



# 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

---

Interaset

---



# 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
- НА и NonProd лицензии включены
- Бесплатная миграция

# Лицензирование ArcSight

4 ключевых продукта – единая метрика

ArcSight Marketplace  
Бесплатный и коммерческий контент | Compliance-паки

ArcSight Logger

основано на потоке событий  
(EPS)

ArcSight ESM

основано на потоке событий  
(EPS)

ArcSight Investigate

основано на потоке событий  
(EPS)

Intersect UEBA

основано на активах  
(пользователи и системы)

ArcSight Secure Open Data Platform

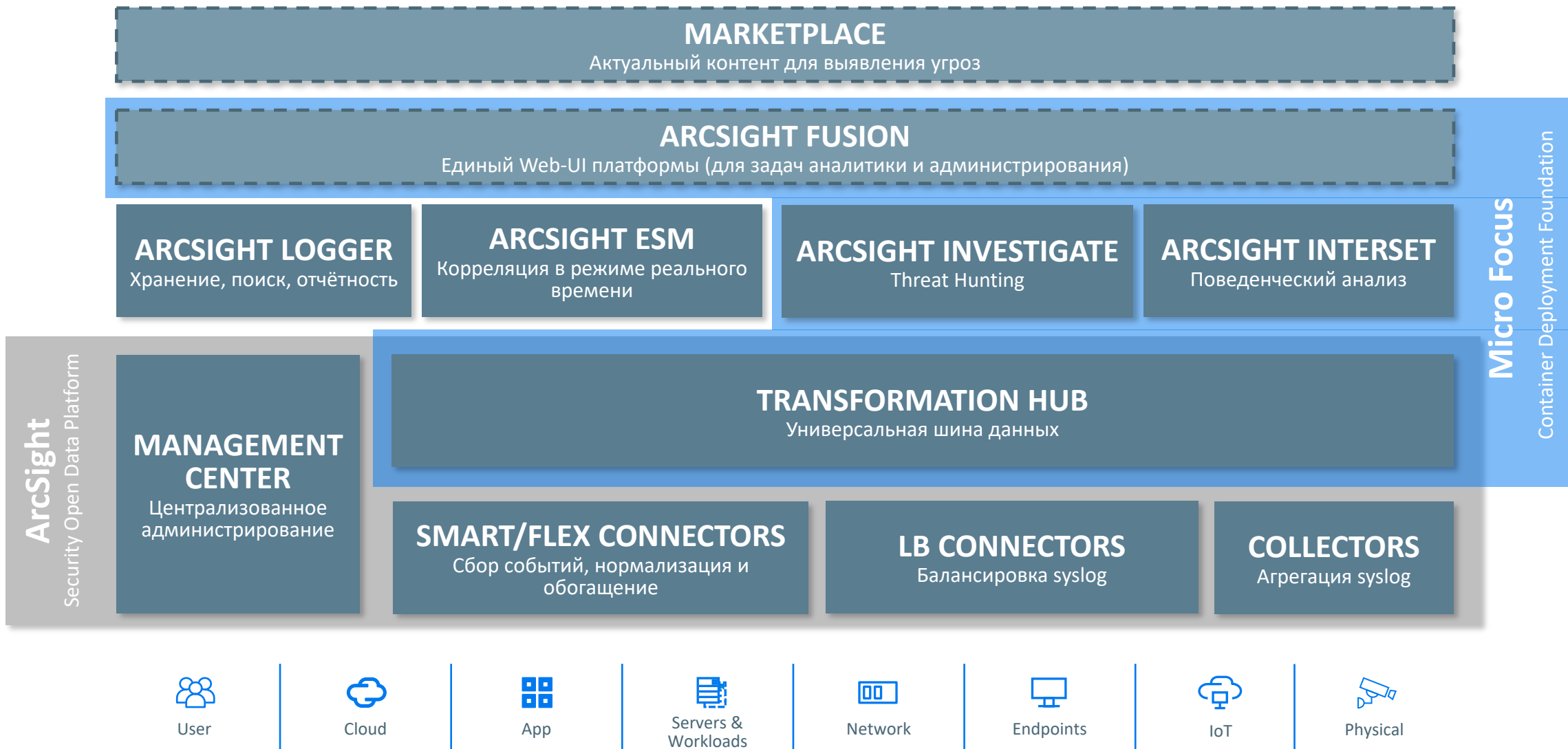
основано на потоке событий (EPS)

