



# Современное управление SIEM и контроль качества SOC

**Игорь Волошин**

**Региональный менеджер по продажам | CIS | SOC Prime**

# О нас



Международный вендор

Компания основана в 2014 г.

200+ лет кумулятивного опыта в ИБ

Опыт 100+ SIEM проектов

**Технологические партнёры:**

HPE ArcSight, IBM QRadar, Splunk,

Qualys, Vulners

# миссия SOC Prime:

## Мы помогаем компаниям улучшить качество и зрелость кибер-безопасности

Повышение качества работы SOC за счет непрерывного мониторинга и обеспечения прозрачности оценки работы технической поддержки.

Снижение общей стоимости владения SOC за счет автоматизации операций и обмена аналитическими правилами обнаружения инцидентов.

Контроль результатов работы SOC в виде понятном руководству.

# Возможности SOC Prime:

Наши собственные исследования: База знаний и десятилетия повседневной практики в ИБ, 200 + лет совокупный опыт наших сотрудников

Глобальные стандарты: база знаний SANS, MITRE ATT&CK, Lockheed Martin Cyber Kill Chain

Собственные и открытые алгоритмы машинного обучения

Мы запускаем модель SaaS Business, поэтому мы не просто «в облаке», но и поддерживаем полностью отказоустойчивую архитектуру в AWS, On-Premise или Offline (без Интернета)

Поддержка, обновления и службы TAM включаются в каждую подписку

Мы решаем наиболее сложные задачи безопасности с нашей платформой, услугами и партнерами

# Наши клиенты

MSSP



Финансы



Телеком



Лого конфиденциально

Государственный сектор

Агропромышленный сектор

Медиа сектор

Легкая промышленность

Forbes Global 2000

# Ну всё ... купили

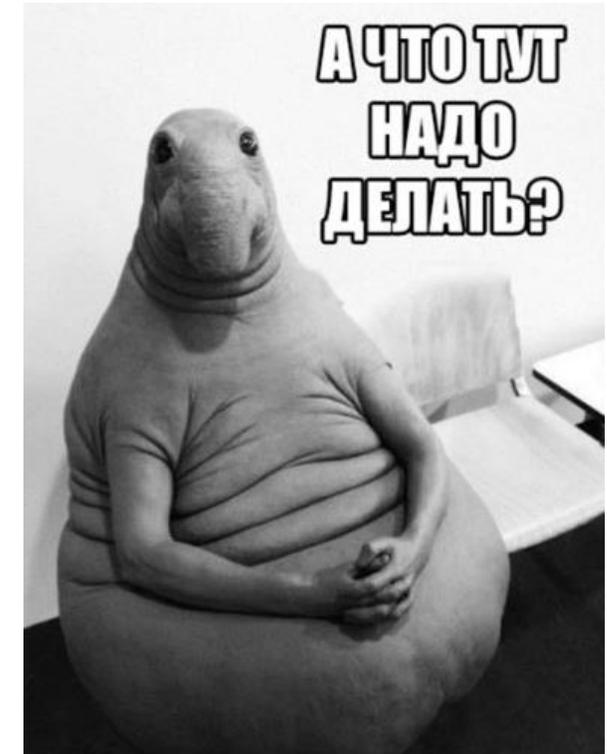
Из коробки



Ожидание



Реальность

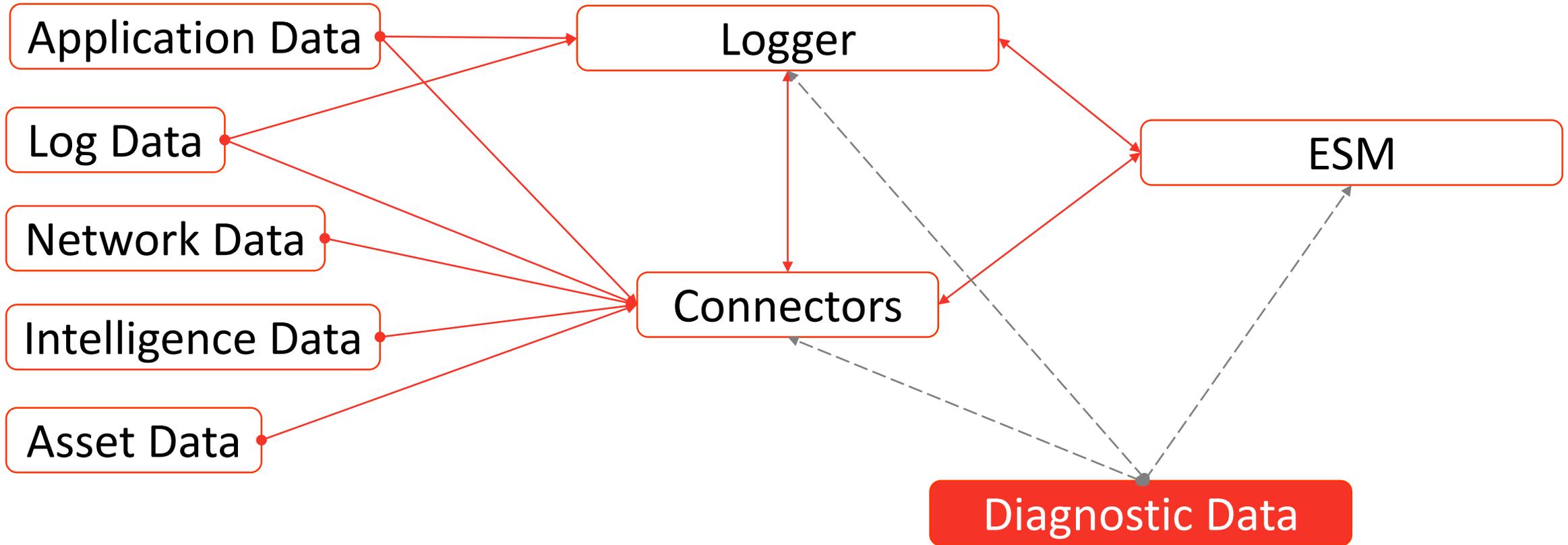


# ОСТОРОЖНО: дальше примеры на ArcSight



ArcSight:  
“I’m old, not obsolete.”

# Данные для SOC на примере ArcSight



# Тренды: SIEM =//= SOC

30% проектов SIEM не имеют выделенных FTE или 1 FTE max  
Средний размер команды SIEM  $\leq$  3 специалистов  
Большинство проектов не имеют выделенного SIEM администратора  
Спрос и дефицит на специалистов высокого класса SIEM растут  
Низкие бюджеты на обучение персонала являются обычным явлением,  
особо остро в Центральной и Восточной Европе и СНГ  
Удержание персонала процесс не простой

# Сбор данных

Доступность: а все ли данные к нам поступают?

Актуальность: данные приходят вовремя?

