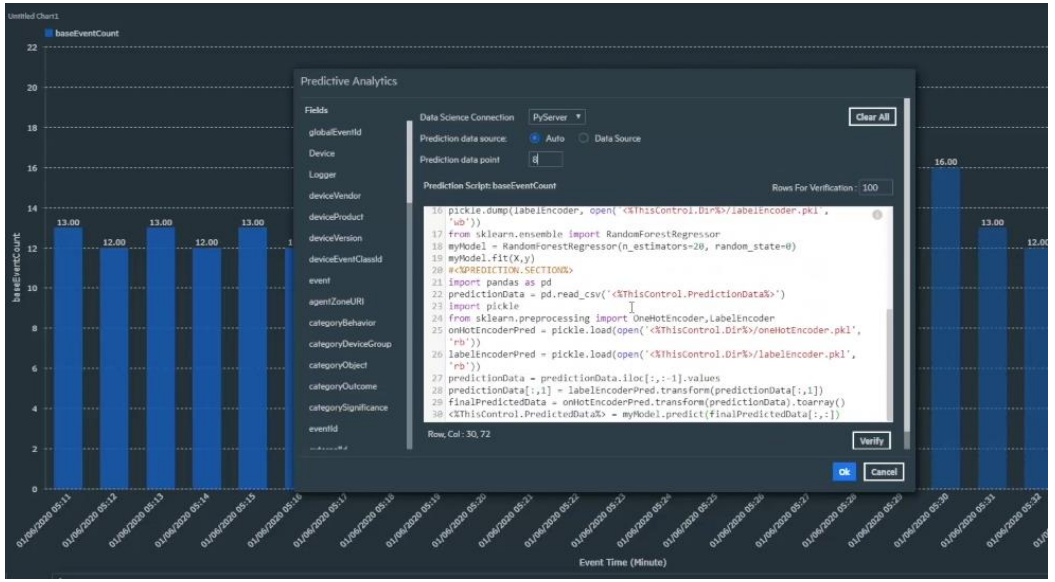
INTRACOM UKRAINE

MICRO FOCUS

ArcSight Logger

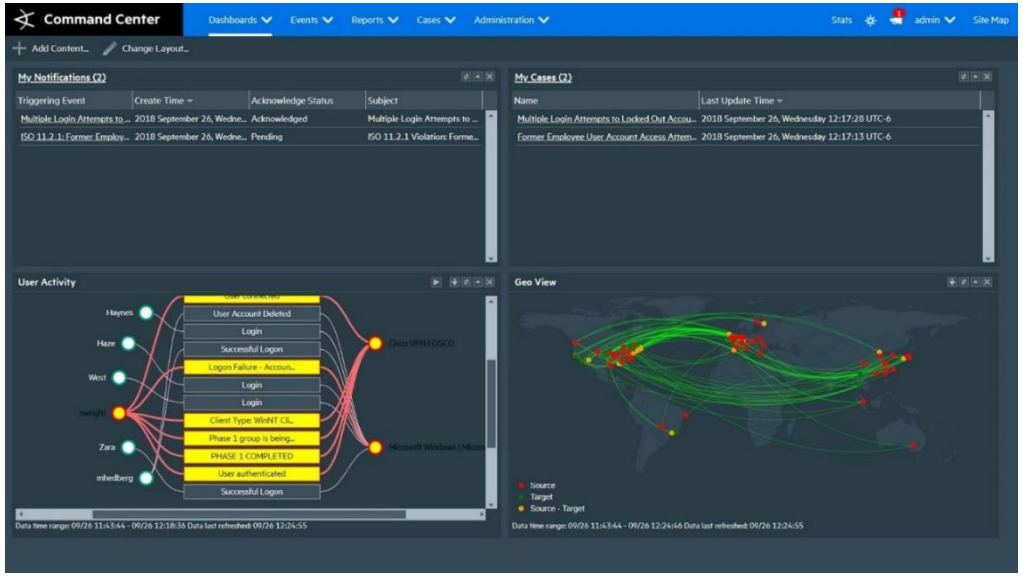
- Централизует **видимость** данных логов
- Унифицирует **поиск, отчетность** и **анализ**
- Непрерывный **комплаенс** безопасности
- **Масштабируемый** (поглощает миллиарды событий в день)
- **Экономически эффективное** долговременное **хранение** данных (в среднем, 10:1 компрессия)