включено в каждый ключевой продукт и доступно отдельно



# Архитектура

# Новая архитектура ArcSight

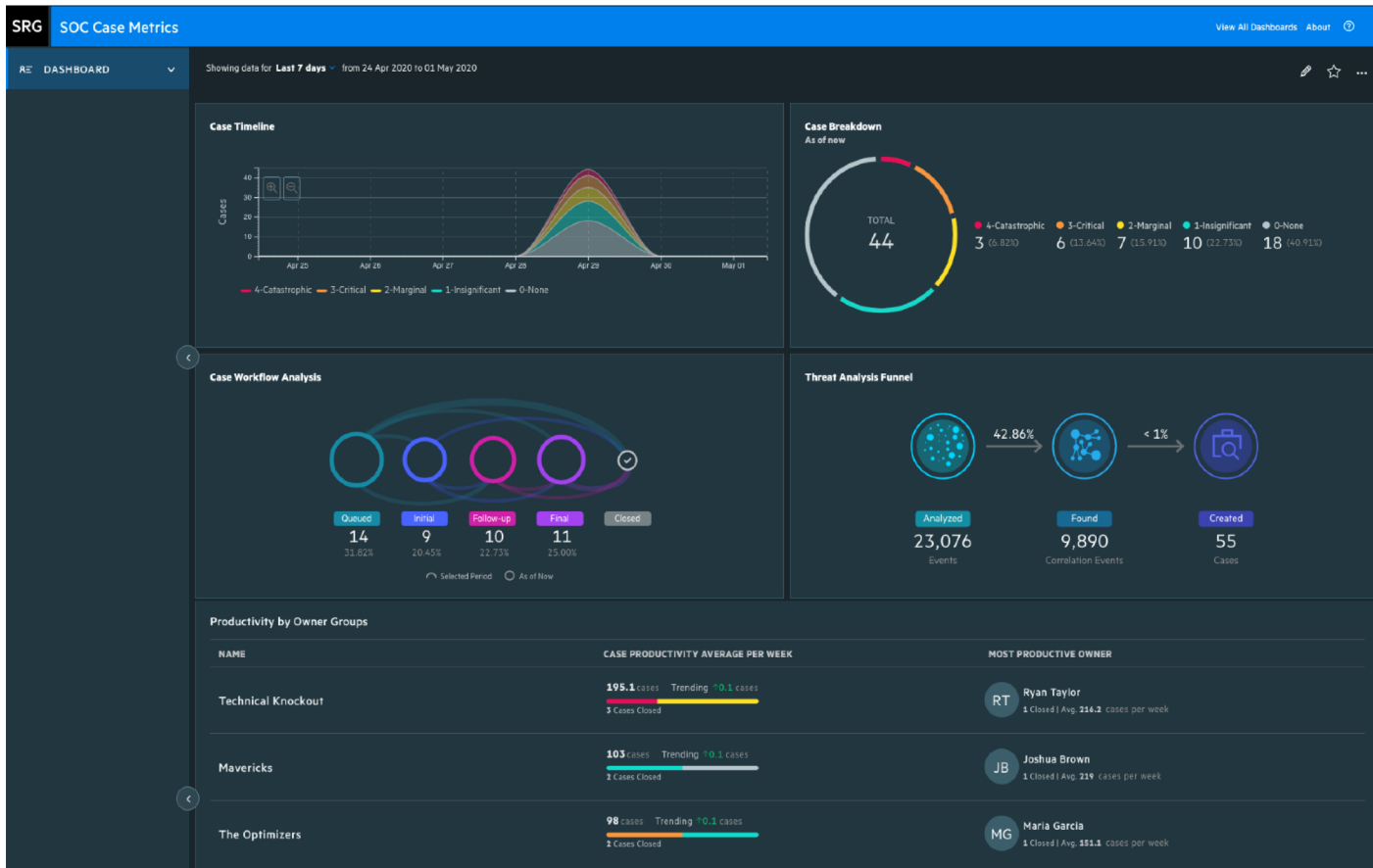




# ESM и Fusion



# ArcSight Fusion



## Наш новый единый UI

- Объединяет ArcSight ESM и Intersect
- 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 корреляторов/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