# Сбор данных: доступность

Все меняется = журналы теряются по пути к SIEM  
Изменение паролей, неправильная конфигурация,  
сетевой доступ, регламентные работы...  
Больше проект = больше FTE

# Диагностика доступности

## 3 места где начинать поиск

Источник журналов

«Коннектор»

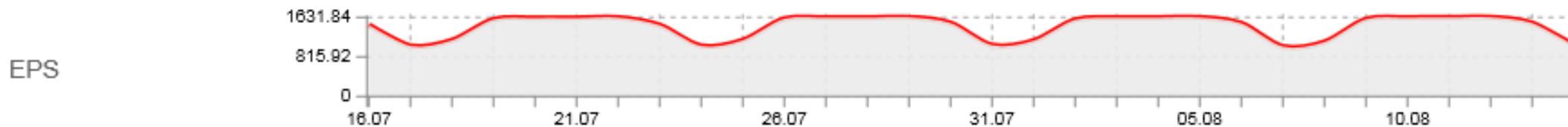
«Logger и ESM»

# Диагностика доступности | источники событий

‘System Monitored’ статус (HPE Activate)

Manager Receipt Time ↑ 1	End Time ⇅	Name ⇅	Event Annotation Stage	Device Vendor ⇅	Device Host Name ⇅	Device Address ⇅
15 Aug 2016 09:16:47 BST	15 Aug 2016 09:16:42 BST	Windows Domain Brute Force Logon	System Monitored	ArcSight		11
15 Aug 2016 09:16:45 BST	15 Aug 2016 09:16:38 BST	Windows Domain Brute Force Logon	System Monitored	ArcSight		11
15 Aug 2016 09:16:41 BST	15 Aug 2016 09:16:36 BST	Windows Domain Brute Force Logon	System Monitored	ArcSight		11
15 Aug 2016 09:16:39 BST	15 Aug 2016 09:16:31 BST	Computer Account Changed	System Monitored	ArcSight		11
15 Aug 2016 09:16:39 BST	15 Aug 2016 09:16:31 BST	Computer Account Changed	System Monitored	ArcSight		11
15 Aug 2016 09:16:35 BST	15 Aug 2016 09:16:08 BST	Computer Account Changed	System Monitored	ArcSight		11
15 Aug 2016 09:16:34 BST	15 Aug 2016 09:16:27 BST	Windows Domain Brute Force Logon	System Monitored	ArcSight		11
15 Aug 2016 09:16:22 BST	15 Aug 2016 09:16:18 BST	Windows Domain Brute Force Logon	System Monitored	ArcSight		11
15 Aug 2016 09:16:18 BST	15 Aug 2016 09:16:12 BST	Windows Brute Force Logon	System Monitored	ArcSight		11
15 Aug 2016 09:16:17 BST	15 Aug 2016 09:16:01 BST	Computer Account Changed	System Monitored	ArcSight		11

Тренд и профилирование EPS для каждого источника



# Диагностика доступности: ADP

## Connector

agent.log

agent.properties

agent.wrapper.conf

agent.out.wrapper.log

## Logger

logger\_web.log

logger\_server.log

## ESM & Express

server.log

server.std.log

server.properties

server.wrapper.conf

arc\_active\_list

arc\_session\_list

arc\_trendinformation\_schema

arc\_resource

# Диагностика доступности | Connector

## Connector: device event statistics

```
[2016-08-15 07:27:09,844][INFO ][default.com.arcsight.agent.ki][logStatus] {Eps=0.1, Evts=21829}
[2016-08-15 07:27:09,844][INFO ][default.com.arcsight.agent.ki][logStatus] Transport flow status:
[2016-08-15 07:27:09,844][INFO ][default.com.arcsight.agent.ki][logStatus] {AddrBasedSysZonePopEvents=11812, AddrBasedSysZonePopRows=136, AddrBasedUserZonePopCusts=1, AddrBasedUserZonePopRows=3, AddrBasedZonePopEvents=0, AddrBasedZonePopRows=136, AgentId=3CuQ28FUBABCCFLtnXBHjyQ==, AgentLocation=, AgentName=CheckPoint_FW, CategorizerCount=4, CategorizerCountCustom=0, CommandResponses Processed=15162, Commands Processed=7, Comment=, Content Version (3CuQ28FUBABCCFLtnXBHjyQ==)=2015-06-25-16-34-20_7475, Current Drop [wi2012|10.10.10.120|ArcSight|ArcSight] eventcount=3080, Device [|10.10.10.20|Check Point|Compliance Blade] eventcount=2, Device [|10.10.10.20|Check Point|GRCAp] eventcount=1, Device [|10.10.10.20|Check Point|HTTPS Inspection] eventcount=2, Device [|10.10.10.20|Check Point|Security Gateway/Management] eventcount=276, Device [|10.10.10.20|Check Point|Security Management] eventcount=1, Device [|10.10.10.20|Check Point|SmartDefense] eventcount=11, Device [|10.10.10.20|Check Point|Unknown] eventcount=168, Device [|10.10.10.20|Check Point|VPN-1] eventcount=13697, DeviceLocation=, Estimated Cache Size=0, First Command Processed=Sat Aug 06 16:39:44 EEST 2016, First CommandResponse Processed=Thu Aug 04 16:04:40 EEST 2016, First CommandResponse Processed=Thu Aug 04 16:04:49 EEST 2016, First GlobalCommandResponse Processed=Thu Aug 04 16:04:40 EEST 2016, First Post-Aggregation Event Processed=Thu Aug 04 16:04:45 EEST 2016, First Post-Aggregation Event Processed=Thu Aug 04 16:04:43 EEST 2016, Global events Processed=32947, GlobalCommandResponses Processed=15162, HostNameResolutionEnabled=false, Last Command Processed=Mon Aug 15 07:26:09 EEST 2016, Last CommandResponse Processed=Mon Aug 15 07:26:09 EEST 2016, Last Global event Processed=Mon Aug 15 07:27:03 EEST 2016, Last GlobalCommandResponse Processed=Mon Aug 15 07:27:03 EEST 2016, Last Post-Aggregation Event Processed=Mon Aug 15 07:27:03 EEST 2016, Last Post-Filtering Event Processed=Mon Aug 15 07:27:03 EEST 2016, LastModified=Mon Jun 13 08:23:24 EEST 2016, MLCacheSize=0, ModifiedBy=bredikhin, NGCustomAdditionalDataMapper0=Generic mappings:(no mappings), NGCustomAdditionalDataMapper1=Mappings for Check_Point\Compliance_Blade:(no mappings), NGCustomAdditionalDataMapper2=Mappings for Check_Point\GRCAp:(no mappings), NGCustomAdditionalDataMapper3=Mappings for Check_Point\HTTPS_Inspection:(no mappings), NGCustomAdditionalDataMapper4=Mappings for Check_Point\Security_Gateway_Management:(no mappings), NGCustomAdditionalDataMapper5=Mappings for Check_Point\Security_Management_Server:(no mappings), NGCustomAdditionalDataMapper6=Mappings for Check_Point\SmartDefense:(no mappings), NGCustomAdditionalDataMapper7=Mappings for Check_Point\Unknown:(no mappings), NGCustomAdditionalDataMapper8=Mappings for Check_Point\VPN-1:(no mappings), NameResolverIPv6Control=IPv4 Only, Post-Aggregation Event rate LTC=Mon Aug 15 07:26:09 EEST 2016, Post-Aggregation Events Processed=21829, Post-Aggregation Events Processed/Sec=0.023744285283851297, Post-Filtering Events/Sec(SLC)=0.1, Post-Filtering Event rate LTC=Mon Aug 15 07:26:09 EEST 2016, Post-Filtering Events Processed(SLC)=6, Post-Filtering Events/Sec=0.023744233628726727, Post-Filtering Events/Sec(SLC)=0.1, RawEventCount=14168, RawEventLen=7115073, Resolver.hAdded=2, Resolver.hQBlocked=0, Resolver.hQRejected=0, Resolver.hQSize=0, Resolver.hSize=2, Resolver.iAdded=4816, Resolver.iEvicted=0, Resolver.iQBlocked=0, Resolver.iQRejected=0, Resolver.iSize=4816, StatusCode=1, TC.dropcount=0, TC.size=0, URL=https://esm68.xsystems.net:8443, ZFiltered=0, aup[acp].version=2015-06-25-16-34-20_7475, aup[system-zone-mappings].version=00000000000000216037, aup[user-categorizations].version=, aup[user-zone-mappings].version=00000000000000216010, bsent=9910, detectedversion=, failedattempts=15484, failedattempts(SLC)=0, hbstatus=Up, queuesize=0, sent=17248, sent(SLC)=6, status=Up, throughput=0.018761066791414416, throughput LTC=Mon Aug 15 07:26:09 EEST 2016, throughput(SLC)=0.1}
[2016-08-15 07:27:09,844][INFO ][default.com.arcsight.agent.ki][logStatus] {C=0, ET=Up, HT=Up, N=CheckPoint_FW, S=17248, T=0.1}
[2016-08-15 07:27:09,844][INFO ][default.com.arcsight.agent.ki][logStatus] Other status:
[2016-08-15 07:27:09,844][INFO ][default.com.arcsight.agent.ki][logStatus] {Last Start Time=1470315879888, Uptime=919349}
```

