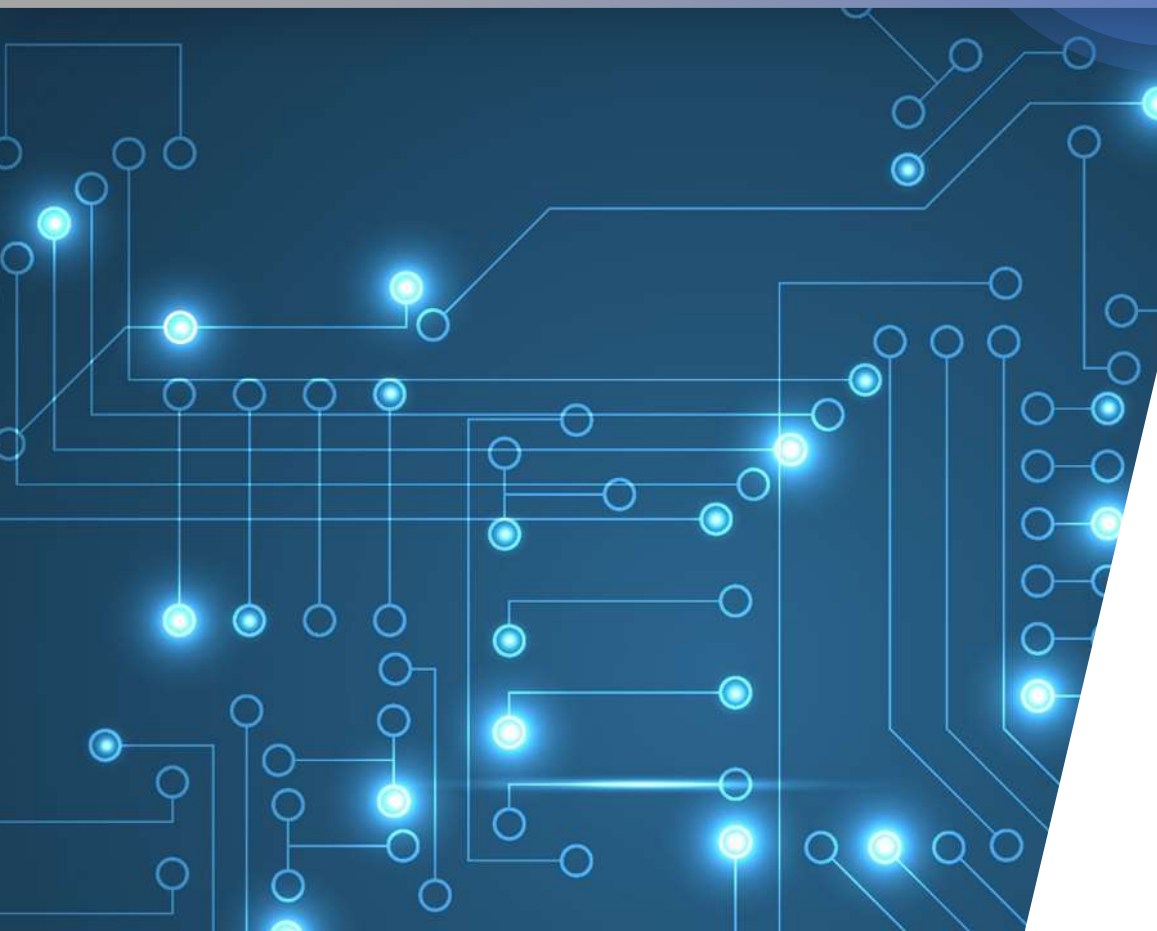
MICRO FOCUS | ArcSight | JETSECURITY CONFERENCE 2018

