Micro Focus ArcSight – последние изменения в продуктах

Вячеслав Тупиков
Архитектор решений ArcSight
Micro Focus, Россия
Июнь 2020

Содержание

Новое лицензирование продуктов

Архитектура

ESM и Fusion

Logger

Interset

Новое лицензирование продуктов

Новое лицензирование ArcSight, основные тезисы

ArcSight

Standard Edition

- Единая модель лицензирования
- Лицензирование только потока событий
- Единая метрика лицензирования
- Фокус на основные продукты
- Разделение ПО и «Железа»
- Отсутствие искусственных ограничений
- HA и NonProd лицензии включены
- Бесплатная миграция

Лицензирование ArcSight

4 ключевых продукта – единая метрика

ArcSight Marketplace
Бесплатный и коммерческий контент | Compliance-паки

ArcSight Logger	ArcSight ESM	ArcSight Investigate	Interset UEBA
основано на потоке событий (EPS)	**основано на потоке событий (EPS)**	**основано на потоке событий (EPS)**	**основано на активах (пользователи и системы)**

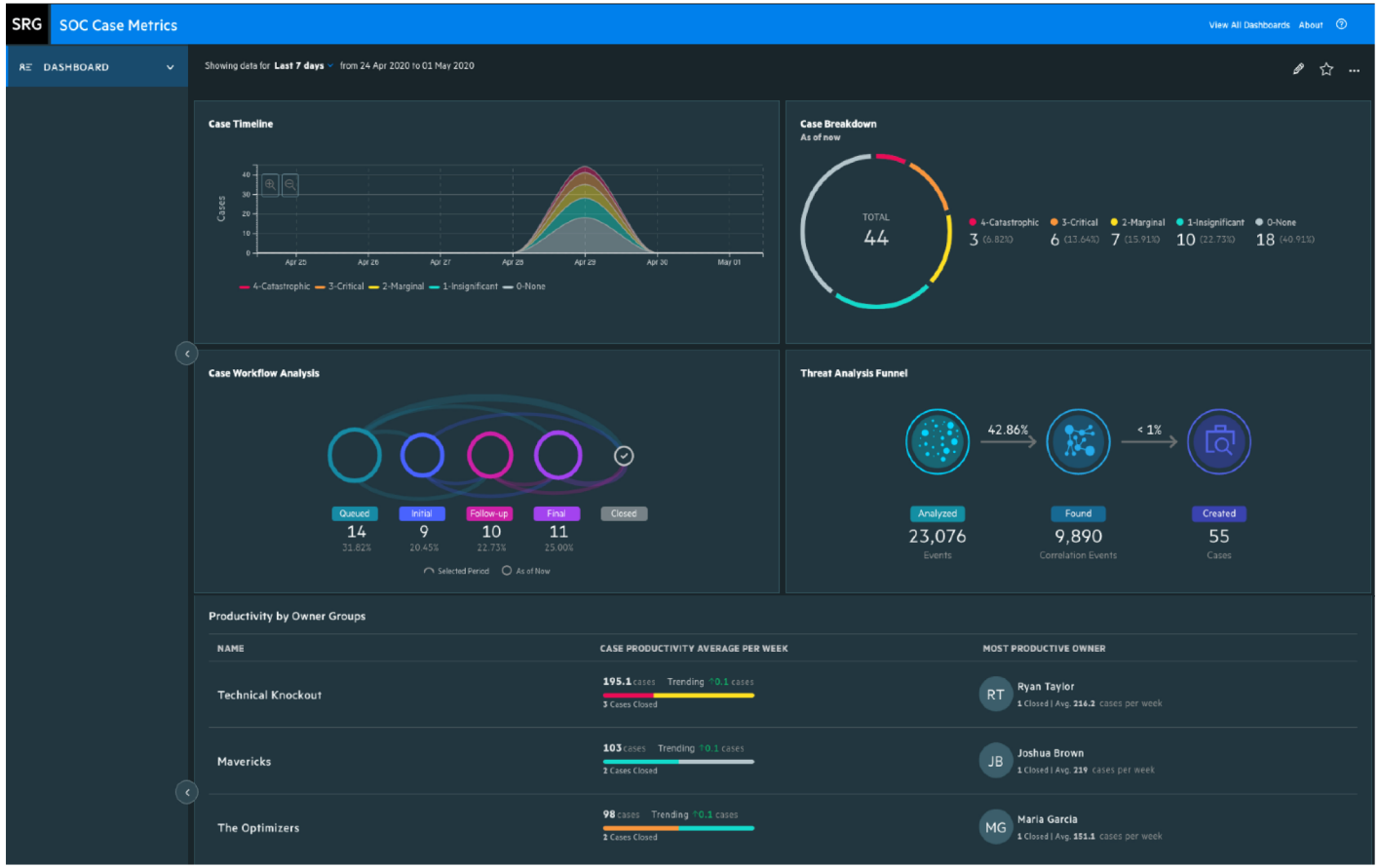
ArcSight Secure Open Data Platform
основано на потоке событий (EPS)
включено в каждый ключевой продукт и доступно отдельно