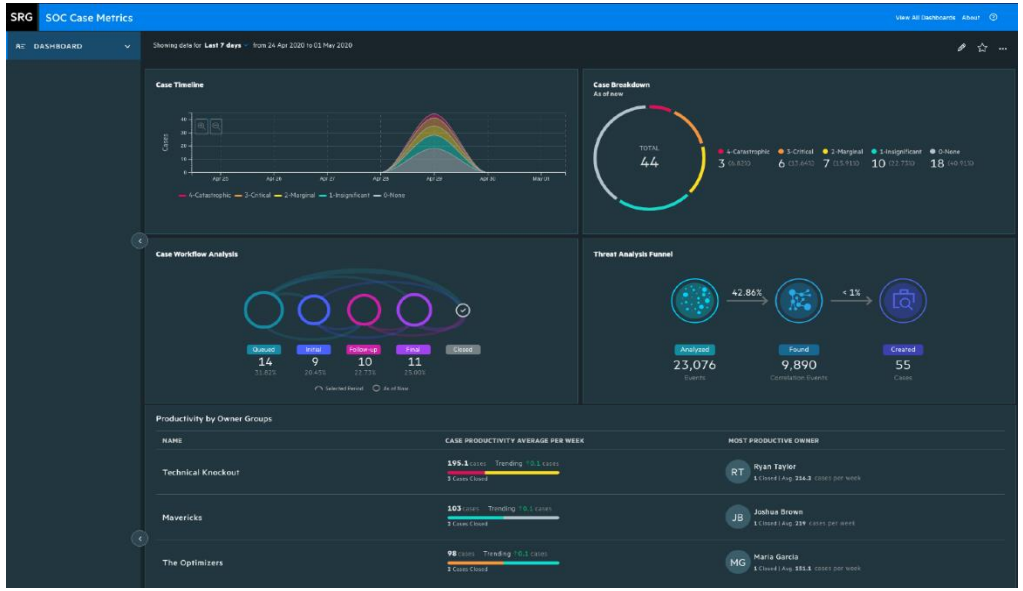




ArcSight ESM

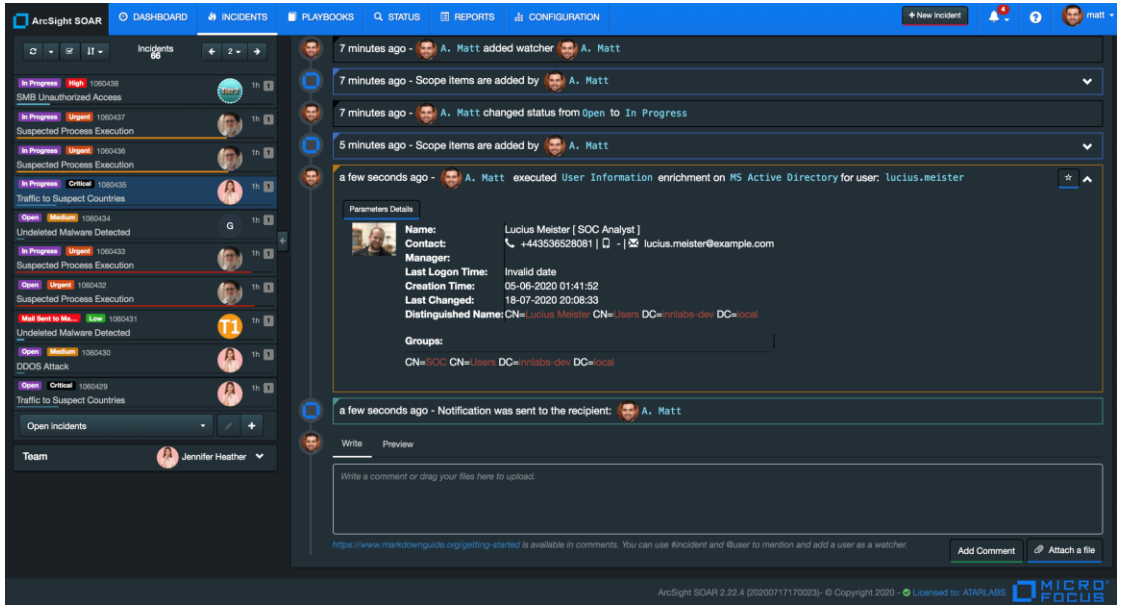
- Ведущая в индустрии **корреляционная машина** с **настраиваемыми** правилами
- **Масштабируемая** (до 100k EPS)
- Отбор, генерация тикетов и **автоматизированное реагирование**
- Много партнеров и **интеграций**
- **Гибкие** архитектура и конфигурирование
- Включает **ArcSight SOAR**