Изменения в архитектуре решений и новые возможности UBA 6.1

FORWARD-LOOKING STATEMENTS

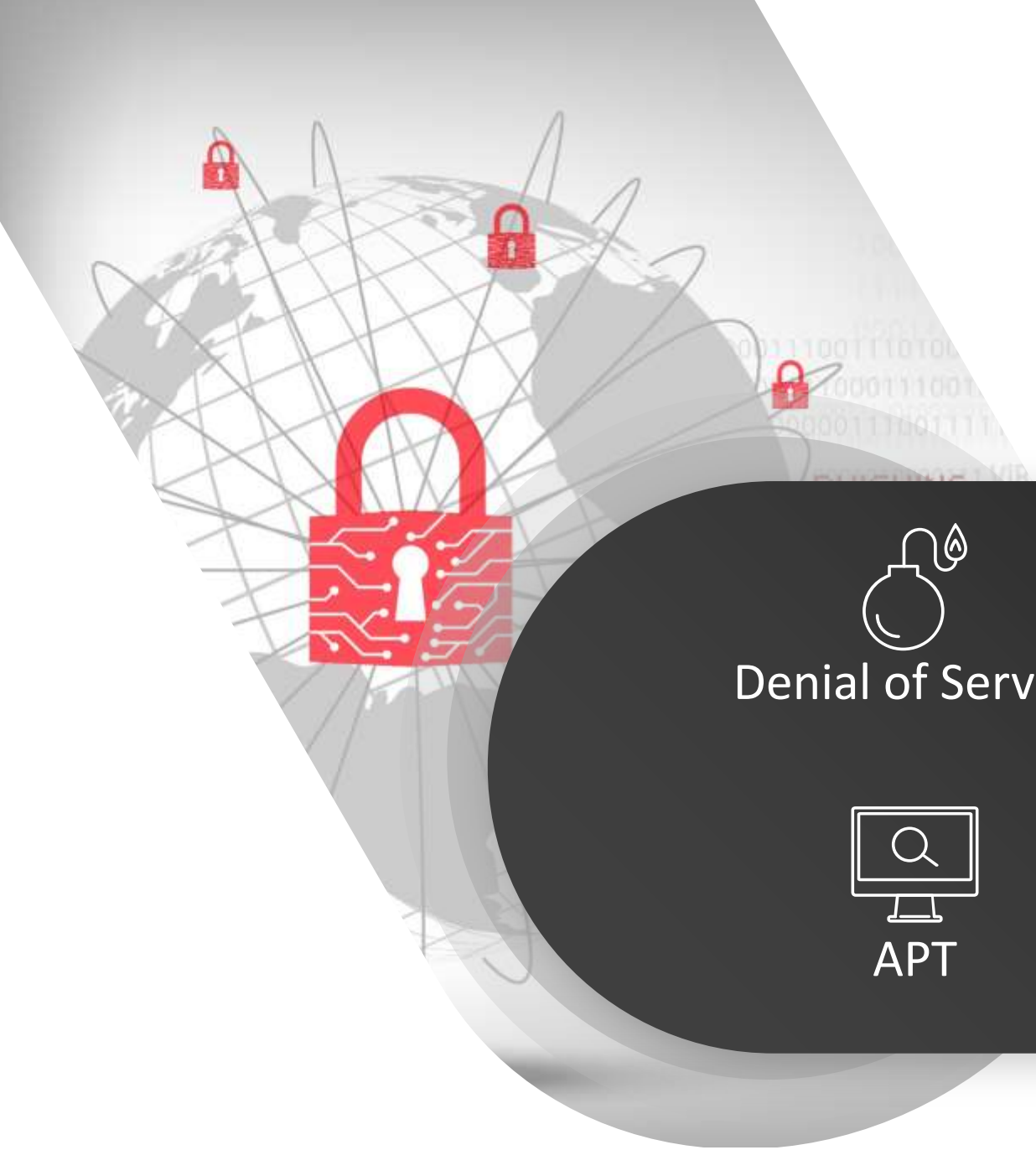
www.microfocus.com



This document contains forward looking statements regarding future operations, product development, product capabilities and availability dates. This information is subject to substantial uncertainties and is subject to change at any time without prior notification. Statements contained in this document concerning these matters only reflect Micro Focus ArcSight's predictions and / or expectations as of the date of this document and actual results and future plans of Hewlett-Packard may differ significantly as a result of, among other things, changes in product strategy resulting from technological, internal corporate, market and other changes. This is not a commitment to deliver any material, code or functionality and should not be relied upon in making purchasing decisions.

User Interface depictions should be considered non-final and subject to re-design and / or removal.

This is a rolling (up to three year) Roadmap and is subject to change without notice.