# Диагностика доступности | «путь тру джедая»

```
[2016-08-15 09:48:44,486][ERROR][default.com.arcsight.agent.qd.t][isAbleToConnectToHost] Testing the thread:  
[WUC[fjCmUFYBABCADGx8ckFFTQ==][3]]. Could not connect to host [10.10.30.60]
```

```
[2016-08-15 9:49:11,261][ERROR] default.com.arcsight.agent.loadable.transport.commandresponse._  
AgentHTTPCommandResponseTransport] [onSingleEvent] com.arcsight.common.db.f:  
java.net.NoRouteToHostException: No route to host  
  at com.arcsight.agent.transport.fb.a(fb.java:638)  
  at com.arcsight.agent.transport.fb.a(fb.java:389)  
  at com.arcsight.agent.transport.fb.a(fb.java:349)  
  at com.arcsight.agent.transport.fb.a(fb.java:307)  
  at com.arcsight.agent.transport.t.onSingleEvent(t.java:101)  
  at com.arcsight.agent.transport.a.m.onSingleEvent(m.java:45)
```

# Доступность: люди против машин

данные для машин

```
[2016-08-15 9:49:11,261] [ERROR]
default.com.arcsight.agent.loadable.transport.commandresponse._
AgentHTTPCommandResponseTransport] [onSingleEvent]
com.arcsight.common.db.f: java.net.NoRouteToHostException: No
route to host
    at com.arcsight.agent.transport.fb.a(fb.java:638)
    at com.arcsight.agent.transport.fb.a(fb.java:389)
    at com.arcsight.agent.transport.fb.a(fb.java:349)
    at com.arcsight.agent.transport.fb.a(fb.java:307)
    at com.arcsight.agent.transport.t.onSingleEvent(t.java:101)
```

информация для людей

Category: Authentication  12:22:21 15.08.2016

**High** Testing the thread: [CONNECTOR]. Could not connect to host [HOST] 

Error Name: Testing the thread: [CONNECTOR]. Could not connect to host [HOST]  
Error Type: ERROR  Do Not Notify  
Error Category: Authentication  
Priority: 8  
Count: 3456  
Description: Logs are NOT collected from reported Host. The connector could not establish connection to host.  
Solution: ★★★★★ A manual diagnostic procedure needs to be performed on the server where the connector is installed. 1) Check the network connectivity to the host (ping / telnet). 2) Check whether a log source is online. 3) Check correctness of account and password. 4) Check whether the account has sufficient privileges.  
External Sources: [Protect724](#) [HP KB](#) [Submit Solution](#) [Expert Fix](#)

# Сбор данных: Актуальность

Какой процент данных поступает вовремя?