Архитектура

Новая архитектура ArcSight

ESM и Fusion

ArcSight Fusion



Наш новый единый UI

- Объединяет ArcSight ESM и Interset
- Использует новые функции API
- Является CDF-контейнером

Включает 2 Dashboards

- How is My SOC Running?
  - Case Breakdown
  - Case Load
  - Case Timeline
  - Case Workflow Analysis
  - Productivity
  - Threat Analysis Funnel
- Entity Priority
  - Active Lists
  - Entity Count Overview

Enterprise Security Manager

- Поддержка Global Event ID
- Использование OpenJDK (Azul Zulu)
- Производительность коррелляторов/агрегаторов (1:1)
- Оптимизация скорости загрузки листов
- Развитие Action в правилах
  - Последовательность действий
  - Возвращение результата внешнего скрипта в логику правила
  - Настраиваемый таймаут выполнения внешнего скрипта
- Настраиваемый таймаут для scheduled rules

Возрождение стандартного контента

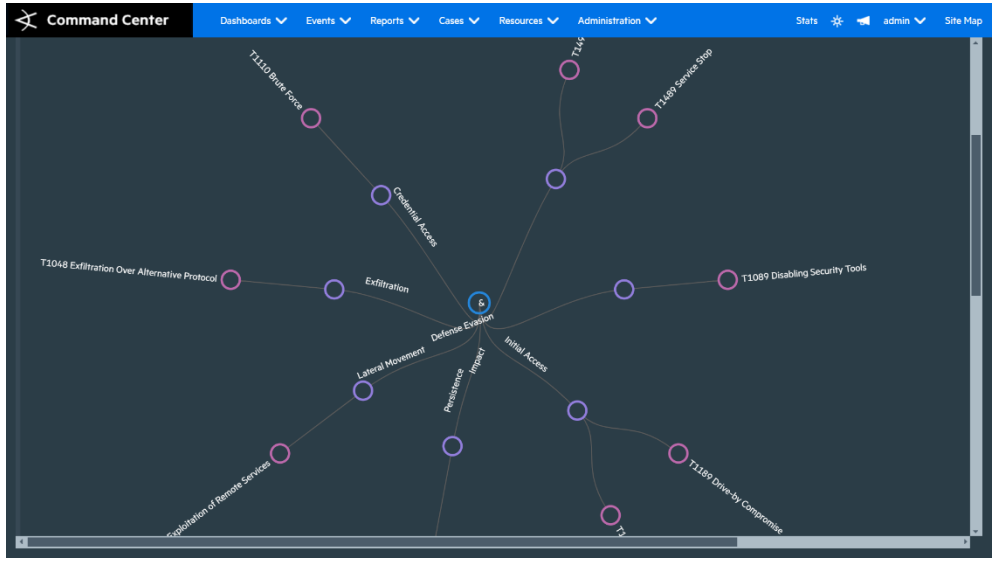
- Выделенное направление по созданию контента
- Стандартный контент по выявлению угроз
- Интеграция контента с MITRE ATT&CK
- Поддержка MISP CIRCL TI (коннектор и контент)
- Обновление Marketplace