Всё больше векторов атаки

Denial of Service

Внутренние угрозы

Корпоративный шпионаж

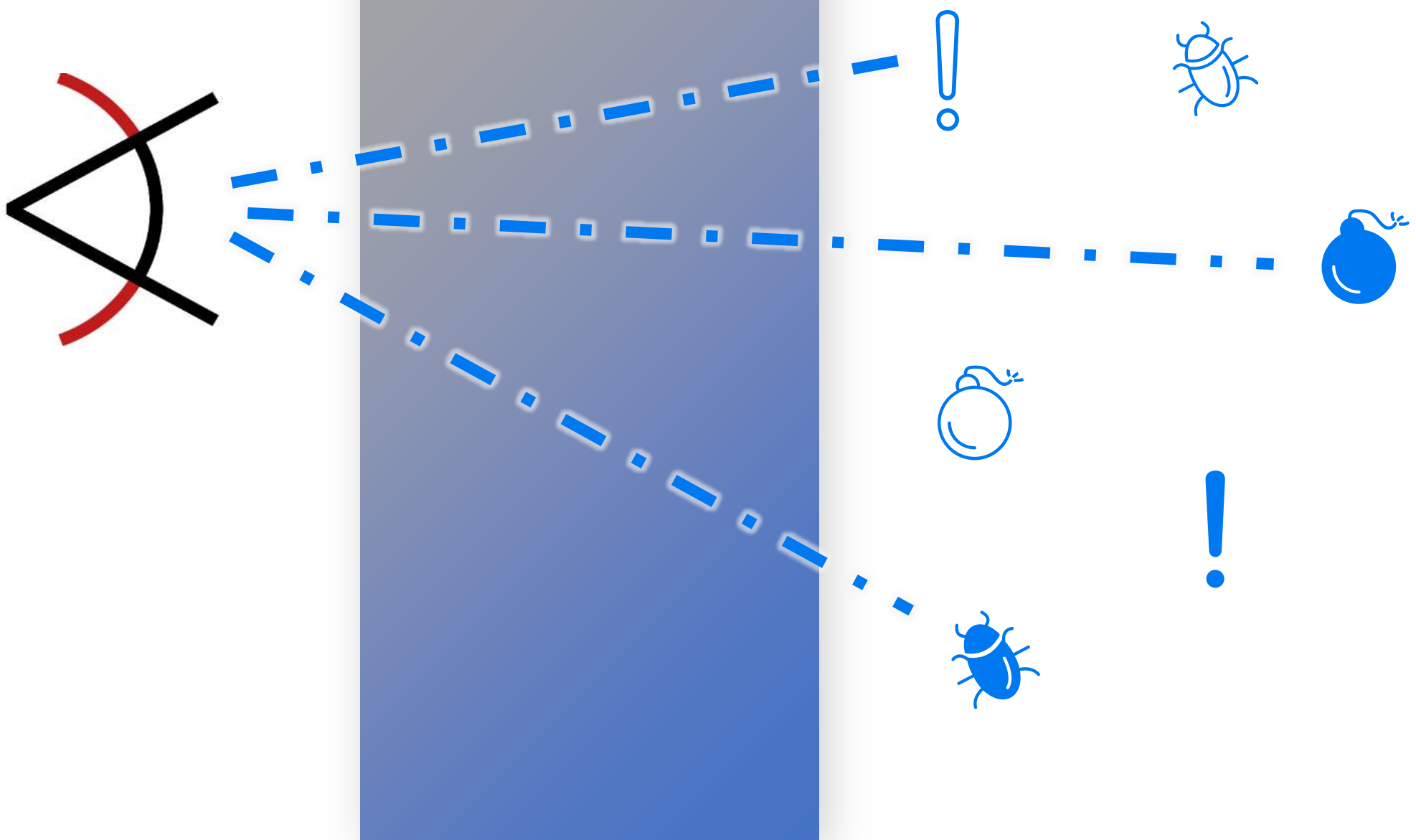
APT

Web-атаки

JETSECURITY CONFERENCE 2018

Enterprise Visibility

Indicators of Compromise



ArcSight

Enterprise Visibility

Пропущенные источники событий

Vulnerability

Sysmon Indicator
(Malicious Process)

Resident Malware

Data Exfil

Credential Abuse

PowerShell Misuse

Agenda

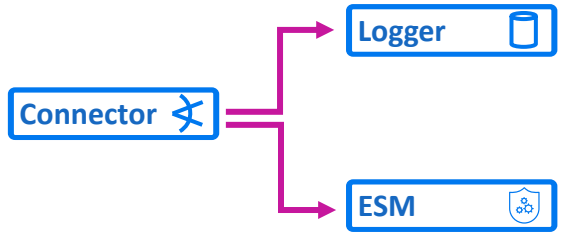
- Новая Архитектура
- ArcSight Data Platform
- ArcSight ESM 7
- ArcSight Investigate
- UEBA 6.1