Скорость обнаружения инцидента < скорость получения данных

# Актуальность «плачет» если плохо с:

Производительностью у источников событий, сети и самой SIEM

Синхронизацией времени

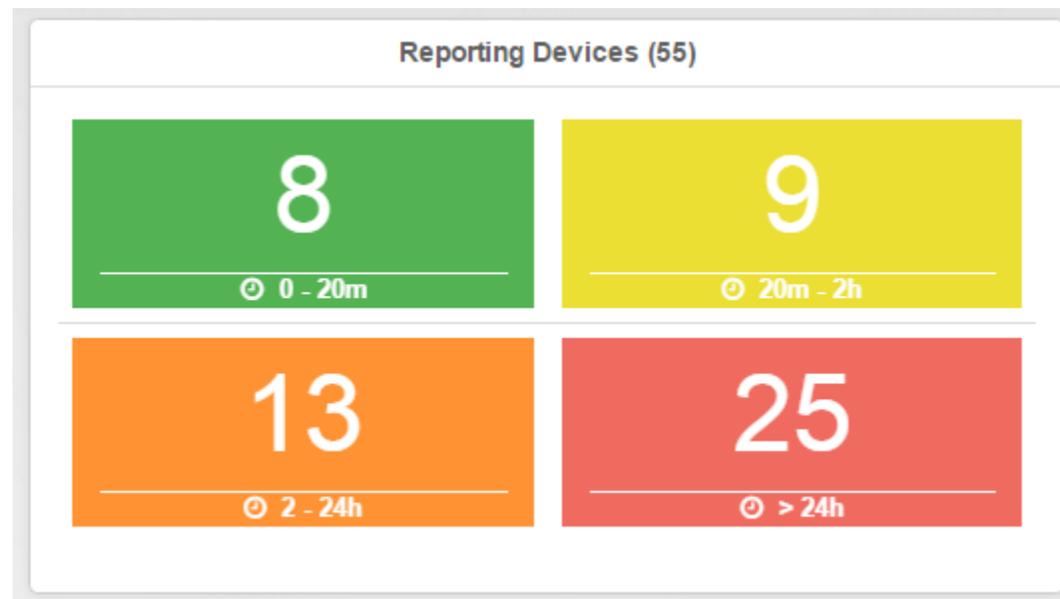
Конфигурацией SIEM

Количеством ошибок, но «плохо» у каждого своё

Всплесками данных вызывающих перегрузку компонент

# Сбор данных: актуальность

Формула: время получения менеджером - время генерации на источнике



# Сбор данных: актуальность

**SOC PRIME** PM Predictive Maintenance

Dashboard Site View Management - Live Alerts Health Check KB Search admin -

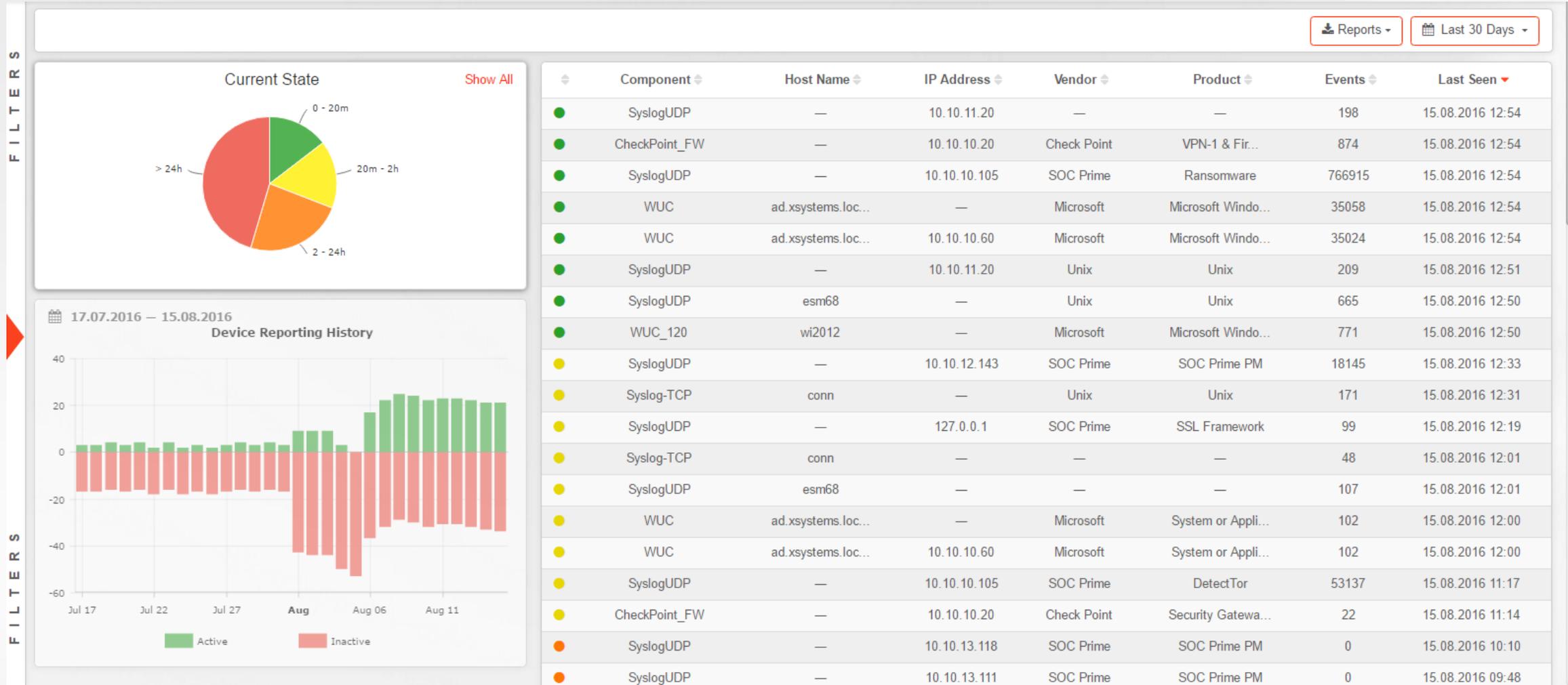
12:35 30 May 2017

### Component Info

Name: Syslog-TCP  
Host Name: srv-arcon-001 (10.10.10.102)  
Type: syslog  
Version: 7.0.7.7279.0  
Health: 76.93  
Data Acquisition: 90  
Data Quality: 79  
Performance: 100  
Security: 97  
Current EPS: 0.00  
Average EPS: 0.33 (1 GB / Day)  
Details: [Link](#)

The network diagram displays a central node labeled 'srv-arcon-001' (IP 10.10.10.102) which is highlighted in green. This central node is connected to a vast network of other nodes, including various servers (e.g., 'srv-arcon-001' through 'srv-arcon-100'), switches, and other infrastructure components. The nodes are represented by different icons (laptops, servers, switches) and are interconnected by lines representing network connections. The overall network structure is complex and dense, with many nodes having multiple connections. The diagram is presented in a zoomed-in view, with navigation controls (arrows, zoom in/out) visible at the bottom.

# Сбор данных: актуальность



# Качество данных

# Garbage In, Garbage Out



**YOUR ANALYSIS IS ONLY  
AS GOOD AS YOUR DATA**

**$f(\text{garbage}) = \text{garbage}$**

# Качество данных: целостность

Не все данные в журналах соответствует стандартам

Не все API одинаковы и стандартизированны

CEF, LEEF, SYSLOG формат «у каждого свой»

Обновление ОС / ПО / Прошивки = обновление парсера

На этапе сбора данных «успешно» проводится парсинг,  
а уже во время корреляции выявляются ошибки мапинга полей

PCI, SOX, ISO 27K = хранить данные в «формате без изменений»

# Качество данных: целостность

«Парсинг» необходимо контролировать непрерывно

Too many devices being created - possible parsing problem				ArcSight	ArcSight
//hotline.ua/img/s/v3/arr_adapt_footer_title.png - HIER_DIRECT/77.222.150.22 image/png		10.10.11.20		Unix	Unix
CMD				Unix	Unix
1471264631.024 175512 10.10.31.75 TCP_TUNNEL/200 1385 CONNECT plus.google.com:443 - HIER_DIRECT/216.58.209.206 -14...					
1471264367.096 240114 10.10.32.45 TCP_TUNNEL/200 127593 CONNECT www.google.com.ua:443 - HIER_DIRECT/216.58.209.1...					
Ransomware Update Entry		82.94.251.220		SOC Prime	Ransomware