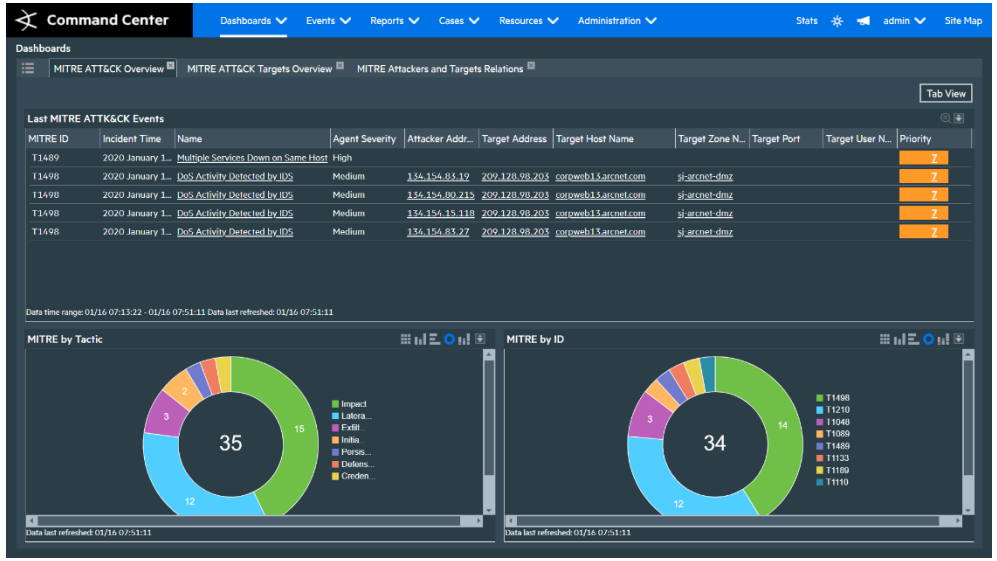
MITRE ATT&CK Dashboards

Предоставляет визуализацию по тактикам матрицы MITRE ATT&CK обнаруженным в инфраструктуре

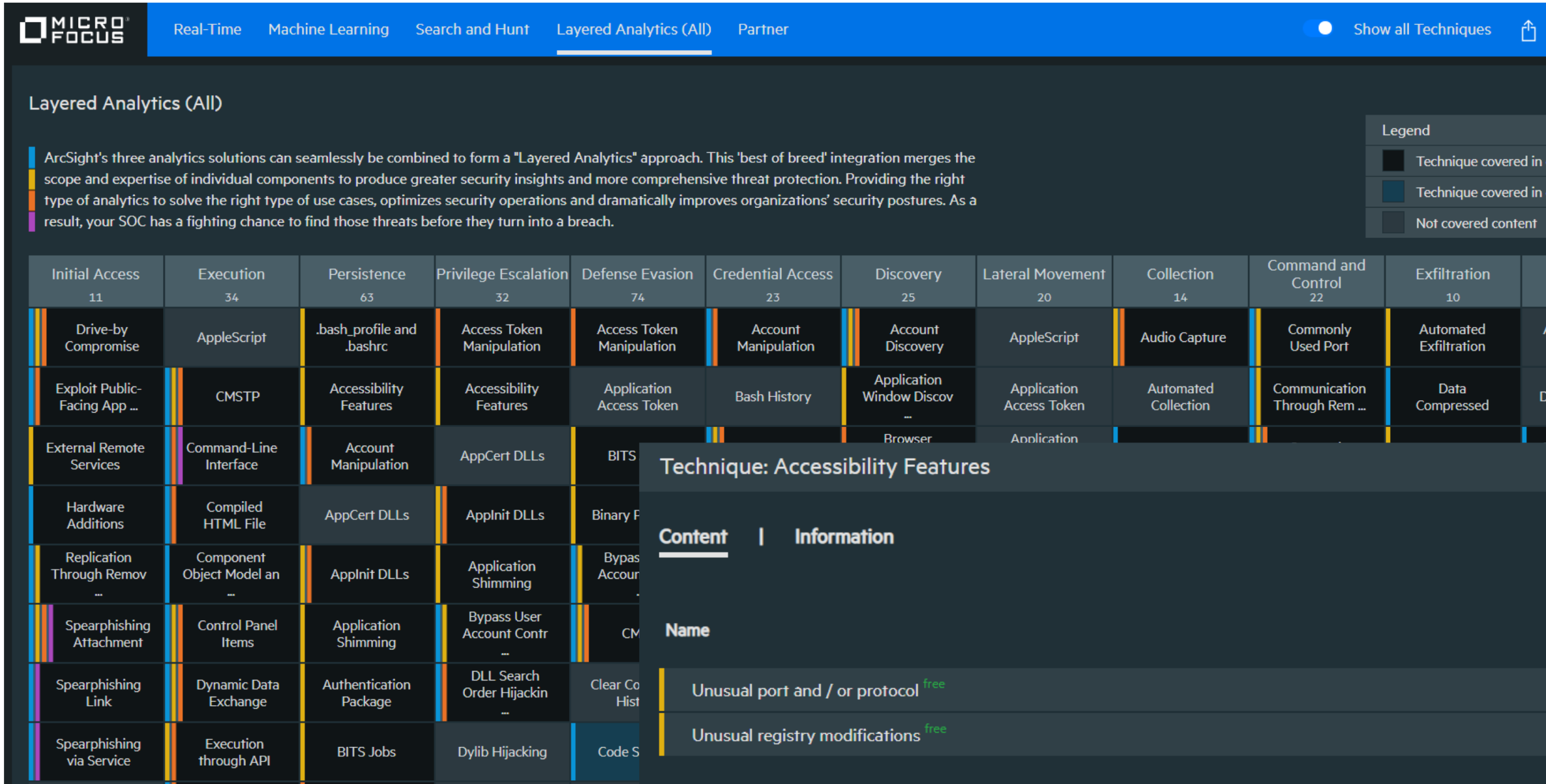
Dashboard включает:

- Top reported MITRE ATT&CK IDs and Tactics
- MITRE ATT&CK IP# relationships
- Latest MITRE ATT&CK events





mitre.microfocus.com

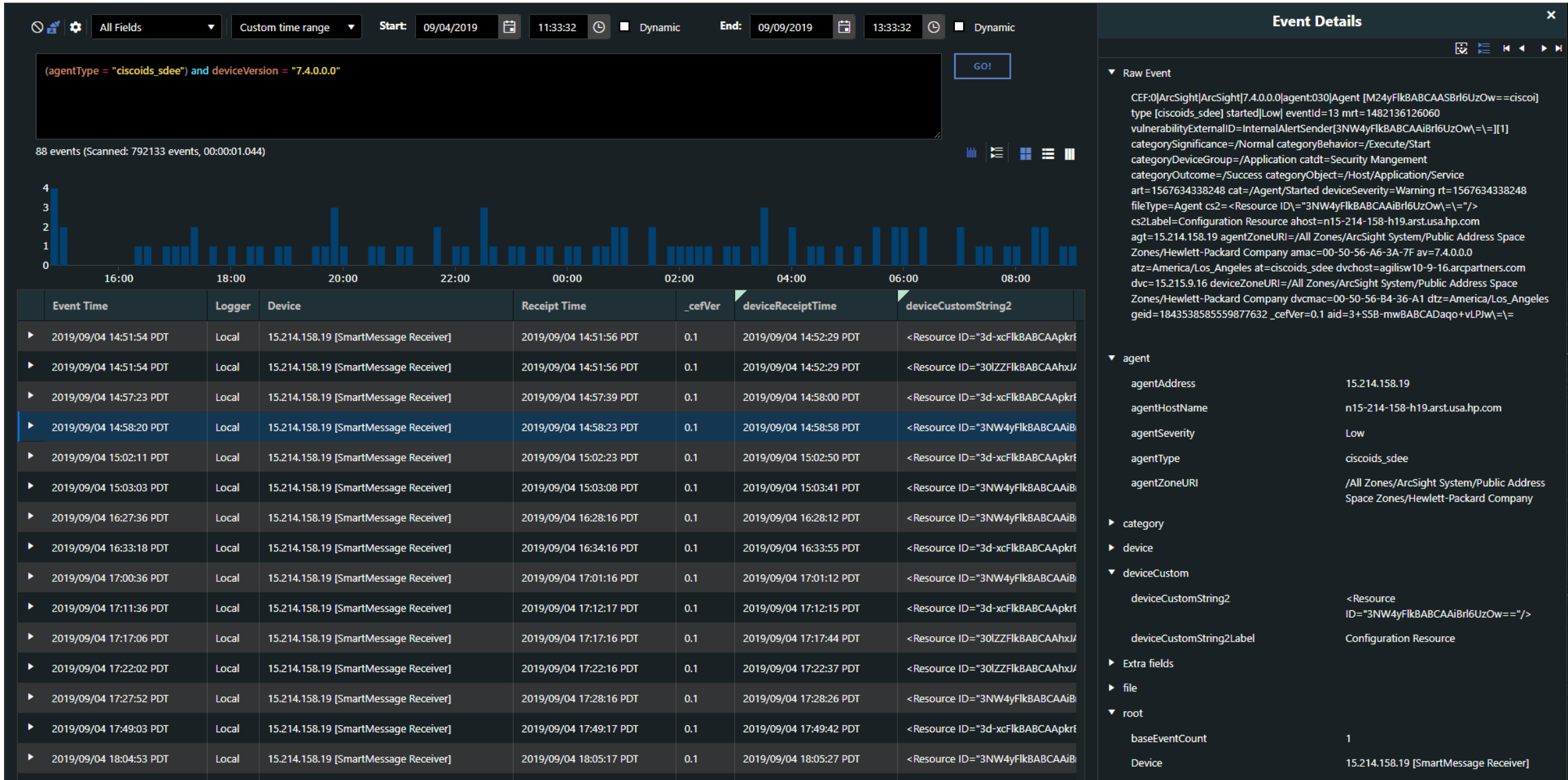


Logger

ArcSight Logger

- До 24 TB онлайн хранения
- EPS лицензирование
- До 25 параллельных поисковых запросов
- Максимальный размер результата до 10kk записей
- Возможность поиска по End Time