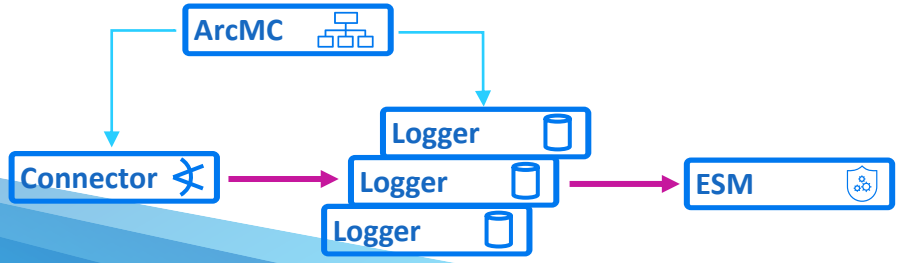
Новая Архитектура

Классические варианты архитектуры

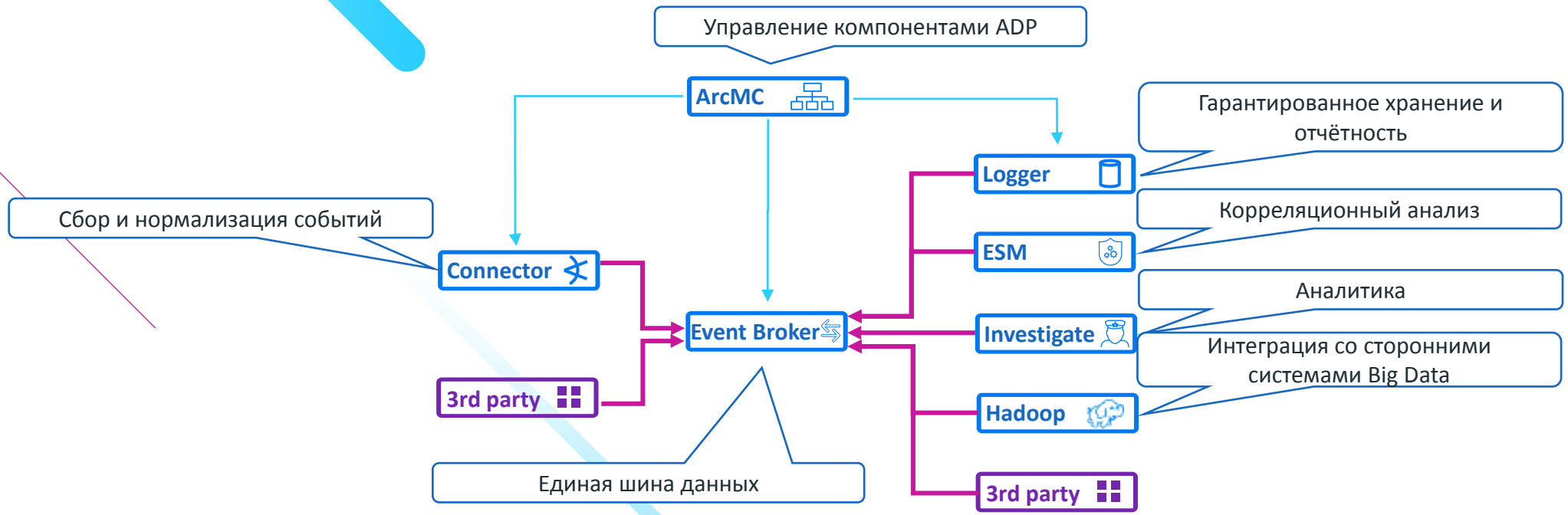
Соответствие стандартам

Выявление угроз





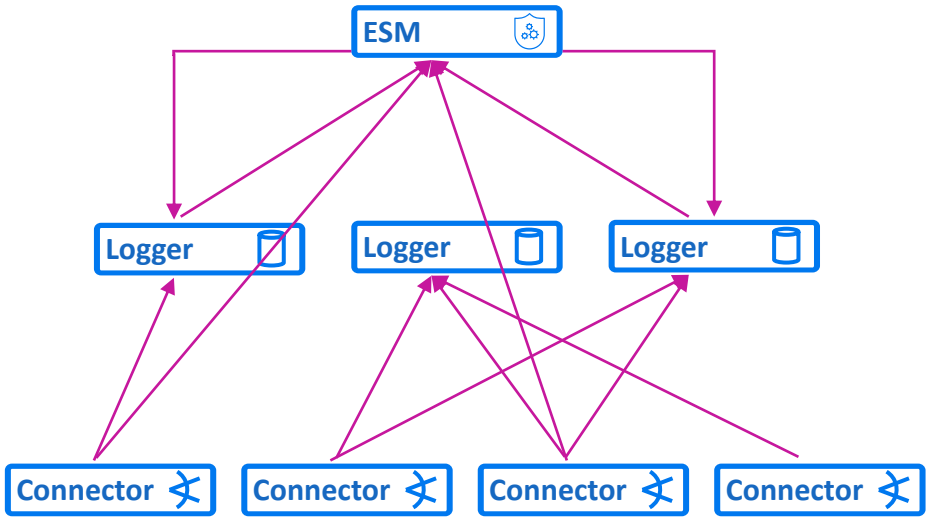