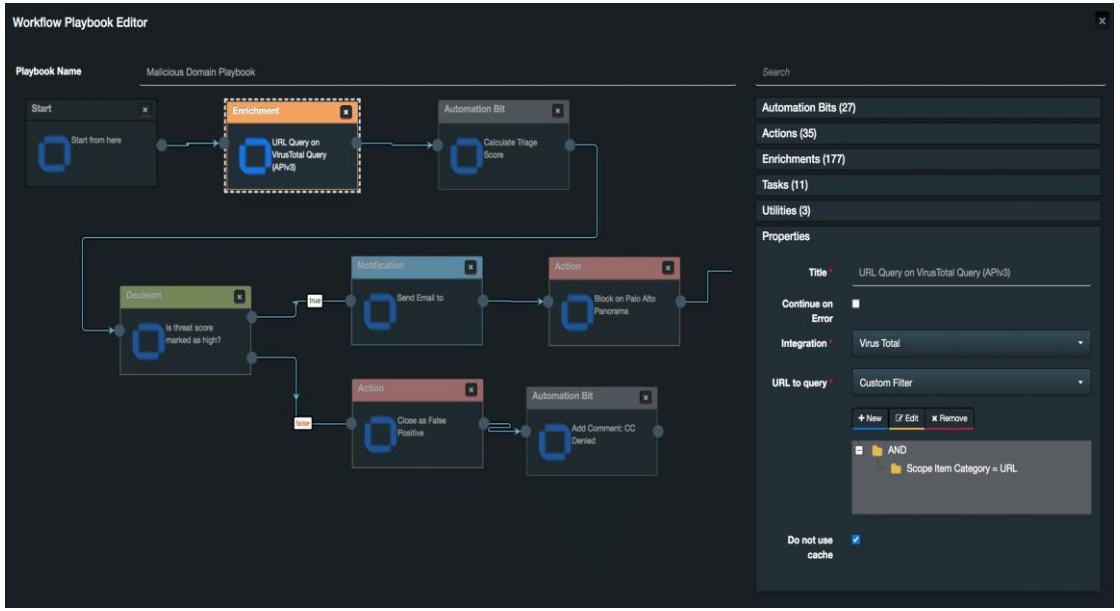




ArcSight SOAR

- **Унифицированные** с ArcSight **вид и восприятие** и единый вход через Fusion
- **Полная или частичная автоматизация** создания инцидента, отбора, расследования, реагирования и т.п.
- **Автоматизация сценариев и рабочих процессов** может быть кастомизирована для эффективного соответствия уникальным потребностям вашего SOC
- **Совместное реагирование на инцидент** для быстрейшей реакции и повышенной эффективности
- **100+ плагинов интеграции** от 70+ вендоров



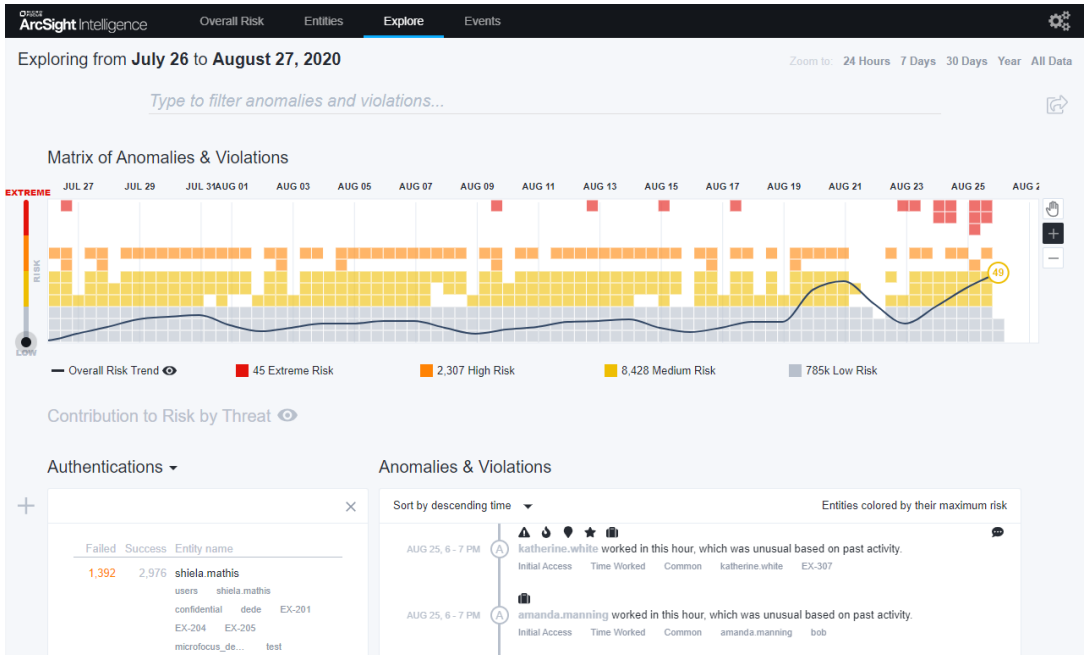


INTRACOM UKRAINE

MICRO FOCUS

ArcSight Intelligence

- Обнаружение аномалий, основанное на поведении, для лучшего обнаружения **инсайдерских угроз**
- Видение потенциальных угроз в **контексте**
- **Отстройка от шума** для расследования приоритетных угроз
- Быстрая **визуализация и реагирование**
- **Масштабирование по мере роста** за счет изначальной архитектуры больших данных ArcSight



INTRACOM UKRAINE

MICRO FOCUS

Security Orchestration, Automation and Response (SOAR)

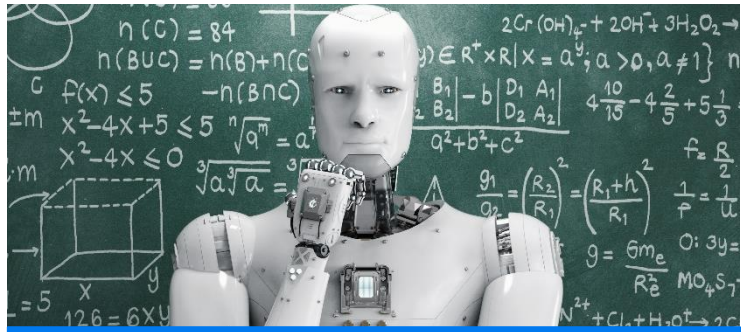
- **Автоматизированное** реагирование
- **Автоматизация на основе сценариев**
- **Улучшенная эффективность**
- **Автоматизированные потоки работ**

Многоуровневое обнаружение угроз

Корреляция в реальном времени

Обнаруживает **известные** угрозы

Сопоставляет *все* данные для поиска угроз



Самостоятельное машинное обучение

Обнаруживает **неизвестные** угрозы

Нет правил или порогов

Продвинутая охота на угрозы

Ищет **трудно обнаруживаемые** угрозы

Судебные расследования

Большинство сценариев угроз в реальном мире требуют смешения всех подходов.