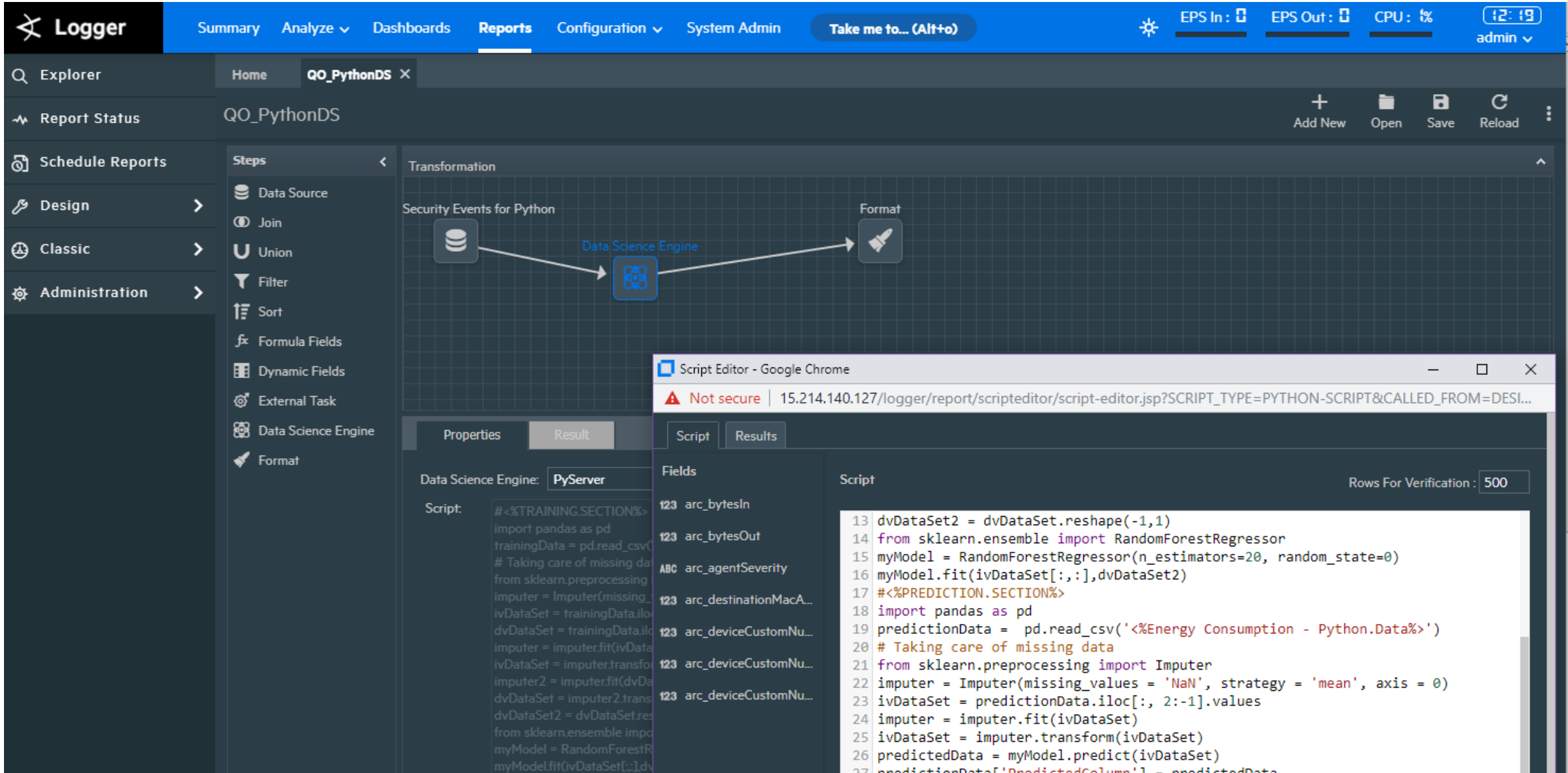
Logger - Новый поисковый UI



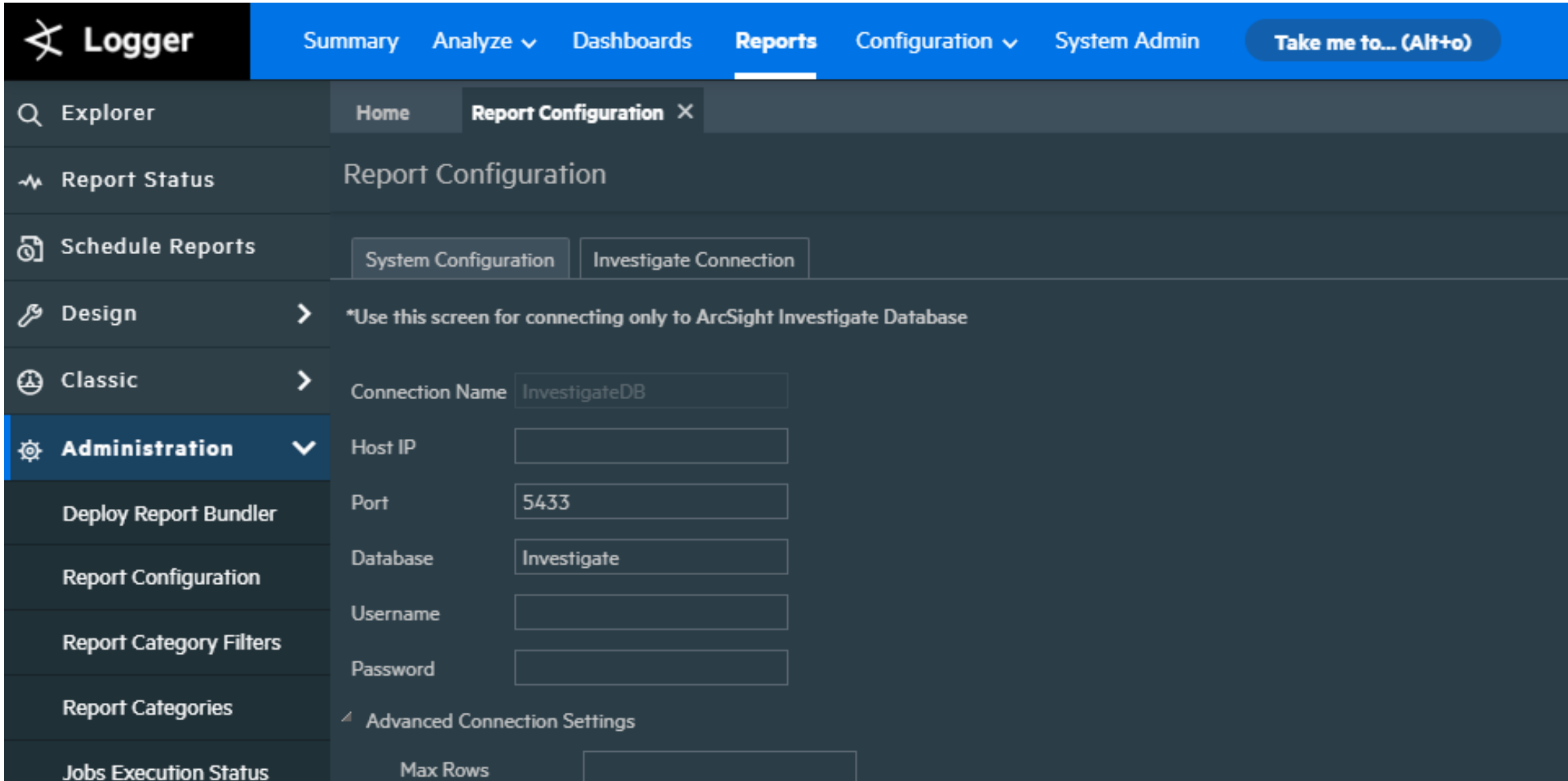
Logger – развитие отчётности

- Data Science Engine
- Отчётность на данных Investigate
- Geo-IP маппинг в отчётах