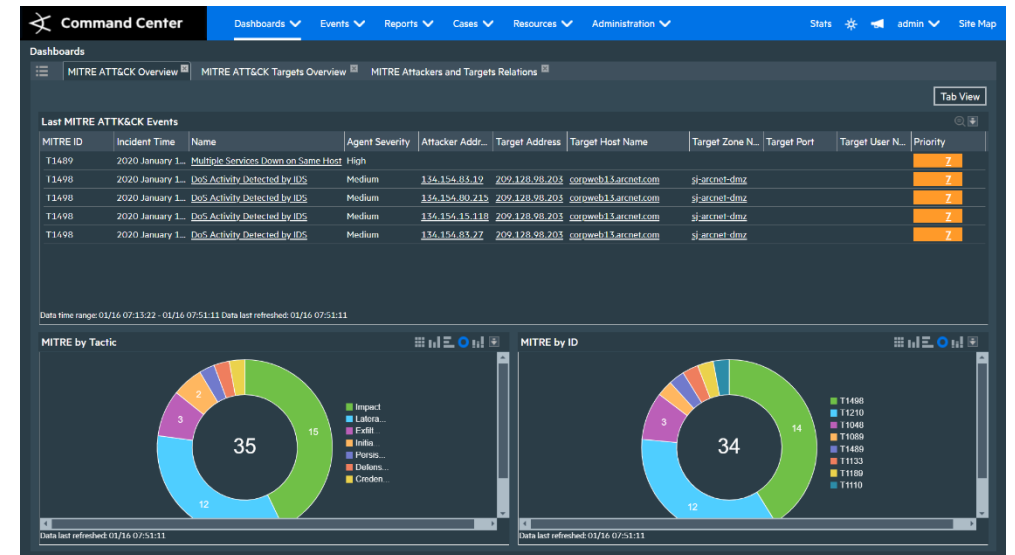
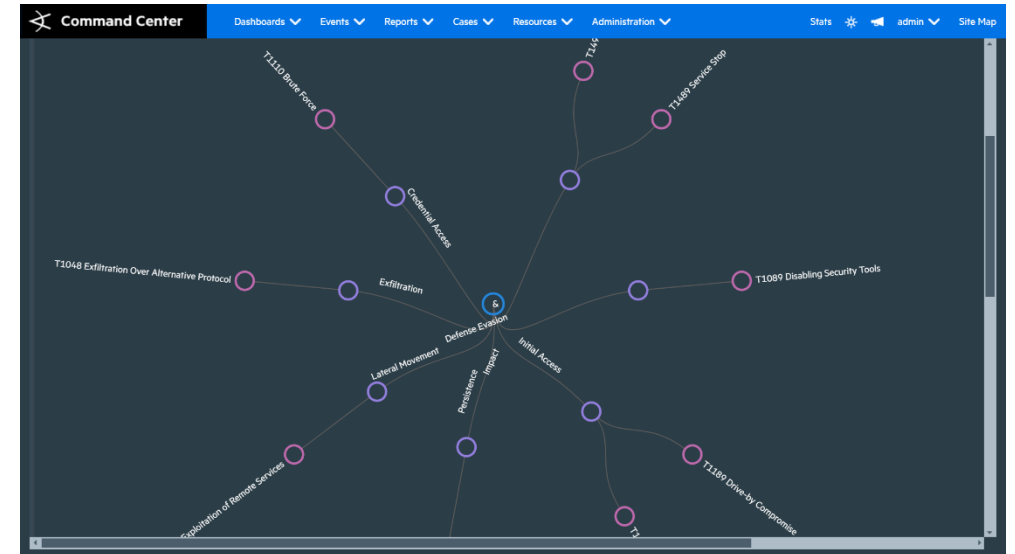
- Выделенное направление по созданию контента
- Стандартный контент по выявлению угроз
- Интеграция контента с MITRE ATT&CK
- Поддержка MISP CIRCL TI (коннектор и контент)
- Обновление Marketplace

# 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



## Layered Analytics (All)

### Legend

- Technique covered in
- Technique covered in
- Not covered content

ArcSight's three analytics solutions can seamlessly be combined to form a "Layered Analytics" approach. This 'best of breed' integration merges the scope and expertise of individual components to produce greater security insights and more comprehensive threat protection. Providing the right type of analytics to solve the right type of use cases, optimizes security operations and dramatically improves organizations' security postures. As a result, your SOC has a fighting chance to find those threats before they turn into a breach.