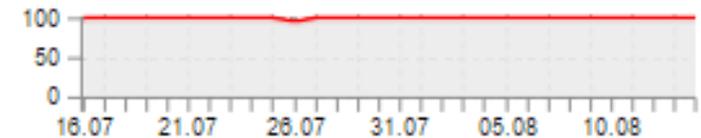
Статус по каждому устройству

Integrity ⓘ



99%

0%



# Качество данных: категоризация

Знать все коды событий

Для всех систем в вашей организации

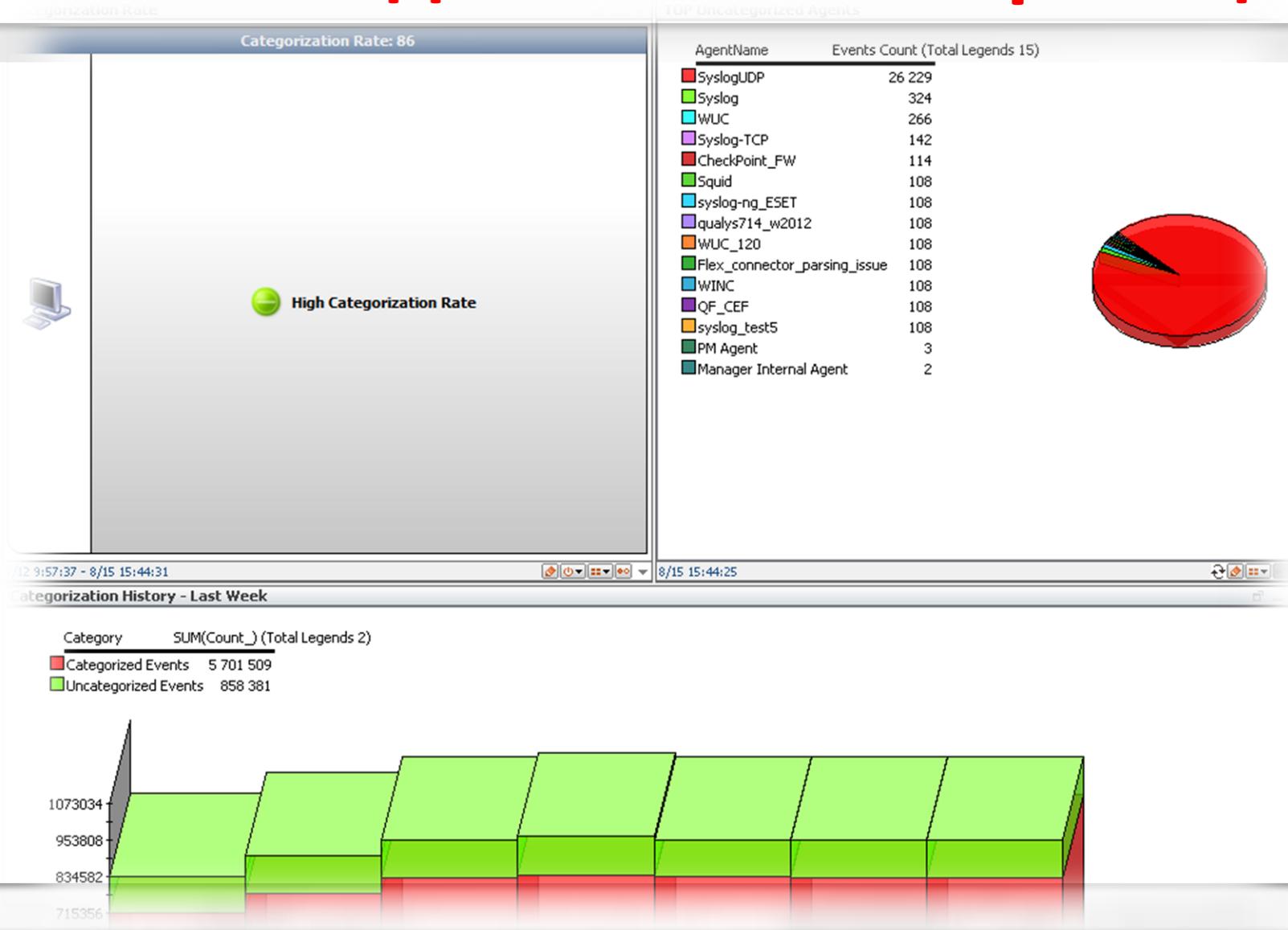
Быть в курсе всех изменений

Ежедневно следить и проводить обновление SIEM

**VS**

Довериться категоризации и универсальному контенту

# Качество данных: категоризация

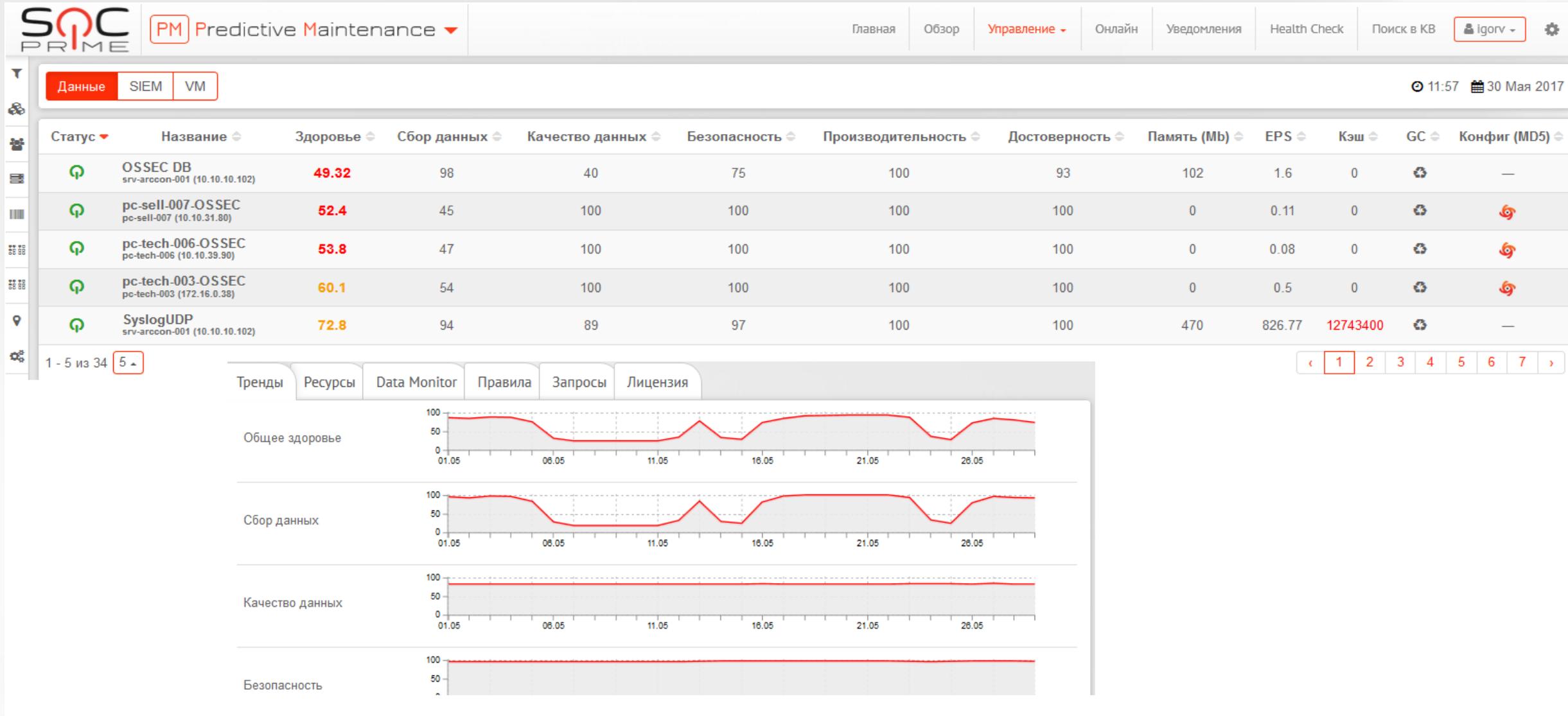


# Качество данных: инвентаризация

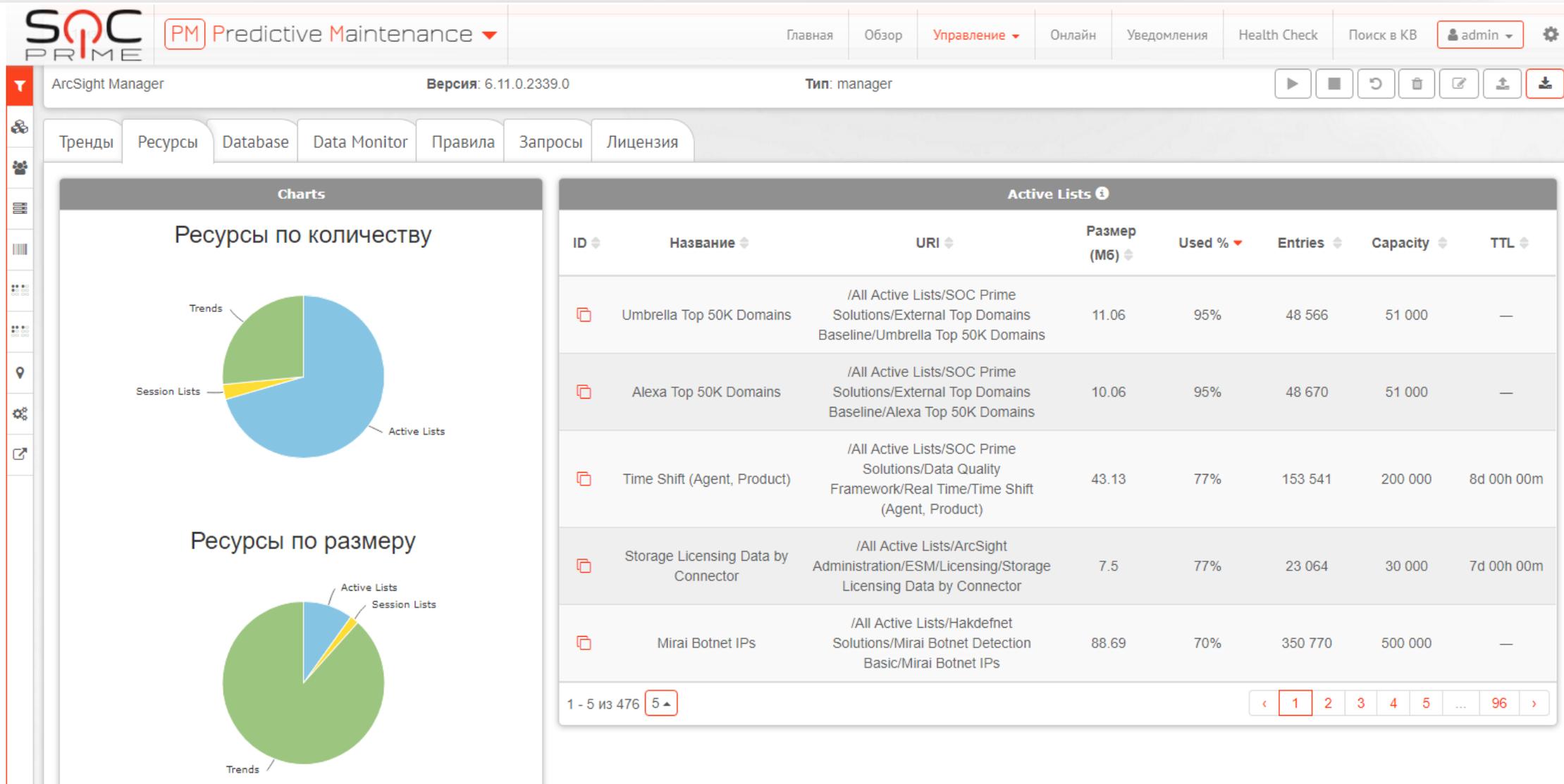
Инвентарная модель – это важно  
Инвентаризация = более точная корреляция &  
расставление приоритетов  
Необходимо создавать & обновлять на ESM уровне