Data Science Engine



Отчётность на данных Investigate



Geo-IP маппинг в отчётах

Географическая информация теперь доступна в отчётах

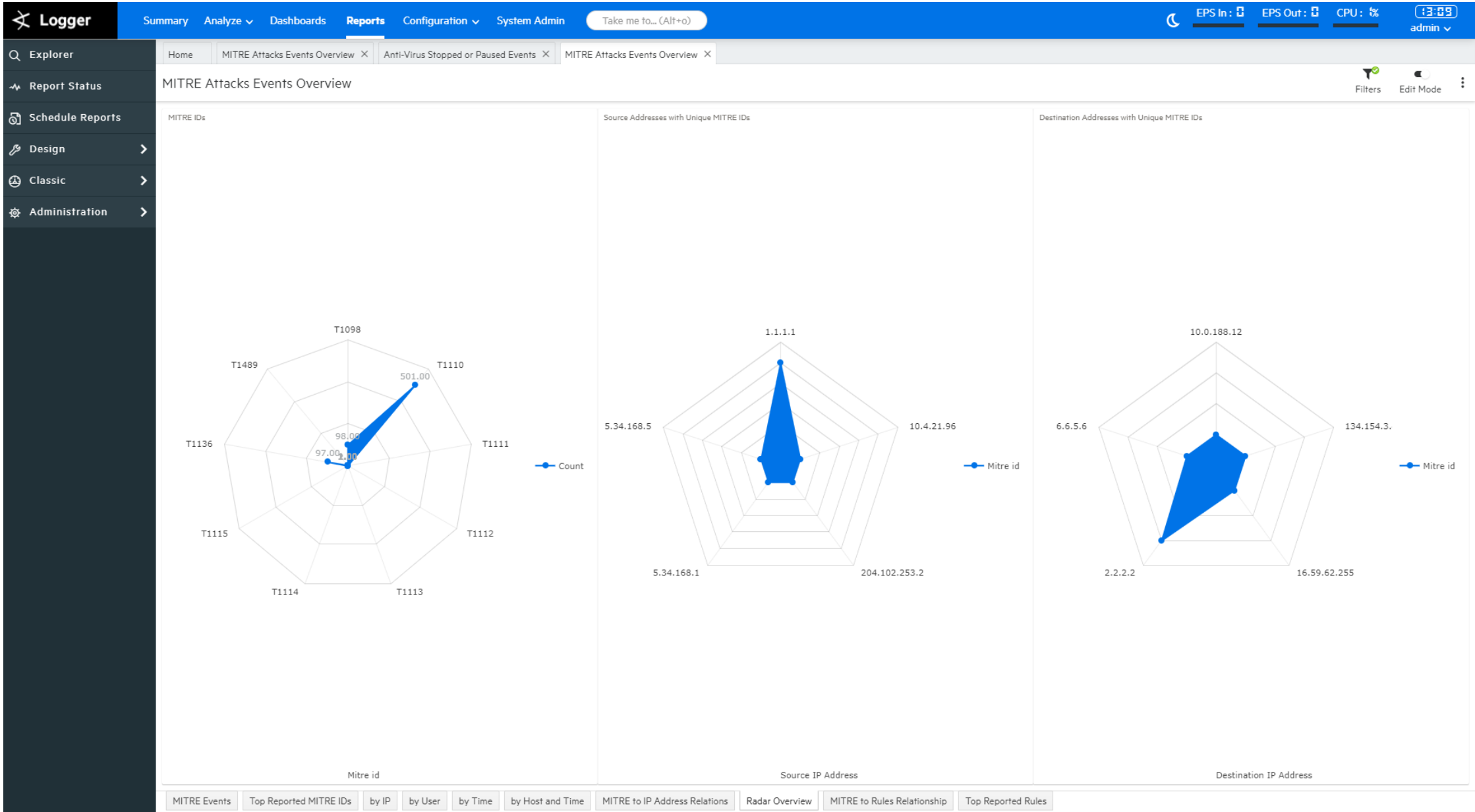
- Визуализация сетевого трафика
- Гео-аномалии

Новый контент для Logger

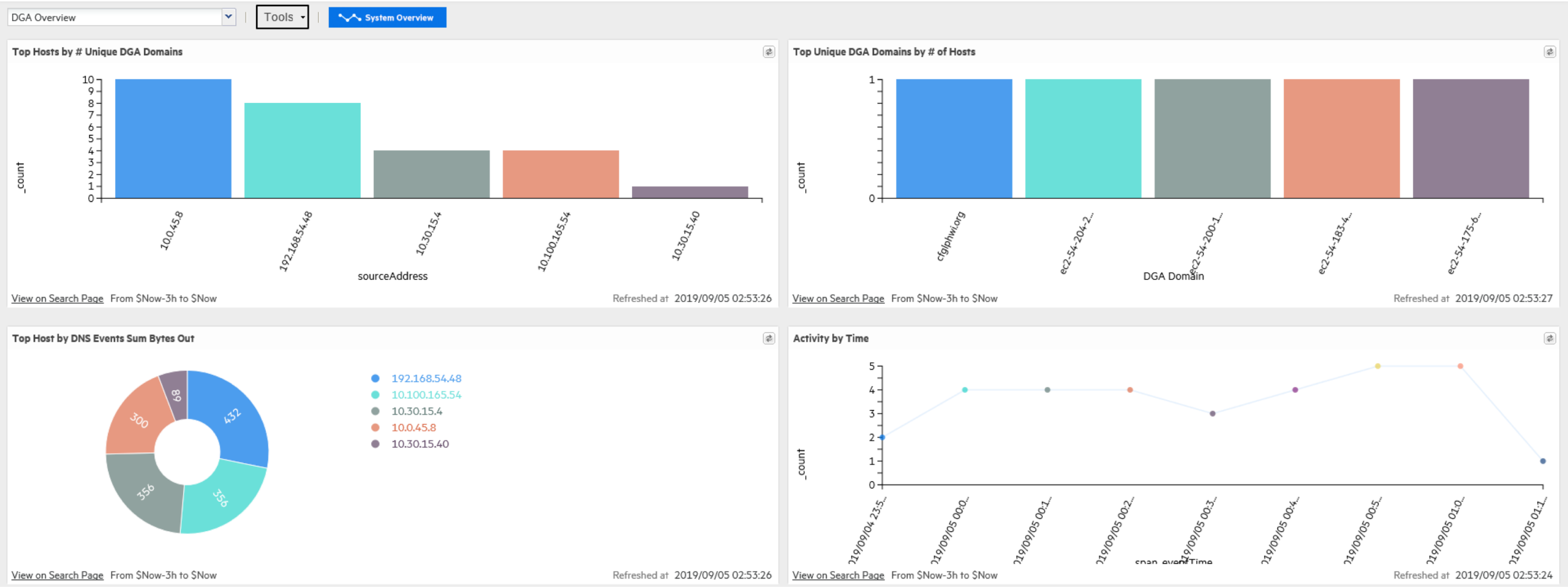
- Глобальная переработка всего контента
- Более 100 новых отчётов:
  - Мониторинг устройств – OS, Anti-Virus, Networking, IDS-IPS, DGA, и другие
  - Foundation – Intrusion, MITRE, Networking, Vulnerability, и другие
  - OWASP
- 8 новых Dashboards
  - Malware Overview
  - DGA
  - MITRE
  - Attack and Suspicious Activity, и другие