Новая архитектура решения



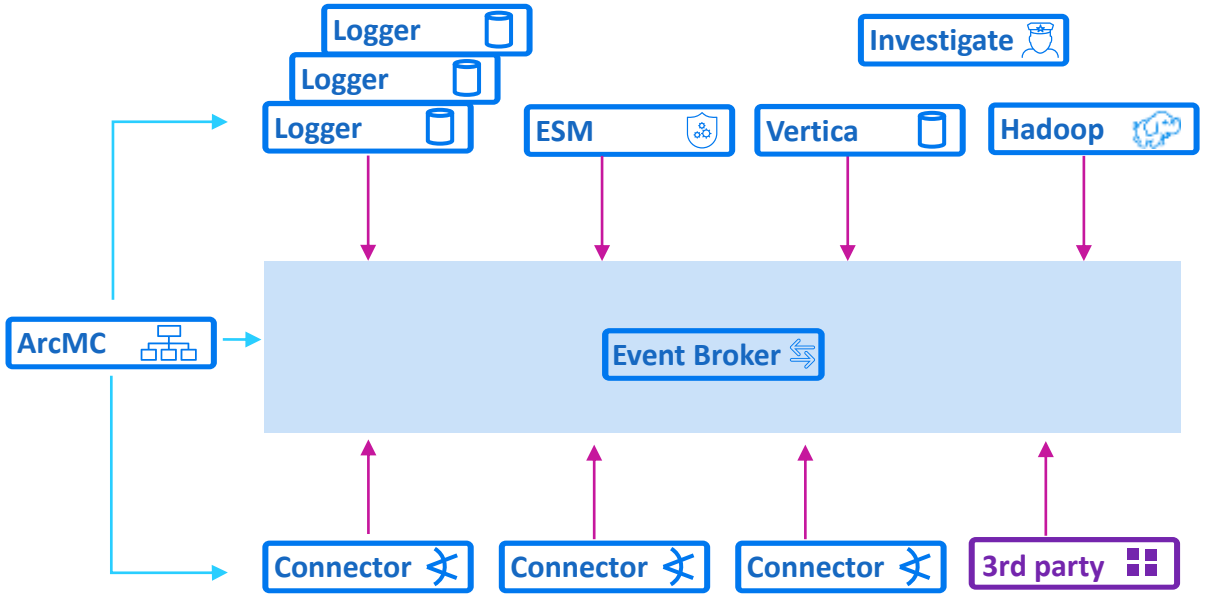
ArcSight Data Platform

Event Broker упрощает комплексную архитектуру

Без Event Broker



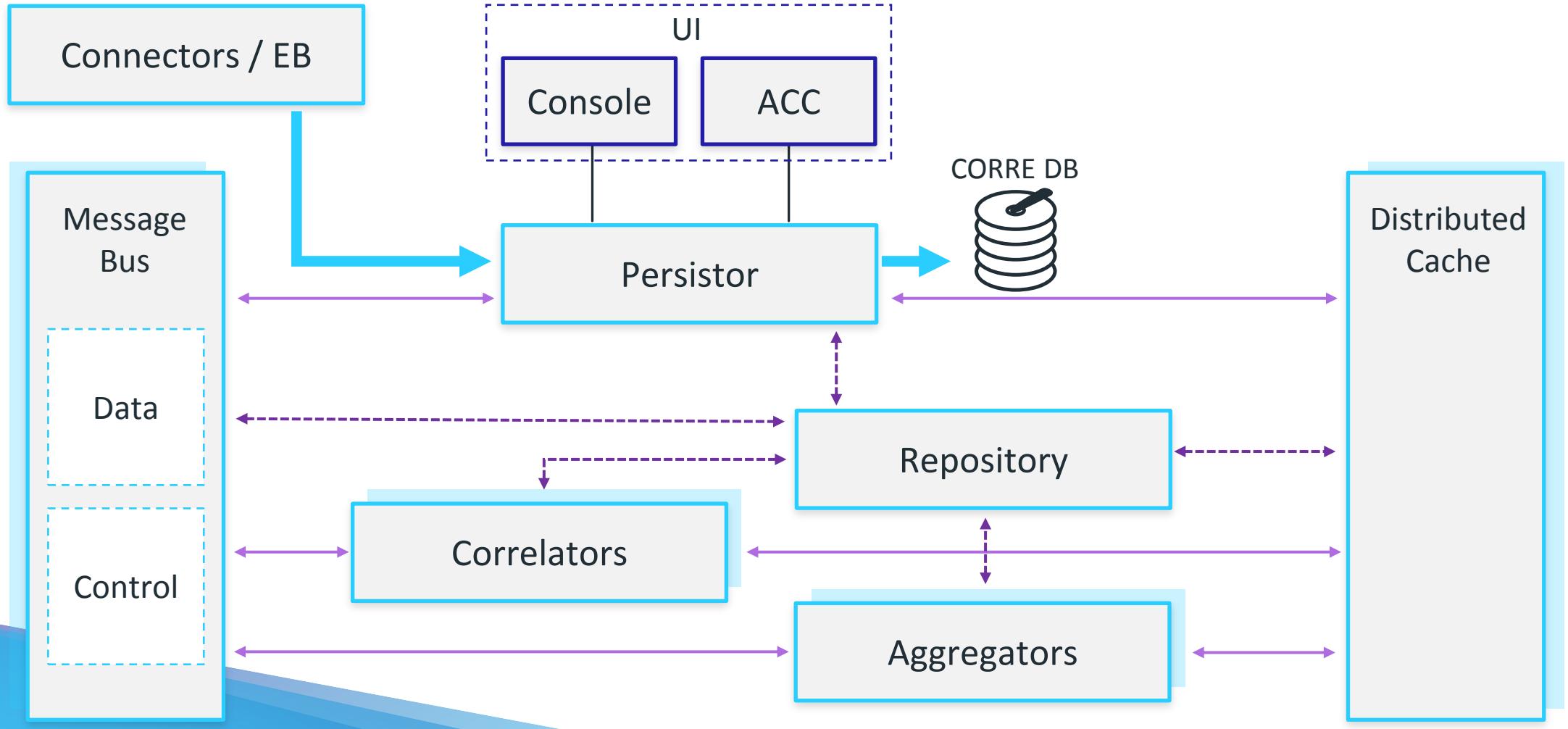
Event Broker