SOC следующего поколения могут обнаруживать:

Помните этих парней….?

В РОЗЫСКЕ

Плохой парень извне

Плохой парень изнутри

Глупый парень изнутри

Инсайдерские угрозы и **Целевые атаки извне** могут проявляться в скрытых поступках и действиях наподобие…

Несанкционированные задания печати

Злоупотребление аккаунтом

Внутренняя разведка

Инфицированный хост

Эксфильтрация данных

Необычные перемещения

Компрометация аккаунта

Бесфайловый вредонос

…и так далее.

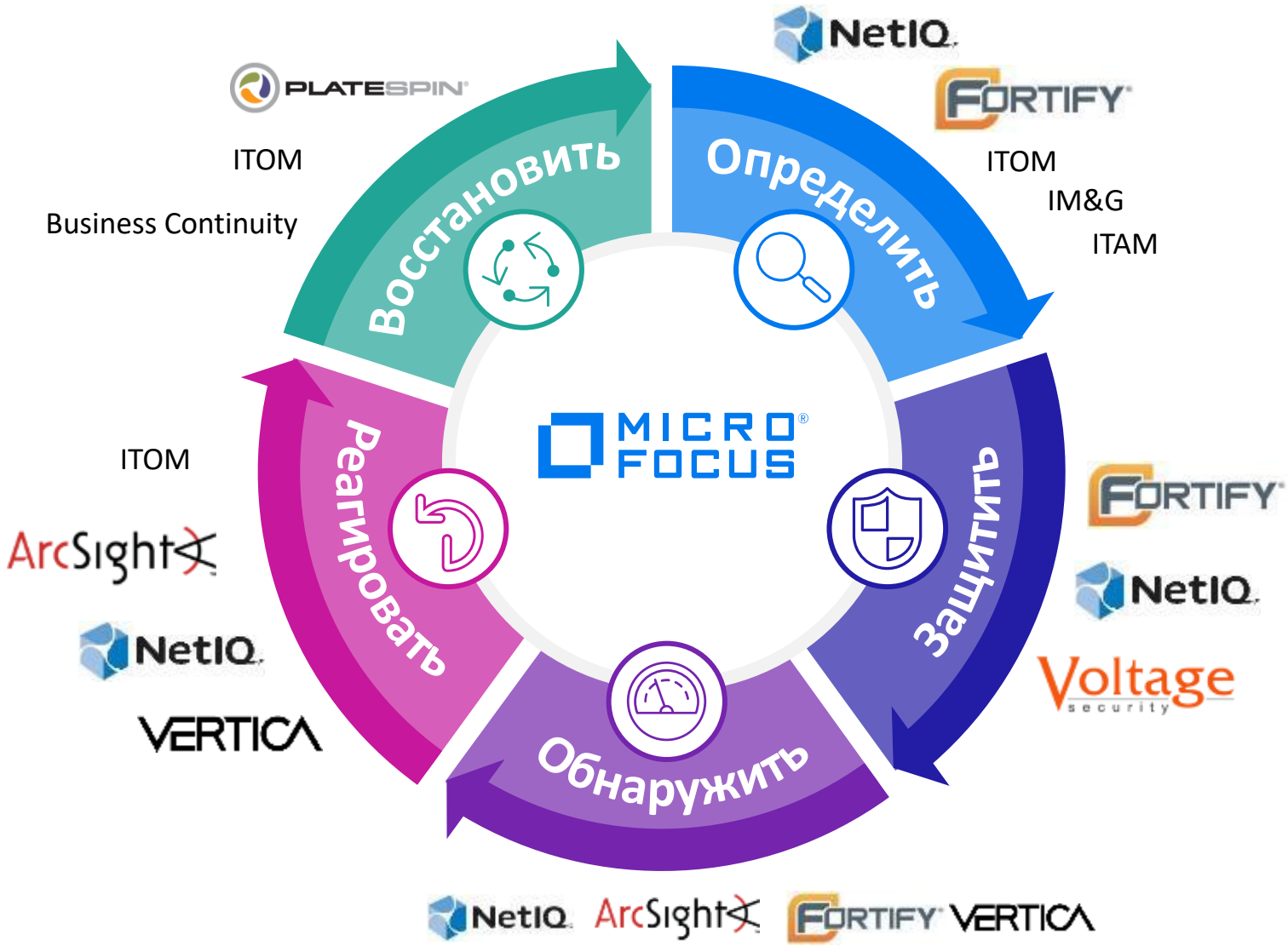
INTRACOM UKRAINE

MICRO FOCUS

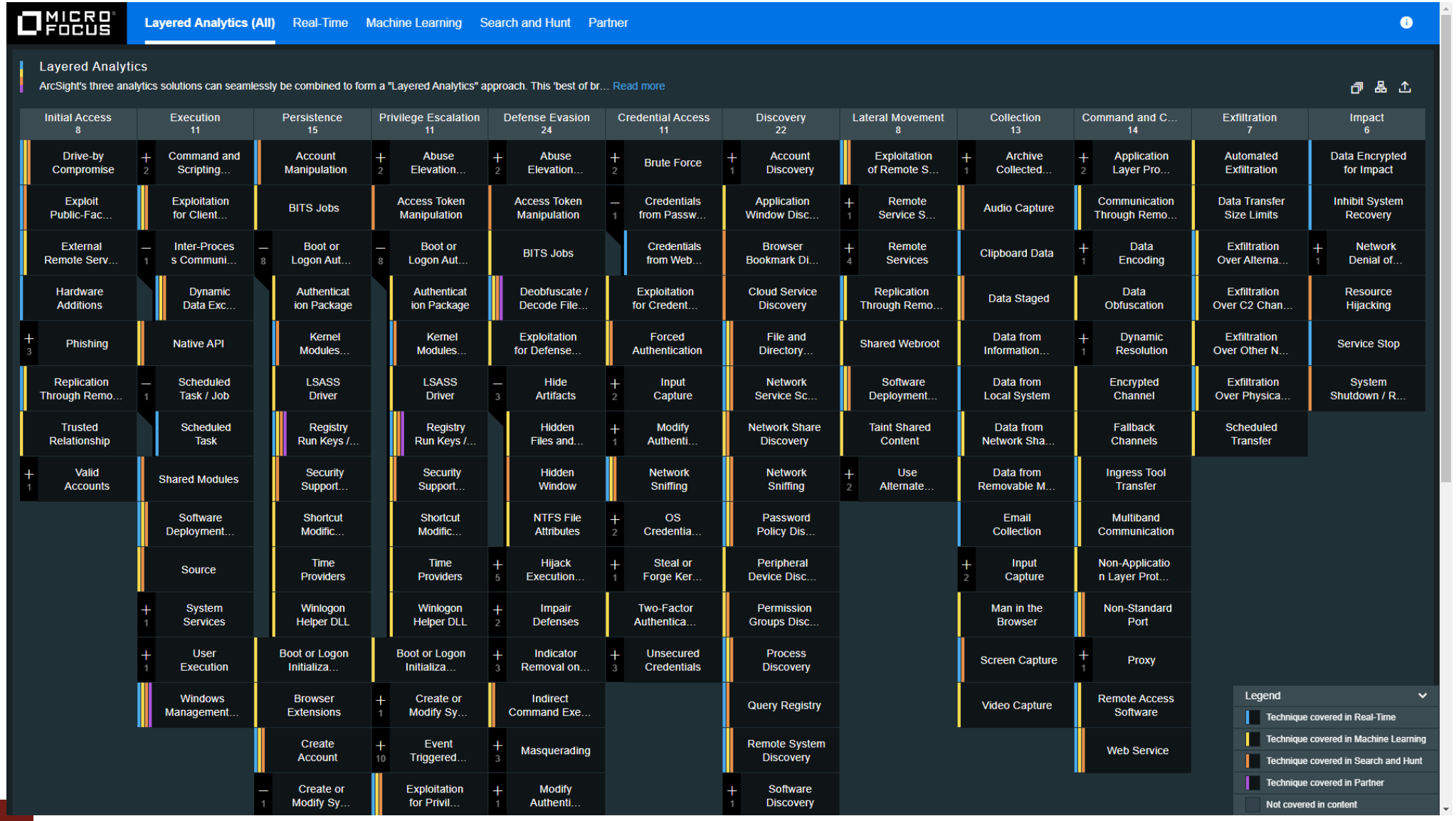
Почему Micro Focus для вашего SOC следующего поколения?

- ✓ **Сквозное** решение для операций безопасности
- ✓ Более быстрое и точное **обнаружение угроз** для как известных, так и неизвестных угроз с **многоуровневой аналитикой** (информация и события безопасности, анализ поведения, охота на угрозы, т.д.)
- ✓ Лучшие в индустрии технологии сбора данных, их нормализации и категоризации для повышения **ценности данных о событии** из 480+ типов источников
- ✓ **Изначальная возможность SOAR в ArcSight** для большей операционной эффективности и быстрейшего реагирования на угрозу
- ✓ **Открытая архитектура** с наибольшей интероперабельностью для повышения отдачи от инвестиций
- ✓ **Более низкая совокупная стоимость владения,** вместе с **гибкостью** масштабирования и расширения покрытия

Портфолио Micro Focus



Расширенный охват MITRE ATT&CK



INTRACOM UKRAINE

MICRO FOCUS

Пример: Использование поведения для определения тактики ATT&CK

Избегание защиты

- Необычные действия с данными или файлами
- Необычные действия процесса
- Необычные связи процесса

Стойкость

- Действия спящего аккаунта
- Необычные действия входа
- Необычная модификация регистра

Исполнение

- Необычные порты или протоколы
- Необычная деятельность процесса
- Необычные сетевые действия

Эскалация прав и доступа к полномочиям

- Необычные аутентификации и доступы
- Доступ к необычным файлам или данным
- Необычные действия PowerShell

Обнаружение и движения в сторону

- Доступ к редким сущностям
- Необычные аутентификации/доступы
- Необычный трафик HTTP

Сбор и эксфильтрация

- Доступ к необычным файлам
- Необычные порты или протоколы
- Бото-подобные действия или работа скриптов