Формула:  $\frac{\text{Общее кол-во IP-адресов с инвентарной моделью}}{\text{Общее кол-во IP-адресов}}$

# Производительность



# Производительность



# Безопасность

SIEM является идеальной мишенью для атаки, так как он имеет:

Хэши паролей Ваших критически важных ИТ-систем

Права доступа к ним же

Интерфейсы удаленного/дистанционного управления

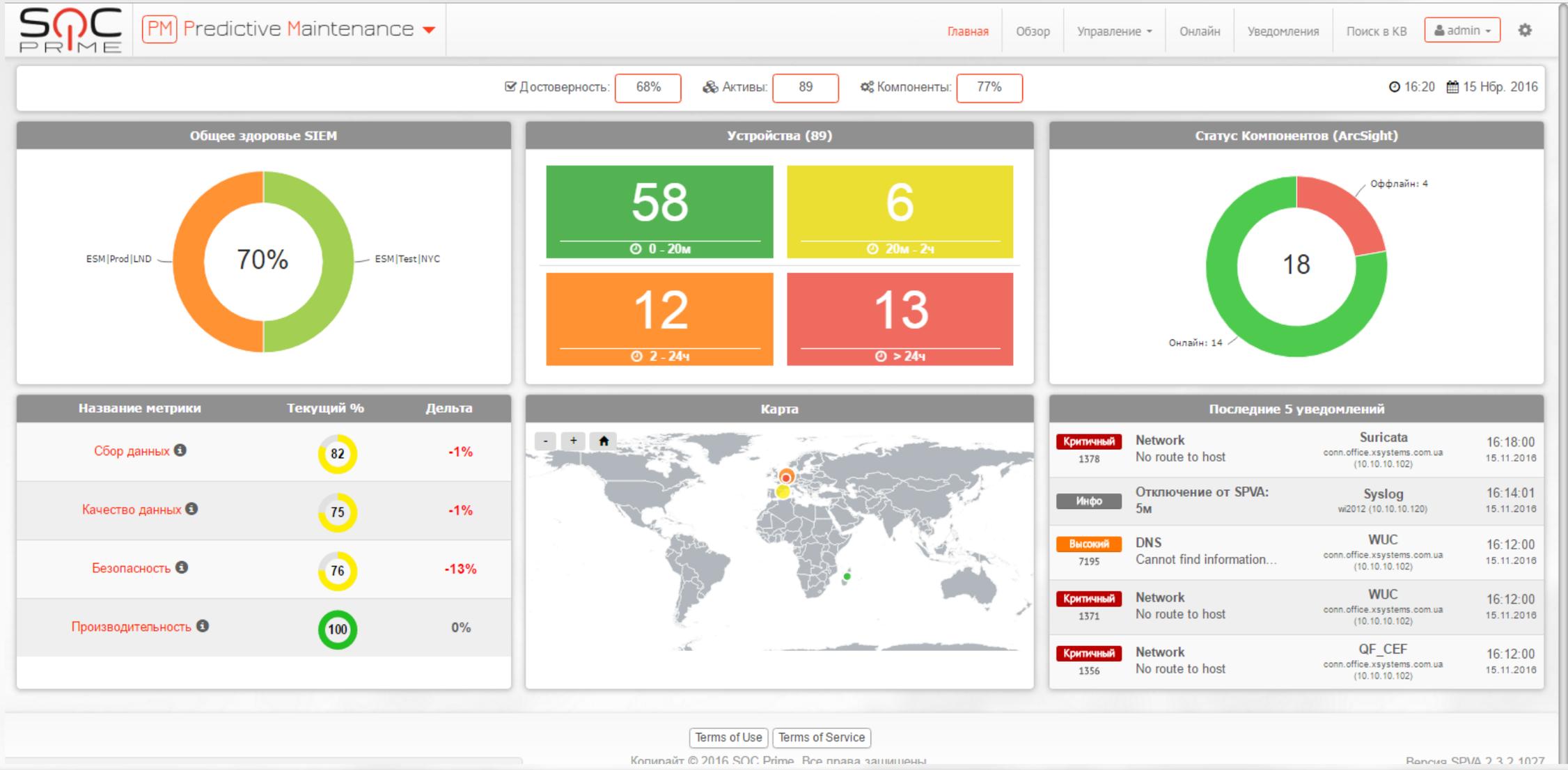
Возможность фильтрации для скрытия данных

Компоненты Endpoint Security и контроля целостности часто не устанавливаются на SIEM

# Безопасность

SOC PRIME		PM Predictive Maintenance		Dashboard Site View Management Live Alerts KB Search		admin	
Component	Type	Error Name	Category	Description	Protect724	HP KB	
Connector	WARN	Thread [NAME] interrupted possible shutdown	Security	Connector was shutdown.	Protect724	HP KB	
<b>Recommendations:</b> If the connector has not been intentionally stopped please review any other alerts on this connector. Check the memory usage and whether source event logs are dropped.							
Connector	ERROR	InterruptedException	Security	Connector operation was interrupted and logs are NOT collected. Possibly, connector has been stopped.	Protect724	HP KB	
<b>Recommendations:</b> If the connector has not been intentionally stopped please review connector's log files for critical errors. Check the memory usage and whether source event logs are dropped.							
Connector	WARN	Interrupted Possible shutdown	Security	Connector process was interrupted - Logs are NOT collected.	Protect724	HP KB	
<b>Recommendations:</b> The cause of this error is shutdown of connector process. If connector was not shutdown manually (or by schedule) check logs for other critical errors.							
Connector	WARN	Forcing disconnection	Security	Forcing disconnection with Destination. The error usually occurs when connector was stopped.	Protect724	HP KB	
<b>Recommendations:</b> If the connector has not been intentionally stopped please review other critical alerts. Check the memory usage and whether source event logs are dropped. Check the availability of Destination.							
Connector	WARN	File queue now dropping events	Security	CRITICAL - log data is lost and Connector is dropping incoming events.	Protect724	HP KB	
<b>Recommendations:</b> Connector may drop incoming events in 2 cases: 1) It does not have enough resources allocated to process incoming event stream. 2) The allocated cache is full and is being rotated. A manual diagnostics is required to determine the root cause and additional tuning may be needed such as Java Heap Size tuning, cache size changes, multithreading or change of file queue parameters. More info is provided at HP support portal at: KM1365984, KM1271053, KM1271778.							
Connector	WARN	InterruptedException	Security	Interruption of Java thread. Insertion of data into array did not happen (method Offer).	Protect724	HP KB	
<b>Recommendations:</b> A single thread was interrupted or perhaps connector as a whole is stopped. To fix the issue you have to review other errors on this connector.							
Connector	ERROR	Interrupted possible shutdown	Security	Connector operation was interrupted. Connector process was shutdown. After this message you should receive message that connector is back up again, otherwise log data won't be collected.	Protect724	HP KB	
<b>Recommendations:</b> If the connector has not been intentionally stopped please review other alerts for this connector and log files for critical errors. Check the memory usage and whether source event logs are dropped.							
Connector	WARN	Starting remote management web services	Security	An attempt is made to start remote management service of connector.	Protect724	HP KB	
<b>Recommendations:</b> This is a notification that someone has initiated a service for remote management of the connector (by default port 9001). If you do not have a Connector Appliance / ConApp or ArcMC in your environment, this means security breach or severe misconfiguration!							
Connector	FATAL	No password has been defined. Will use default	Security	Password was not defined in connector configuration and default one is used.	Protect724	HP KB	

# Собираем всё вместе



# Преимущества для бизнеса с Predictive Maintenance

Контроль качества и простое управление сервисом SOC

Снижение затрат и уверенность в соответствии GDPR, SOX, PCI DSS

Возможность прогнозировать аномалии в работе SIEM и устранять ошибки, до того как они перерастут в критичные сбои системы

# Use Case Cloud



## Use Case Library 2.0: global community cloud revolution.

500+ users, 70+ countries, 3 top SIEMs and 100+ threat-centric use cases.  
Your answer to WannaCry, NotPetya and the next APT.