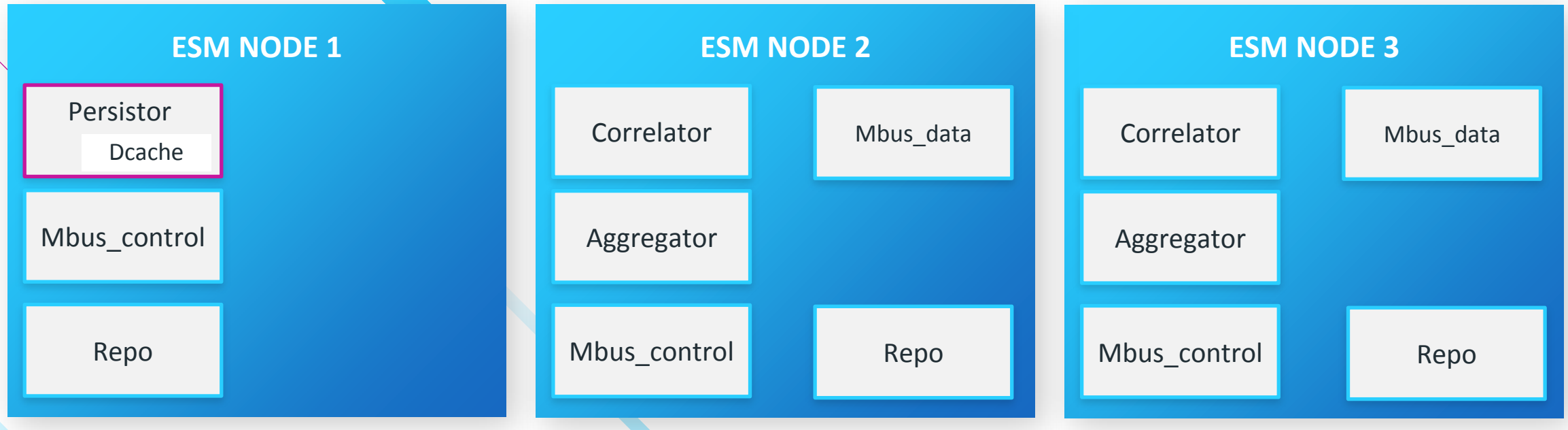
JETSECURITY CONFERENCE 2018

ArcSight ESM 7
Распределённая корреляция

Архитектура распределённой корреляции ESM7



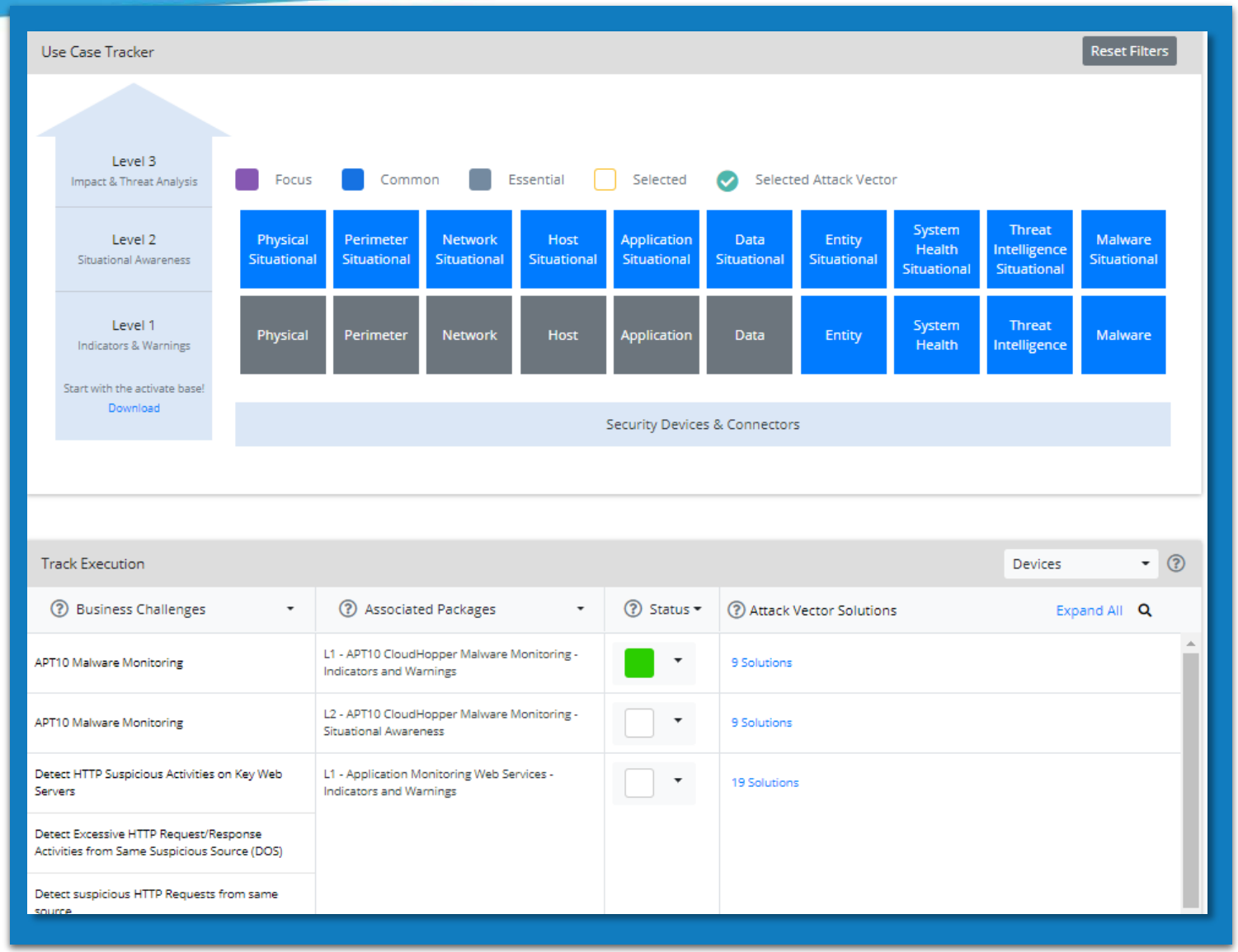
Пример конфигурации для 3х нод



- Persistor существует только на первой ноде и не может быть распределён
- Все остальные компоненты распределяются и масштабируются в соответствии с потребностями в производительности корреляции