Initial Access 11	Execution 34	Persistence 63	Privilege Escalation 32	Defense Evasion 74	Credential Access 23	Discovery 25	Lateral Movement 20	Collection 14	Command and Control 22	Exfiltration 10
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration
Exploit Public-Facing App ...	CMSTP	Accessibility Features	Accessibility Features	Application Access Token	Bash History	Application Window Discov ...	Application Access Token	Automated Collection	Communication Through Rem ...	Data Compressed
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	BITS		Browser	Application			
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	Binary F						
Replication Through Remov ...	Component Object Model an ...	AppInit DLLs	Application Shimming	Bypas Account						
Spearphishing Attachment	Control Panel Items	Application Shimming	Bypass User Account Contr ...	CM						
Spearphishing Link	Dynamic Data Exchange	Authentication Package	DLL Search Order Hijackin ...	Clear Co Hist						
Spearphishing via Service	Execution through API	BITS Jobs	Dylib Hijacking	Code S						

### Technique: Accessibility Features

#### Content | Information

#### Name

Unusual port and / or protocol <sup>free</sup>

Unusual registry modifications <sup>free</sup>



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

🔍 ⚙️ All Fields Custom time range Start: 09/04/2019 11:33:32 Dynamic End: 09/09/2019 13:33:32 Dynamic

(agentType = "ciscoids\_sdee" and deviceVersion = "7.4.0.0") GO!

88 events (Scanned: 792133 events, 00:00:01.044)

Event Time	Logger	Device	Receipt Time	_cefVer	deviceReceiptTime	deviceCustomString2
▶ 2019/09/04 14:51:54 PDT	Local	15.214.158.19 [SmartMessage Receiver]	2019/09/04 14:51:56 PDT	0.1	2019/09/04 14:52:29 PDT	<Resource ID="3d-xcFlkBABCAApkrf
▶ 2019/09/04 14:51:54 PDT	Local	15.214.158.19 [SmartMessage Receiver]	2019/09/04 14:51:56 PDT	0.1	2019/09/04 14:52:29 PDT	<Resource ID="30ZZFkIBABCAAhxJ/
▶ 2019/09/04 14:57:23 PDT	Local	15.214.158.19 [SmartMessage Receiver]	2019/09/04 14:57:39 PDT	0.1	2019/09/04 14:58:00 PDT	<Resource ID="3d-xcFlkBABCAApkrf
▶ 2019/09/04 14:58:20 PDT	Local	15.214.158.19 [SmartMessage Receiver]	2019/09/04 14:58:23 PDT	0.1	2019/09/04 14:58:58 PDT	<Resource ID="3NW4yFlkBABCAiBi
▶ 2019/09/04 15:02:11 PDT	Local	15.214.158.19 [SmartMessage Receiver]	2019/09/04 15:02:23 PDT	0.1	2019/09/04 15:02:50 PDT	<Resource ID="3d-xcFlkBABCAApkrf
▶ 2019/09/04 15:03:03 PDT	Local	15.214.158.19 [SmartMessage Receiver]	2019/09/04 15:03:08 PDT	0.1	2019/09/04 15:03:41 PDT	<Resource ID="3NW4yFlkBABCAiBi
▶ 2019/09/04 16:27:36 PDT	Local	15.214.158.19 [SmartMessage Receiver]	2019/09/04 16:28:16 PDT	0.1	2019/09/04 16:28:12 PDT	<Resource ID="3NW4yFlkBABCAiBi
▶ 2019/09/04 16:33:18 PDT	Local	15.214.158.19 [SmartMessage Receiver]	2019/09/04 16:34:16 PDT	0.1	2019/09/04 16:33:55 PDT	<Resource ID="3d-xcFlkBABCAApkrf
▶ 2019/09/04 17:00:36 PDT	Local	15.214.158.19 [SmartMessage Receiver]	2019/09/04 17:01:16 PDT	0.1	2019/09/04 17:01:12 PDT	<Resource ID="3NW4yFlkBABCAiBi
▶ 2019/09/04 17:11:36 PDT	Local	15.214.158.19 [SmartMessage Receiver]	2019/09/04 17:12:17 PDT	0.1	2019/09/04 17:12:15 PDT	<Resource ID="3d-xcFlkBABCAApkrf
▶ 2019/09/04 17:17:06 PDT	Local	15.214.158.19 [SmartMessage Receiver]	2019/09/04 17:17:16 PDT	0.1	2019/09/04 17:17:44 PDT	<Resource ID="30ZZFkIBABCAAhxJ/
▶ 2019/09/04 17:22:02 PDT	Local	15.214.158.19 [SmartMessage Receiver]	2019/09/04 17:22:16 PDT	0.1	2019/09/04 17:22:37 PDT	<Resource ID="30ZZFkIBABCAAhxJ/
▶ 2019/09/04 17:27:52 PDT	Local	15.214.158.19 [SmartMessage Receiver]	2019/09/04 17:28:16 PDT	0.1	2019/09/04 17:28:26 PDT	<Resource ID="3NW4yFlkBABCAiBi
▶ 2019/09/04 17:49:03 PDT	Local	15.214.158.19 [SmartMessage Receiver]	2019/09/04 17:49:17 PDT	0.1	2019/09/04 17:49:42 PDT	<Resource ID="3d-xcFlkBABCAApkrf
▶ 2019/09/04 18:04:53 PDT	Local	15.214.158.19 [SmartMessage Receiver]	2019/09/04 18:05:17 PDT	0.1	2019/09/04 18:05:27 PDT	<Resource ID="3NW4yFlkBABCAiBi