OWASP\A 2 - Broken Authentication\Broken Authentication Events (Signatures)

MITRE - Radar Overview



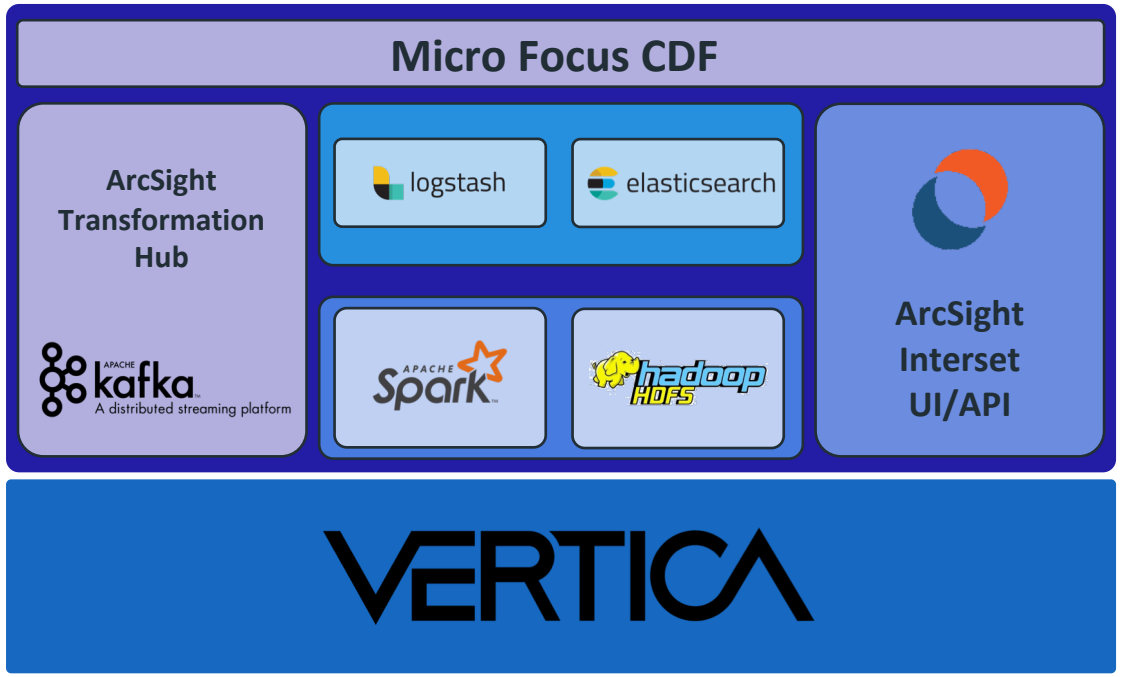
DGA Dashboard



Interset

ArcSight Interset 6.0

- Новая архитектура решения
- Инсталляция с помощью ArcSight CDF
- Поддержка единого UI (Fusion)
- Получение событий от коннекторов ArcSight
- Использование Transformation Hub в архитектуре
- Vertica в качестве хранилища
- Системные требования существенно снижены (по сравнению с версией 5.9)
- Релиз ограниченной доступности



Вопросы?

Спасибо

vyacheslav.tupikov@microfocus.com