SOC следующего поколения в облаках

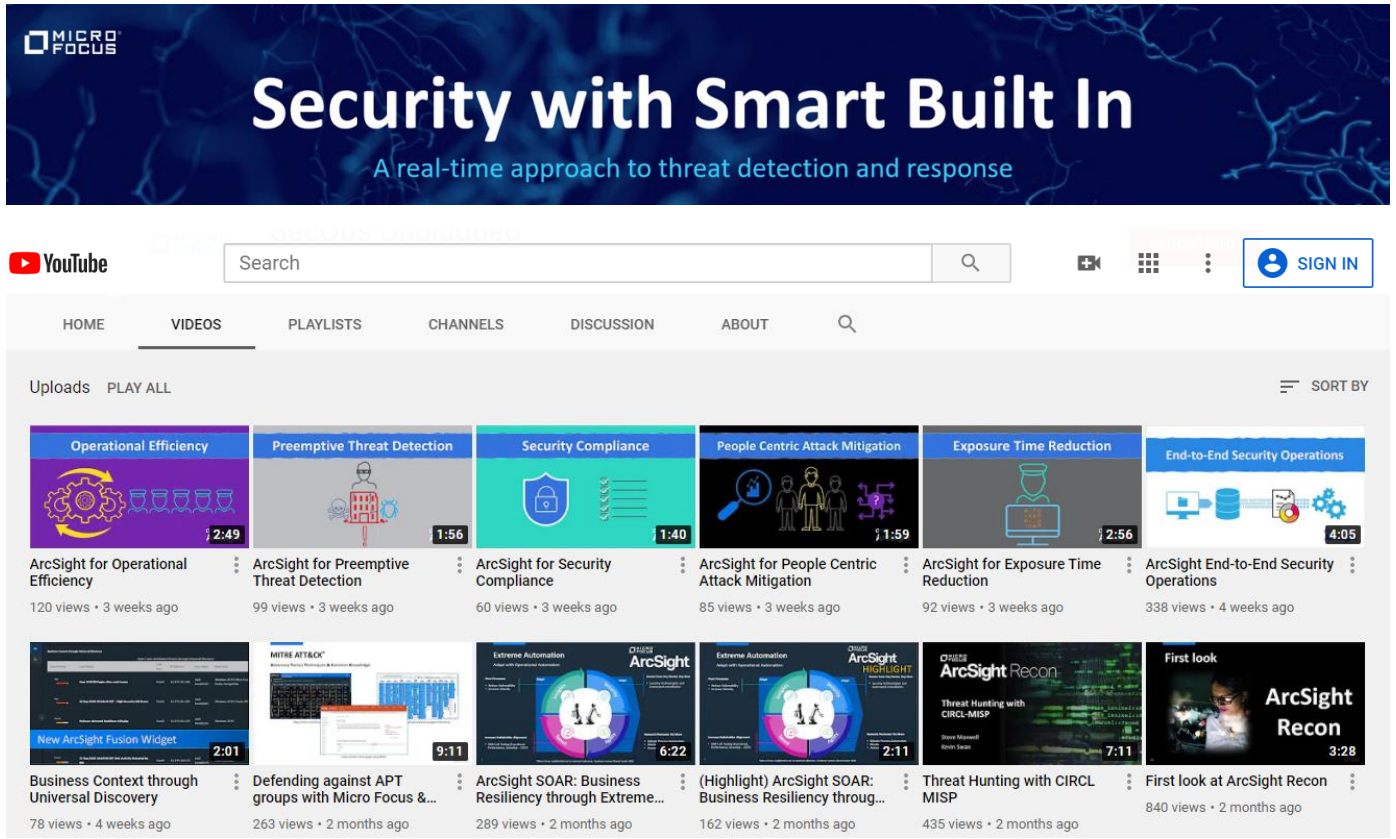
- **Коннекторы** поглощают облачные данные
- **ESM, Logger, T-Hub** и **ArcMC** доступны на **AWS** и **Azure**
- **ArcSight Intelligence:**
  - **Оптимизировано** для **AWS**, при использовании нативных облачных сервисов
  - **Предложения для хостов**
    - ArcSight Intelligence как Сервис **(SaaS)**
    - ArcSight Intelligence для CrowdStrike

SecOps вживую

Официальный канал YouTube для Micro Focus Security Operations и портфолио ArcSight

Включает:

- Истории успеха
- Видео о решении
- Видео инструкции
- Обновления «что нового»
- Видео сценариев использования
- Видео вебинаров/конференций