Make your SIEM Smarter. Use Case Cloud.

# Cyber Incidents Insight



# Use Case Library

**SOC PRIME** UCL Use Case Library Use Case Cloud Admin Igor Voloshin

Искать в: Все Поиск... (разделитель запятой)

### Service Accounts Tracker Basic

HPE ArcSight

### Gazer Backdoor Detector

HPE ArcSight

### Sysmon Framework

HPE ArcSight

#### FEATURED VIDEO

SOC PRIME Platform Overview

#### MOST POPULAR

Use Case Name	Count
WannaCry / WannaCrypt ran...	393
Petya A / Petr-Wrap Ransom...	326
DetectTor	297
Ransomware Hunter	228
Windows Security Monitor	167

#### LATEST USE CASES

Time	Use Case Name	SIEM
16:57 08.09.2017	Service Accounts Tracker	HPE ArcSight
16:50 08.09.2017	Gazer Backdoor Detector	HPE ArcSight
16:45 08.09.2017	Sysmon Framework	HPE ArcSight
16:14 04.09.2017	Clear text communications discovery	HPE ArcSight

#### USE CASES (104)

Название	Тип	SIEM	Статус	Released	Дата обновления	Действие	Структура кейса
Activity Monitoring of User Group v 1.0.0 36 / 0 / 0 / 5	Basic	IBM QRadar	Under R&D		28.04.2017	Голосовать	
APT Framework v 1.0.0 157 / 33 / 0	Basic	HPE ArcSight	Available	13.01.2017	13.04.2017	Бесплатный	
APT Framework v 1.0.0							

Need help?

# Use Case Library

**SOC PRIME** UCL Use Case Library Use Case Cloud Igor Voloshin

**APT Framework - Advanced** v1.0.0

APC Prime HPE ARCSIGHT

APT Framework - это специализированный аналитический модуль который можно моментально развернуть на наиболее распространенных в мире SIEM-системах, таких как HPE ArcSight, IBM QRadar и Splunk. Он позволяет постоянно вести наблюдение за инфраструктурой компании и обнаруживать признаки APT на различных стадиях проведения атаки с применением методологии Lockheed Martin Cyber Kill Chain. Модуль использует методы статистического профилирования и поведенческого анализа, позволяет максимально эффективно использовать существующие в компании технологии, такие как IDS/IPS, FW, Proxy, Antivirus, Vulnerability Scanners.

Contents	Additional Info
Фильтры: 11	Дата обновления: 04 Мая 2017
Rules: 21	Case version: 1.0.0
Dashboards: 2	Compatibility: HPE ArcSight 6.9.1.2195.0
Queries: 7	Size: 35.17 KB
Query Viewers: 7	SHA-256 hash: Show
Trends: 0	
Reports: 0	
Active Lists: 8	
Active Channels: 1	
Integration Scripts: 0	
Categorizer: 0	
Additional Parsers: 0	
Attacker Tactics: 11	
Attacker Techniques: 55	

MITRE Attack™  
SOC Workflow  
Зависимости и рекомендации  
Log Source Health Check Requirements  
Список изменений

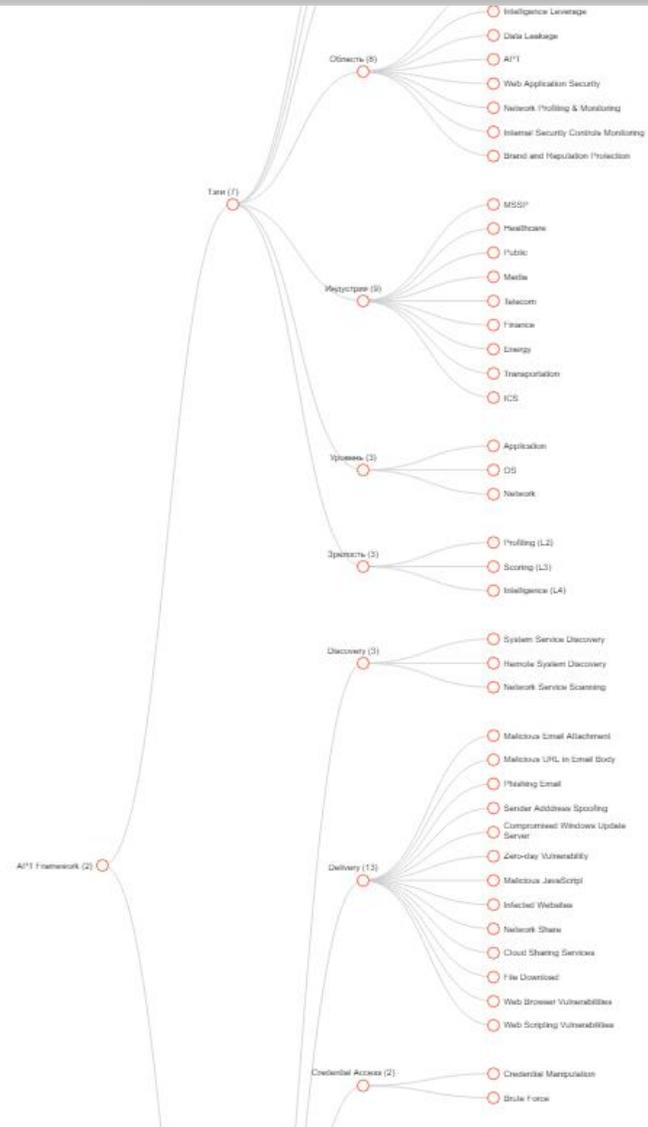
Куплен Скачать Документация Поддержка Добавить Отзыв

Structure

Need help?

Online

# Use Case Library



### MITRE Attack™ - APT Framework - Basic

<b>Recon</b> 3 Techniques	<b>Deliver</b> 13 Techniques	<b>Creds</b> 2 Techniques	<b>Escalate</b> 3 Techniques	<b>Evade</b> 7 Techniques
<b>Persist</b> 4 Techniques	<b>C&amp;C</b> 14 Techniques	<b>Lateral</b> 7 Techniques	<b>Execute</b> 3 Techniques	<b>Collect</b> 1 Techniques
<b>Extract</b> 6 Techniques				

#### Privilege Escalation

Privilege escalation is the result of actions that allow an adversary to obtain a higher level of permissions on a system or network. Certain tools or actions require a higher level of privilege to work and are likely necessary at many points throughout an operation. Adversaries can enter a system with unprivileged access and must take advantage of a system weakness to obtain local administrator or SYSTEM privileges. A user account with administrator-like access can also be used. User accounts with permissions to access specific systems or perform specific functions necessary for adversaries to achieve their objective may also be considered an escalation of privilege.

**Tactic includes 3 techniques:**

- New Service

When operating systems boot up, they can start programs or applications called services that perform background system functions. A service's configuration information, including the file path to the service's executable, is stored in the Windows Registry. Adversaries may install a new service that can be configured to execute at startup by using utilities to interact with services or by directly modifying the Registry. The service name may be disguised by using a name from a related operating system or benign software with Masquerading. Services may be created with administrator privileges but are executed under SYSTEM privileges, so an adversary may also use a service to escalate privileges from administrator to SYSTEM. Adversaries may also directly start services through Service Execution.

Detection	Examples	<b>Mitigations</b>
-----------	----------	--------------------

Limit privileges of user accounts and remediate Privilege Escalation vectors so only authorized administrators can create new services. Identify and block unnecessary system utilities or potentially malicious software that may be used to create services by using whitelisting tools, like AppLocker, or Software Restriction Policies where appropriate.