### Event Details

Raw Event

```
CEF:0|ArcSight|ArcSight|7.4.0.0|agent:030|Agent [M24yFlkBABCAASBr6UzOw==cisco] type [ciscoids_sdee] started|Low| eventId=13 mrt=1482136126060 vulnerabilityExternalID=InternalAlertSender[3NW4yFlkBABCAiBr6UzOw\=\=\][1] categorySignificance=/Normal categoryBehavior=/Execute/Start categoryDeviceGroup=/Application catdt=Security Mangement categoryOutcome=/Success categoryObject=/Host/Application/Service fileType=Agent cs2=<Resource ID=\"3NW4yFlkBABCAiBr6UzOw\=\=\"/> cs2Label=Configuration Resource ahost=n15-214-158-h19.arst.usa.hp.com agt=15.214.158.19 agentZoneURI=/All Zones/ArcSight System/Public Address Space Zones/Hewlett-Packard Company amac=00-50-56-A6-3A-7F av=7.4.0.0 atz=America/Los_Angeles at=ciscoids_sdee dvchost=agilsw10-9-16.arcpartners.com dvc=15.215.9.16 deviceZoneURI=/All Zones/ArcSight System/Public Address Space Zones/Hewlett-Packard Company dvmac=00-50-56-B4-36-A1 dtz=America/Los_Angeles geid=184353858559877632 _cefVer=0.1 aid=3+S5B-mwBABCADaQo+vLPJw\=\=\
```

agent

- agentAddress: 15.214.158.19
- agentHostName: n15-214-158-h19.arst.usa.hp.com
- agentSeverity: Low
- agentType: ciscoids\_sdee
- agentZoneURI: /All Zones/ArcSight System/Public Address Space Zones/Hewlett-Packard Company

category

device

deviceCustom

- deviceCustomString2: <Resource ID="3NW4yFlkBABCAiBr6UzOw==" />
- deviceCustomString2.Label: Configuration Resource

Extra fields

file

root

- baseEventCount: 1
- Device: 15.214.158.19 [SmartMessage Receiver]



# Logger – развитие отчётности

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

# Data Science Engine

The screenshot displays the Data Science Engine interface. At the top, there is a navigation bar with tabs for Summary, Analyze, Dashboards, Reports, Configuration, and System Admin. The Reports tab is active. On the right side of the navigation bar, there are system metrics: EPS In, EPS Out, CPU usage, and the current time (12:19) and user (admin).