ArcSight Content Brain Assessment

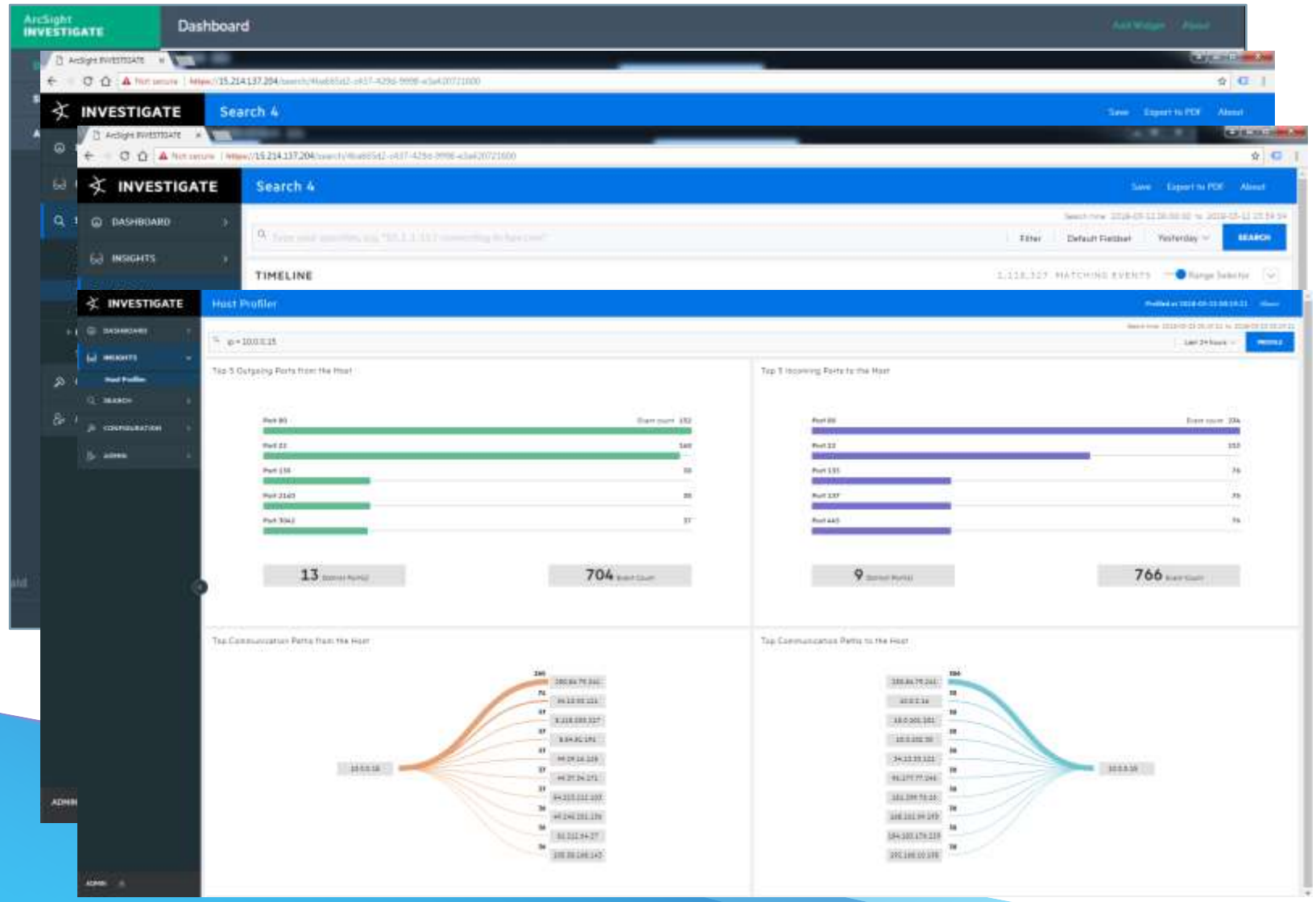
- Бесплатный доступ к готовым наборы корреляционных ресурсов под различные векторы атак и типы источников событий
- Функционал планирования и отслеживания изменений применения наборов контента
- Все ресурсы разработаны выделенной командой специалистов ArcSight и инженерами Professional Services



https://arcsightcontentbrain.com

ArcSight Investigate

ArcSight Investigate



- Надёжное и быстрое решение для аналитики событий
- Google-like search
- Гибкие возможности визуализации
- Встроенные функции профилирования сетевой активности
- Использование листов в качестве критериев для поисковых запросов

JETSECURITY CONFERENCE 2018

User Behavior Analytics (UEBA) 6.1

User and Entity Behavior Analytics

- Hadoop вместо MySQL
- Real-time анализ
- Сопоставление с Kill-Chain
- Интуитивный интерфейс поиска

Спасибо

mailto: vyacheslav.tupikov@microfocus.com
web: https://www.microfocus.com/
community: https://community.softwaregrp.com/

JETSECURITY CONFERENCE 2018

MICRO FOCUS