Подписаться

INTRACOM UKRAINE

MICRO FOCUS

Почему ArcSight? Тому есть 5 причин…

MICRO FOCUS ArcSight

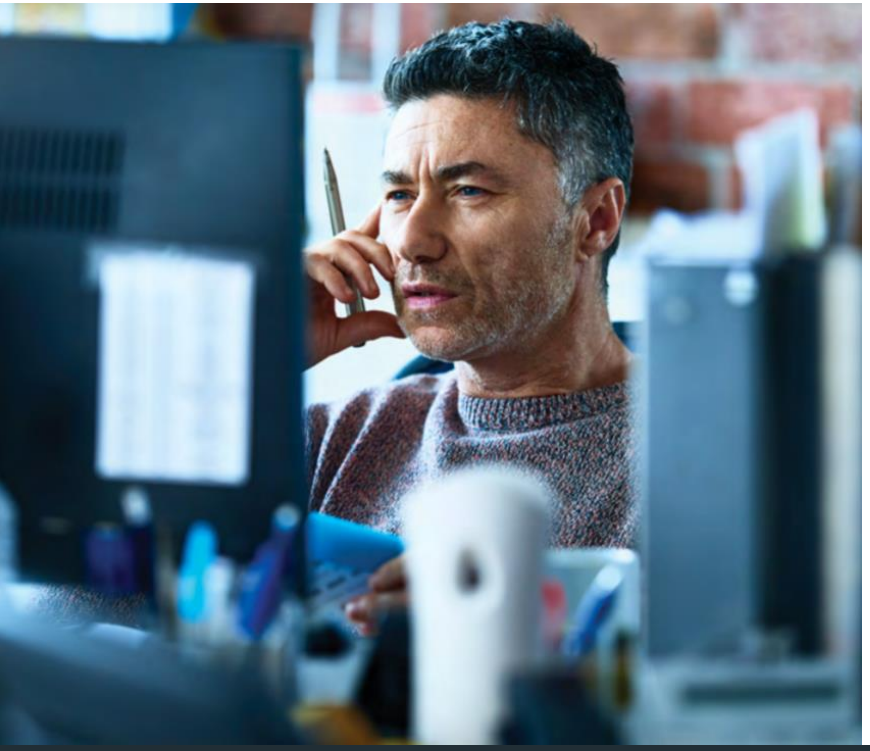
1. **Лучшая корреляционная машина**
   - ArcSight ESM
2. **Расследование угроз**
   - MITRE, MISP, RepSM+
3. **Интеграция UEBA и SOAR**
   - ArcSight Intelligence, ArcSight SOAR
4. **Открытая, эффективная и масштабируемая платформа данных**
   - Security Open Data Platform
5. **Мощная поддержка сообщества**
   - Marketplace, Ideas Exchange

Прочтите флайер

INTRACOM UKRAINE

MICRO FOCUS

Мощная кибер – устойчивость посредством ArcSight



- **Индустрия**

  MSSP / Телекоммуникации

- **Месторасположение**

  Ближний Восток

- **Вызовы**

  Обеспечить наивысший уровень наблюдаемости и расширенной способности к обнаружению угроз для главных телекоммуникационных заказчиков с большой и сложной сетевой средой

- **Решение**

  Развернут ArcSight ESM с подходом «ядерного контента» Obrela, для проактивной идентификации угроз с целью смягчить или минимизировать прерывания бизнеса

OBRELA SECURITY INDUSTRIES

РЕЗУЛЬТАТЫ

10x
Рост в покрытии MSS

10,000+
Наблюдаемых устройств

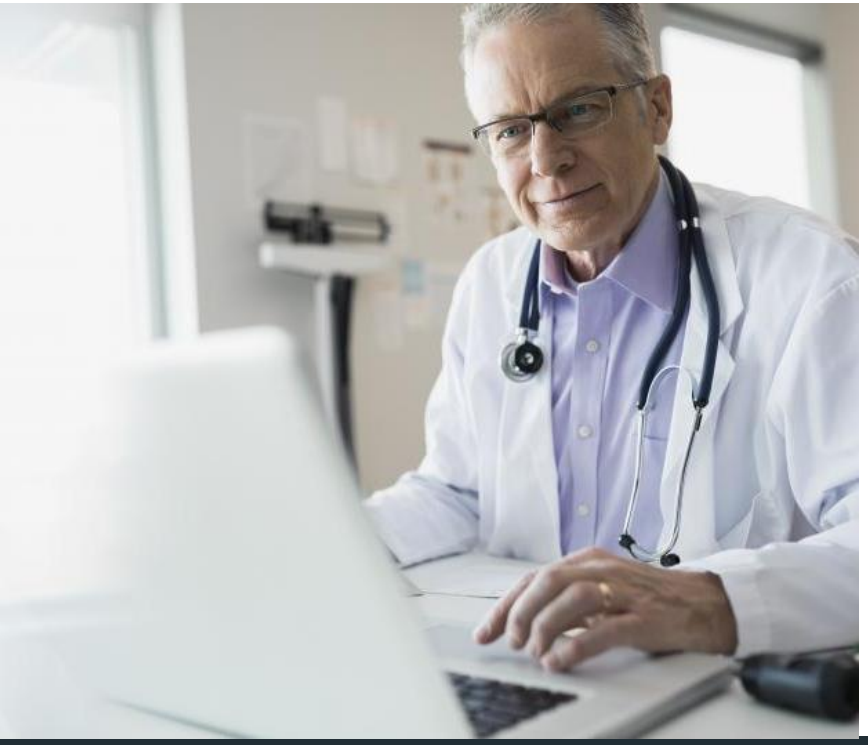
8,000,000
Ежемесячных алертов, обрабатываемых автоматически

250+
Кастомизированных дашбордов

INTRACOM UKRAINE

MICRO FOCUS

ArcSight обеспечивает безопасность в сложной среде здравоохранения



- **Индустрия**

  Здравоохранение

- **Местоположение**

  Новая Англия, США

- **Вызовы**

  Противостоять угрозам кибербезопасности, предоставить всеобъемлющую обратную связь с аудитом, обеспечить работу и безопасность ИТ-структуры для тысяч пользователей в высоко зарегулированной среде здравоохранения.