The main workspace is divided into several sections:

- Explorer:** Shows the current report 'QQ\_PythonDS' and a 'Report Status' section.
- Schedule Reports:** A section for managing report schedules.
- Design:** A central area for building workflows. It shows a 'Transformation' step with a 'Data Source' icon connected to a 'Data Science Engine' icon, which is then connected to a 'Format' icon.
- Administration:** A sidebar menu with options like Design, Classic, and Administration.
- Steps:** A list of available steps including Data Source, Join, Union, Filter, Sort, Formula Fields, Dynamic Fields, External Task, Data Science Engine, and Format.

Below the workflow diagram, there are two panels:

- Properties:** Shows the 'Data Science Engine' set to 'PyServer'.
- Script Editor:** A window titled 'Script Editor - Google Chrome' showing a Python script. The script includes imports for pandas and sklearn, data loading, model fitting, and prediction. The 'Script' tab is active, and the 'Results' tab is also visible. The script content is as follows:

```
13 dvDataSet2 = dvDataSet.reshape(-1,1)
14 from sklearn.ensemble import RandomForestRegressor
15 myModel = RandomForestRegressor(n_estimators=20, random_state=0)
16 myModel.fit(ivDataSet[:,:],dvDataSet2)
17 #<%PREDICTION.SECTION%>
18 import pandas as pd
19 predictionData = pd.read_csv('<%Energy Consumption - Python.Data%>')
20 # Taking care of missing data
21 from sklearn.preprocessing import Imputer
22 imputer = Imputer(missing_values = 'NaN', strategy = 'mean', axis = 0)
23 ivDataSet = predictionData.iloc[:, 2:-1].values
24 imputer = imputer.fit(ivDataSet)
25 ivDataSet = imputer.transform(ivDataSet)
26 predictedData = myModel.predict(ivDataSet)
27 predictionData['PredictedColumn'] = predictedData
```

The 'Results' tab shows a list of fields with their corresponding values, such as 'arc\_bytesIn', 'arc\_bytesOut', 'arc\_agentSeverity', etc.

# Отчётность на данных Investigate

The screenshot shows the ArcSight Investigate web interface. At the top, there is a navigation bar with a 'Logger' logo and several menu items: 'Summary', 'Analyze', 'Dashboards', 'Reports' (which is highlighted), 'Configuration', and 'System Admin'. A 'Take me to... (Alt+o)' button is also present. Below the navigation bar, there is a breadcrumb trail: 'Home' > 'Report Configuration'. The main content area is titled 'Report Configuration' and contains two tabs: 'System Configuration' and 'Investigate Connection'. The 'Investigate Connection' tab is active. A warning message states: '\*Use this screen for connecting only to ArcSight Investigate Database'. Below this, there are several input fields for configuration: 'Connection Name' (filled with 'InvestigateDB'), 'Host IP', 'Port' (filled with '5433'), 'Database' (filled with 'Investigate'), 'Username', and 'Password'. At the bottom, there is a section for 'Advanced Connection Settings' with a 'Max Rows' input field.

Logger

Summary Analyze Dashboards **Reports** Configuration System Admin [Take me to... \(Alt+o\)](#)

Explorer Home **Report Configuration**

Report Status Report Configuration

Schedule Reports System Configuration Investigate Connection

Design > \*Use this screen for connecting only to ArcSight Investigate Database

Classic >

**Administration** >

Deploy Report Bundler

Report Configuration

Report Category Filters

Report Categories

Jobs Execution Status

Connection Name

Host IP

Port

Database

Username

Password

Advanced Connection Settings

Max Rows

# Geo-IP мappинг 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

✦ Logger

Summary Analyze ▾ Dashboards Reports Configuration ▾ System Admin

Take me to... (Alt+o)
EPS In:   
EPS Out:   
CPU:   %
13:09
admin ▾

MITRE Attacks Events Overview
Filters Edit Mode

MITRE IDs

Mitre id

Source Addresses with Unique MITRE IDs

Source IP Address

Destination Addresses with Unique MITRE IDs

Destination IP Address

MITRE Events
Top Reported MITRE IDs
by IP
by User
by Time
by Host and Time
MITRE to IP Address Relations
Radar Overview
MITRE to Rules Relationship
Top Reported Rules