- ✔ Legitimate Credentials
- ✔ Web Shell

# Health Check

**SOC PRIME** **HC Health Check** **S. M. A. Cloud** **ArcSight Health Check** **Igor Voloshin**

Последние 7 дней 12:21 30 Мая 2017

Название	Time	Пользователь	Health	Действие
Demo Log Data <small>logs.zip</small>	01.01.1971 12:00:00	demo	73	

1 - 1 of 1

### Basic Information

Тип: nt\_local Start Date: 16:32:14 20.02.2015  
Version: 7.0.7.7279.0 End Date: 17:11:48 26.03.2015  
Event Count: 13666 Error Count: 16677  
Cache: 0 AVG EPS: 0.03  
AVG Memory: 48 Mb  
Confidence: 99 Все: 16677 Known: 16588 Security: 55  
Data Quality: 65 Parsed: 8889 Unparsed: 4777 Performance: 100

### Errors

by Type: ERROR, WARN  
by Category: Security, Configuration, Network Events Flow, Parsing, DNS, General

Trends Errors Devices (4)

Диапазон Тип Category Priority Sort by: Last Seen Очистить фильтр Reports

### Errors on Demo Log Data

**High** Category: DNS **▲** 17:11:23 26.03.2015  
17:45:22 16.03.2015  
Cannot find information for [HOST]

Error Name: Cannot find information for [HOST]  
Error Type: WARN  
Error Category: DNS  
Priority: 8  
Count: 4781  
Описание: Ошибка возникает если SmartConnector получил сообщение в поле которого содержится Source (Destination) Address / Source (Destination) Host Name и не смог выполнить resolve данного поля.  
Solution: Необходимо выполнить следующие действия с сервера где установлен коннектор: 1) Проверить доступность DNS сервера (ping / telnet). 2) Выполнить DNS запрос вручную (nslookup). 3) Проверить наличие необходимых записей на DNS сервере в случае необходимости добавить. 4) При отсутствии необходимости можно отключить резолвинг на коннекторе.  
Diagnostics: Raw Logs Protect724 HP KB Submit Solution

**Low** Category: General **▲** 17:10:42 26.03.2015  
16:32:56 20.02.2015  
Number of bad threat level values received and corrected

# Преимущества для бизнеса с Use Case Library

Передовые технологии для вашей команды по борьбе с киберугрозами

Онлайн доступ к глобальной экспертизе в отрасли кибербезопасности

Сделайте вашу SIEM умнее, выявляйте и расследуйте инциденты быстрее

# CyberView SOC мониторинг

## Эффективность мониторинга

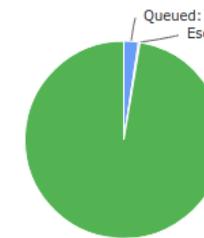


Вчера Неделя Месяц

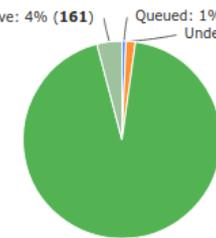
Обзор Тренда

## Инциденты по статусу

### Текущий



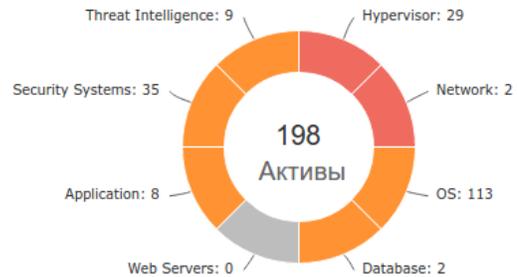
### Предыдущий



Вчера Неделя Месяц

Обзор Тренда

## Статус источников данных



Текущий +7 Дней +14 Дней +1 Месяц +6 Месяцев +1 Год

Обзор Тренда

## Эффективность Use Case

Use Case	Правила	Уведомления	EI	E3P	Подтвержденные	Ложные	No Root
DNS Security Check Basic	1	2	0	0	2	0	0
VPN Security Monitor	4	181	0	0	172	0	0
Password Security Basic	1	30	0	0	30	0	0
DetectTor Advanced	1	1	0	0	1	0	0
Brute Force Detection Advanced	3	75	0	0	75	0	0

1 - 5 из 10

1 2

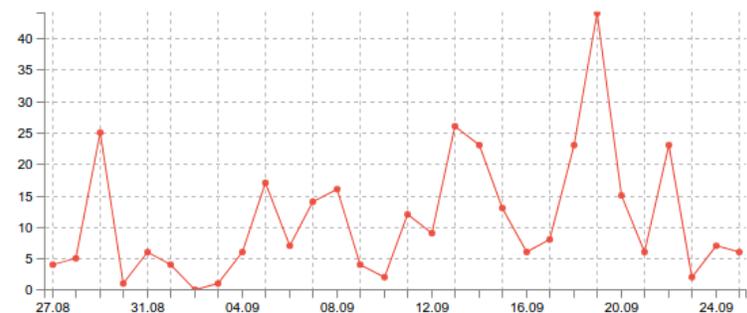
Вчера Неделя Месяц Все

# CyberView SOC мониторинг



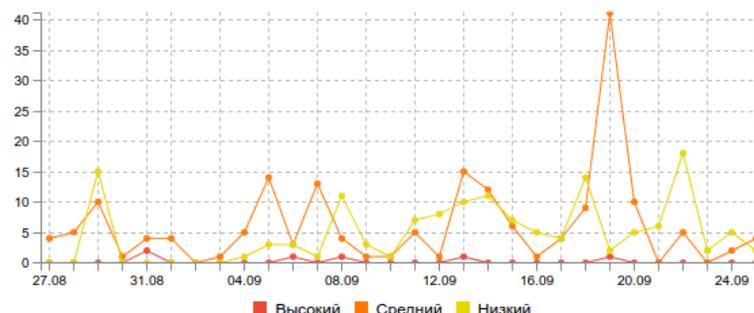
# CyberView SOC мониторинг

Инциденты



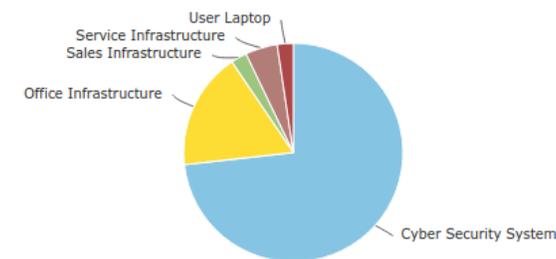
🕒 | День | Неделя | Месяц Вид →

Инциденты по приоритету



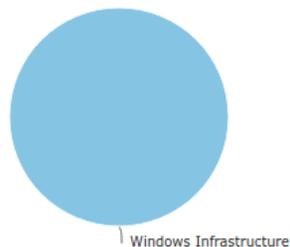
🕒 | День | Неделя | Месяц Вид →

Инциденты по категории актива



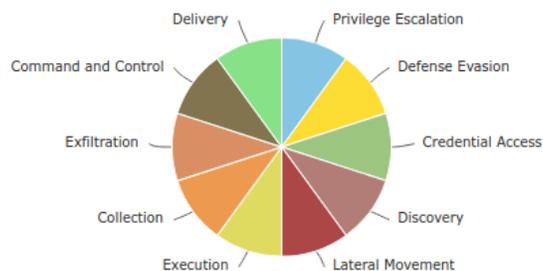
🕒 | День | Неделя | Месяц Вид →

Инциденты по технологии



🕒 | День | Неделя | Месяц Вид →

Инциденты по тактике



🕒 | День | Неделя | Месяц Вид →

ТОП 5 инцидентов по владельцу актива

Владелец	Подразделение	Количество
Oleksandr Bredikhin	R&D	96
Eugeniy Samborskiy	DevOps	28
Oleksandr Verbnyak	R&D	3

🕒 | День | Неделя | Месяц Вид →

# Преимущества для бизнеса с CyberView

Постоянное методичное улучшение эффективности и зрелости SOC

Проактивное управление рисками и быстрое принятие решений

Качественные и простые отчеты и метрики для диалога на одном языке для всех сторон вовлеченных в безопасность компании

# SOC Prime: сохранит время для более важных дел!



**Берегите себя!**

[sales@socprime.com](mailto:sales@socprime.com)