- **Решение**

  Установить ArcSight ESM и Logger для обнаружения угроз в реальном времени, управления аналитикой, потоками работ и комплаенсом.

РЕЗУЛЬТАТЫ

Отслеживание безопасности среди:

25,000 пользователей

22,000 рабочих станций

Определение и обработка инцидента за **10-15 мин**

+ Ответы аудиту

+ Мониторинг привилегий

+ Управление узлами IoT

INTRACOM UKRAINE

MICRO FOCUS

Большая наблюдаемость и меньше рисков с ArcSight

- **Индустрия**

  Энергетика и коммунальное хозяйство

- **Местоположение**

  Дубай, ОАЭ

- **Вызовы**

  Консолидировать ИТ и Операционные Технологии с тем, чтобы данные были доступны в обоих системах для улучшения расследования угроз и мониторинга устройств

- **Решение**

  Установить ArcSight ESM, SODP и Investigate с тем, чтобы построить совершенную экосистему безопасности, которая способна взаимодействовать с существующими решениями Hadoop, Spark и Elastic

هيئة كهرباء ومياه دبي
Dubai Electricity & Water Authority

РЕЗУЛЬТАТЫ

30% сокращение алармов безопасности

98% уровень смягчения рисков

99% наблюдаемость устройств

\+ сокращение мошенничества с счетчиками

INTRACOM UKRAINE

MICRO FOCUS

Обнаружение высокотехнологичной кражи интеллектуальной собственности при помощи ArcSight Intelligence

- **Индустрия**

  Хай-Тек

- **Местоположение**

  Глобально

- **Вызовы**

  Ущерб от кражи исходного кода в результате инсайдерских угроз, поиск решения, способного обнаружить этот тип сложной угрозы. Потрачено 1 млн USD и год времени на решение, неспособное найти что-либо.

- **Решение**

  Установлен ArcSight Intelligence для обнаружения поведенческих аномалий для нахождения сложных угроз.

РЕЗУЛЬТАТЫ

За

2 недели

ArcSight Intelligence обнаружил:

2

известных инженеров, кравших данные

+3

североамериканских пользователей, кравших данные

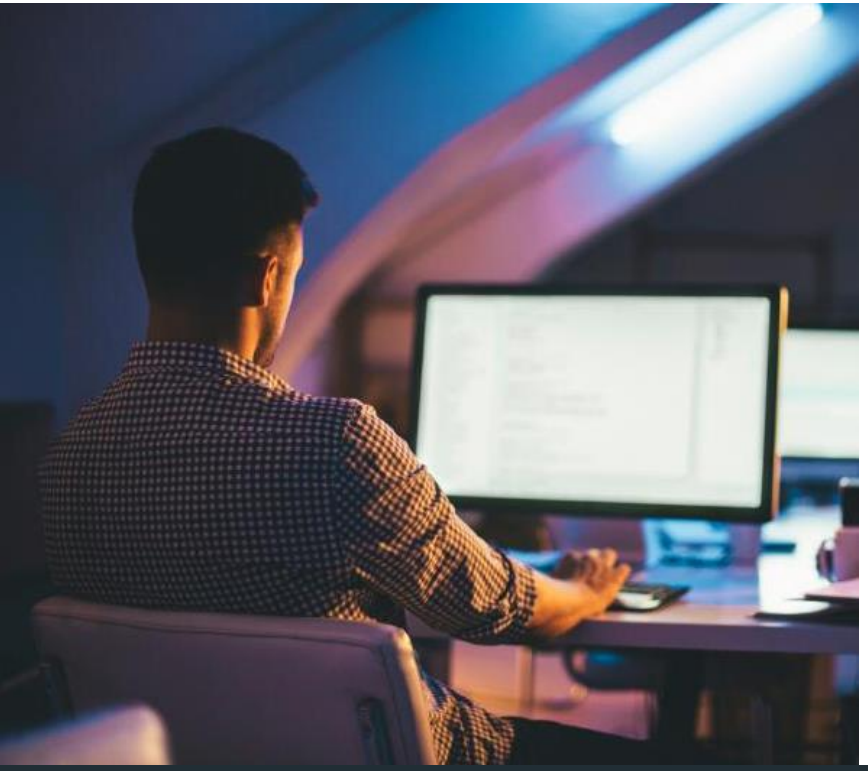
+8

китайских пользователей, кравших данные

INTRACOM UKRAINE

MICRO FOCUS

ArcSight Intelligence поймал кражу печати в неурочное время



- **Индустрия**
  Финансы
- **Местоположение**
  Северная Америка
- **Вызовы**
  Обнаружить и предотвратить ущерб от инсайдерских угроз
- **Решение**
  Установить ArcSight Intelligence для обнаружения поведенческих аномалий для идентификации и смягчения ущерба от злоумышленных или небрежных инсайдеров. ArcSight Intelligence немедленно обнаружил, когда сотрудник начал вести несанкционированную печать, тем самым дав возможность заказчику отреагировать.

РЕЗУЛЬТАТЫ

На протяжении
2 выходных дней
обнаружены необычные действия одного сотрудника:

3:00
действия в офисе

350+
документов напечатано

INTRACOM UKRAINE

Благодарим за внимание!

info@intracom-ukraine.com

www.intracom-ukraine.com

+38 044 277 1622

MICRO FOCUS
Gold Partner
Security