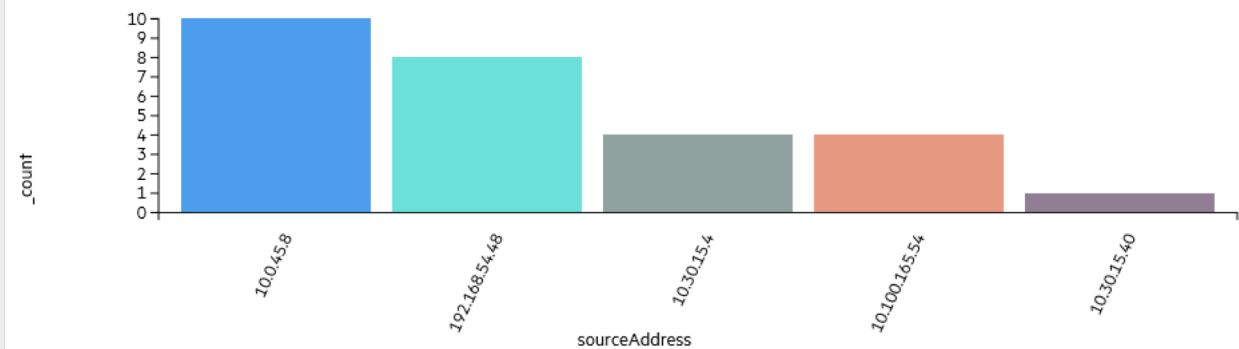
# DGA Dashboard

DGA Overview

Tools

System Overview

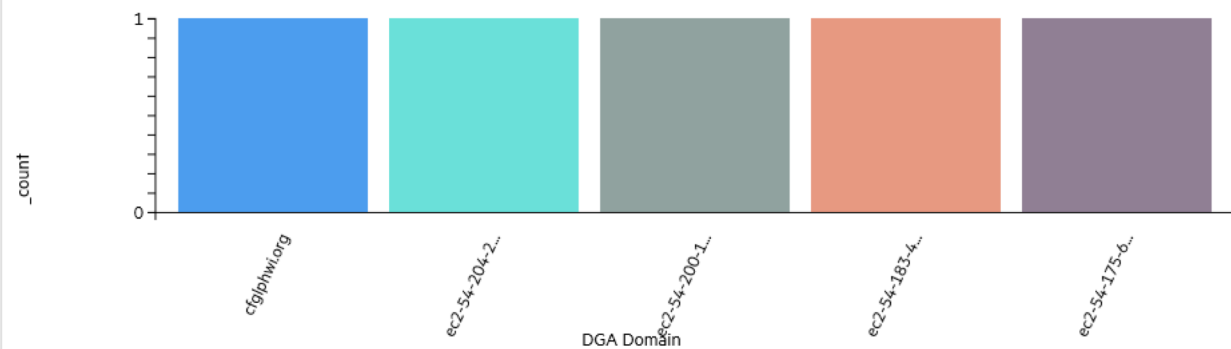
Top Hosts by # Unique DGA Domains



[View on Search Page](#) From \$Now-3h to \$Now

Refreshed at 2019/09/05 02:53:26

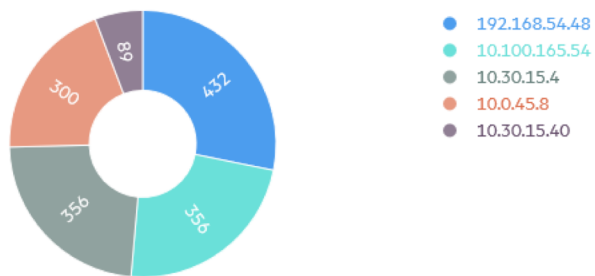
Top Unique DGA Domains by # of Hosts



[View on Search Page](#) From \$Now-3h to \$Now

Refreshed at 2019/09/05 02:53:27

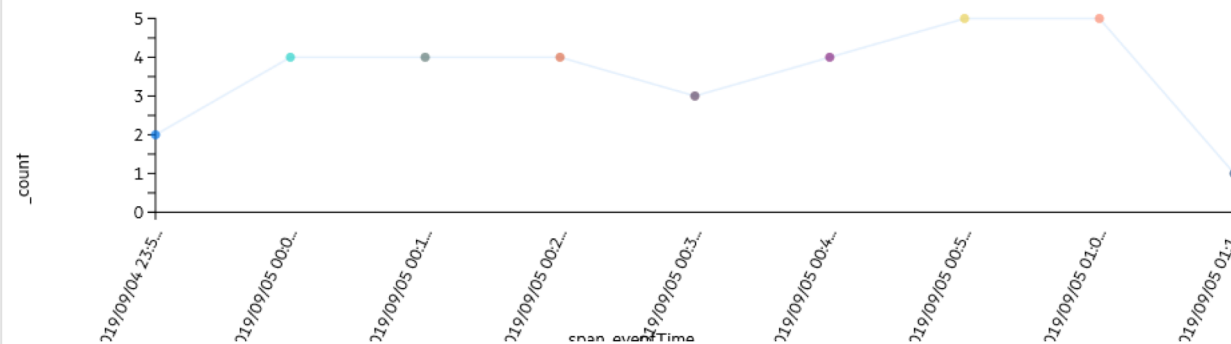
Top Host by DNS Events Sum Bytes Out



[View on Search Page](#) From \$Now-3h to \$Now

Refreshed at 2019/09/05 02:53:26

Activity by Time



[View on Search Page](#) From \$Now-3h to \$Now

Refreshed at 2019/09/05 02:53:24

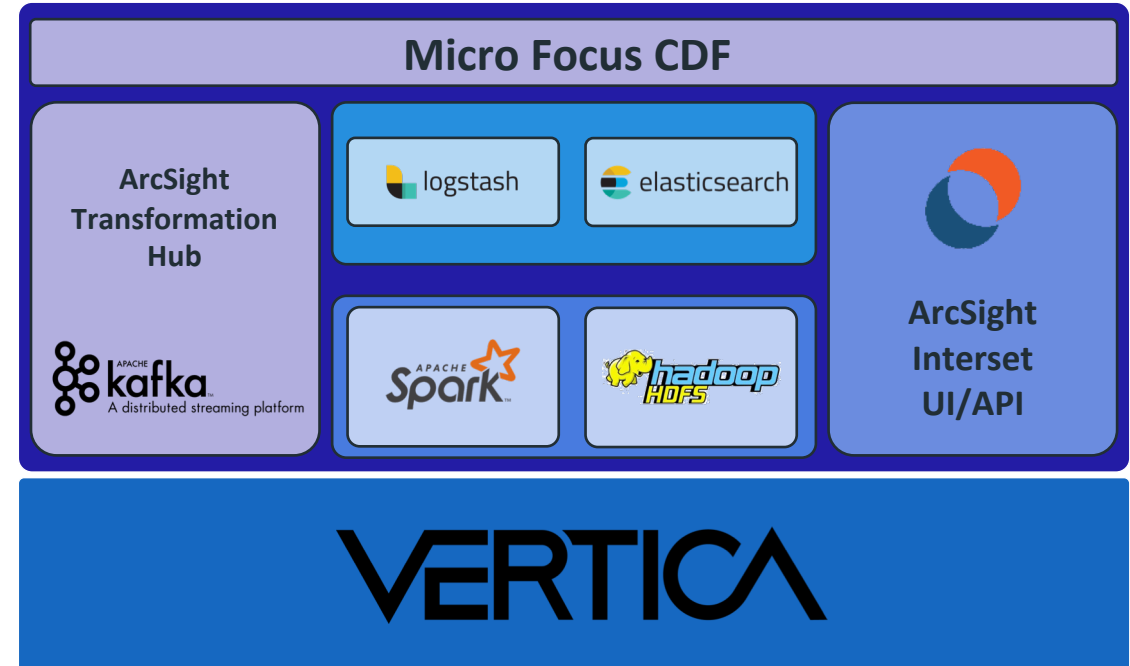




**Interaset**

# ArcSight Interaset 6.0

- Новая архитектура решения
- Установка 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](mailto:vyacheslav.tupikov@microfocus.com)**