SOC PRIME
SECURITY QUALITY CONTROL

# 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



Подкаст «Методологии внедрения SIEM» https://risspa.podster.fm/23

# 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

motiv

ISSP
Information Systems Security Partners

## Финансы

BNP PARIBAS

SBERBANK
PUBLIC JOINT STOCK COMPANY

Raiffeisen BANK

otpbank

EUROBANK

## Телеком

Kcell™

ВОЛЯ

## Лого конфиденциально

Государственный сектор

Агропромышленный сектор

Медиа сектор

Легкая промышленность

Forbes Global 2000



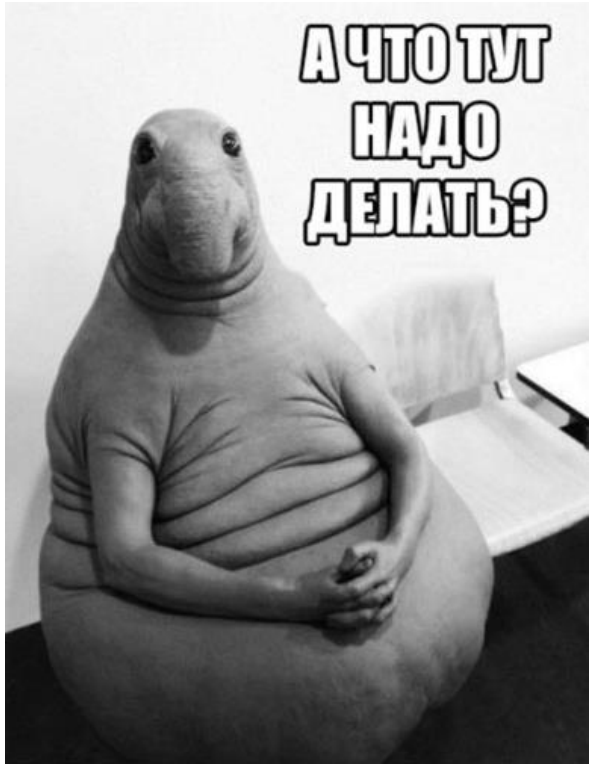
SOC PRIME
POWER ON SECURITY

# Ну всё … купили

## Из коробки

## Ожидание

## Реальность

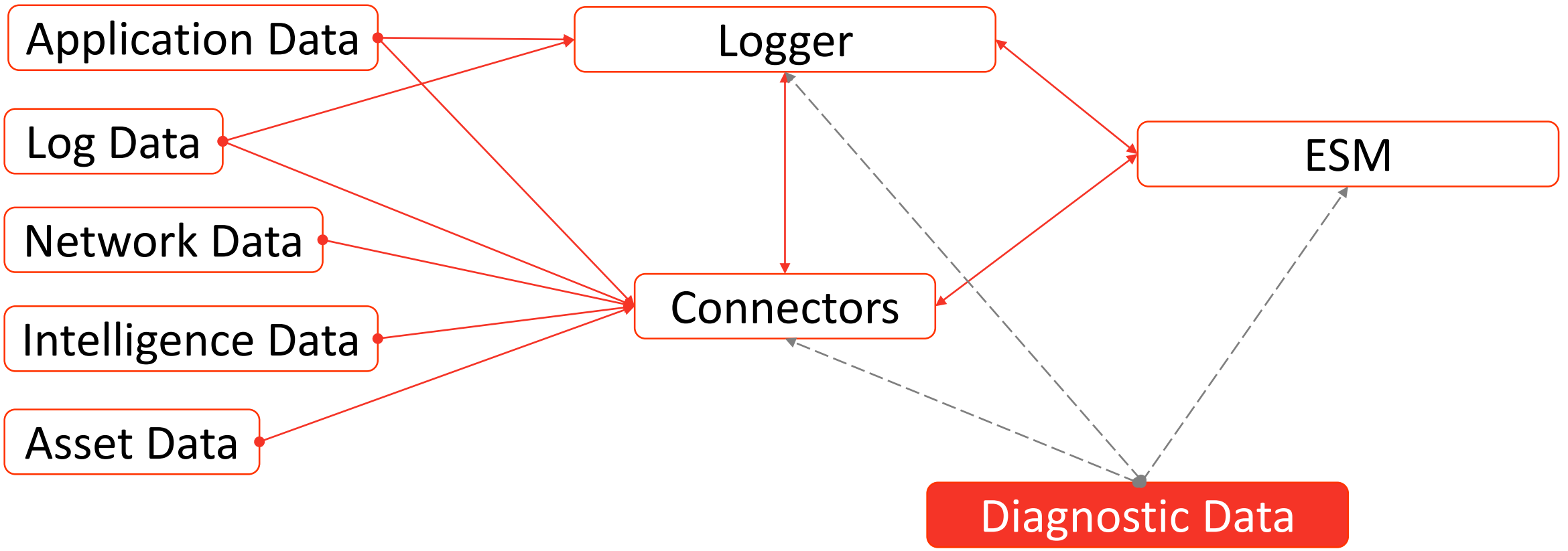




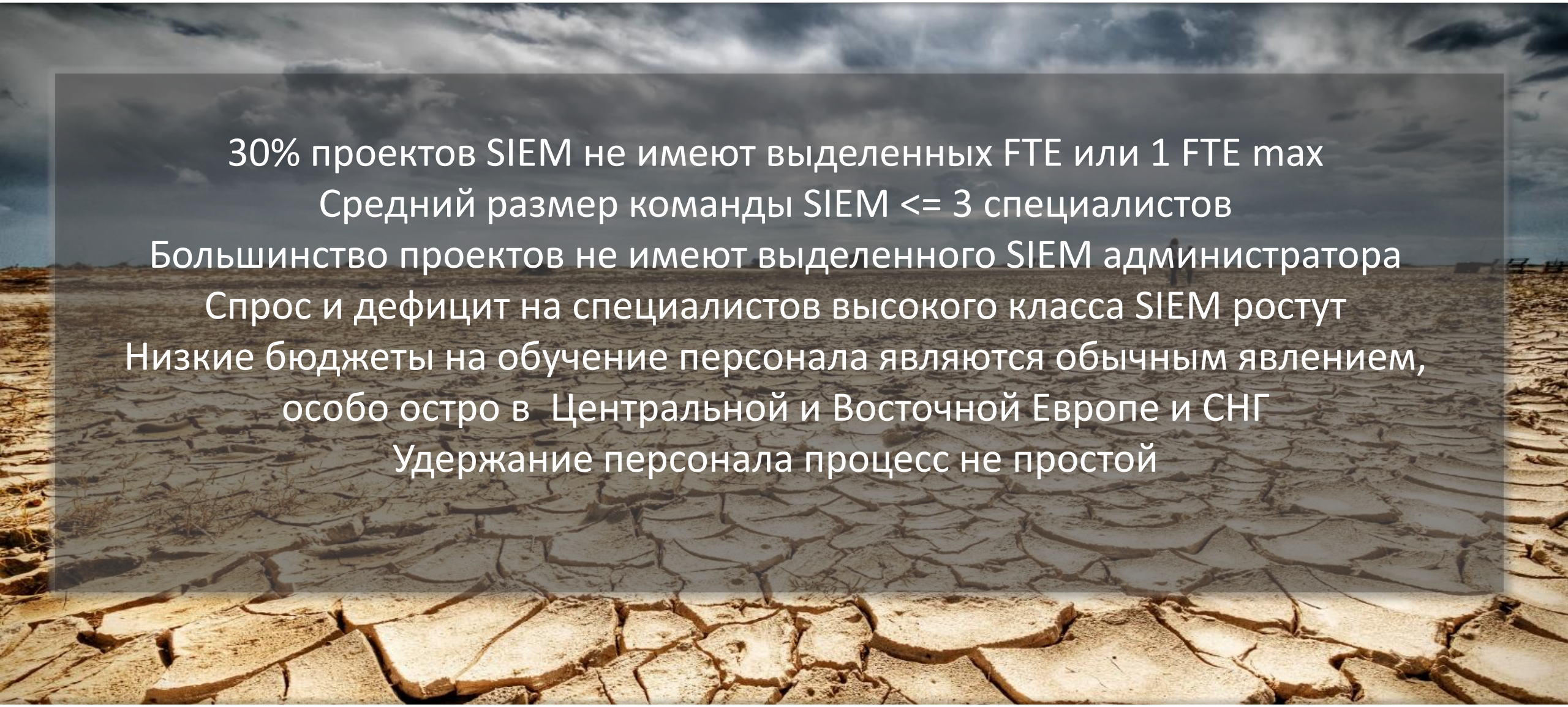

SOC PRIME
POWER ON SECURITY

# ОСТОРОЖНО: дальше примеры на ArcSight

# Данные для SOC на примере ArcSight



# Тренды: SIEM =//= SOC

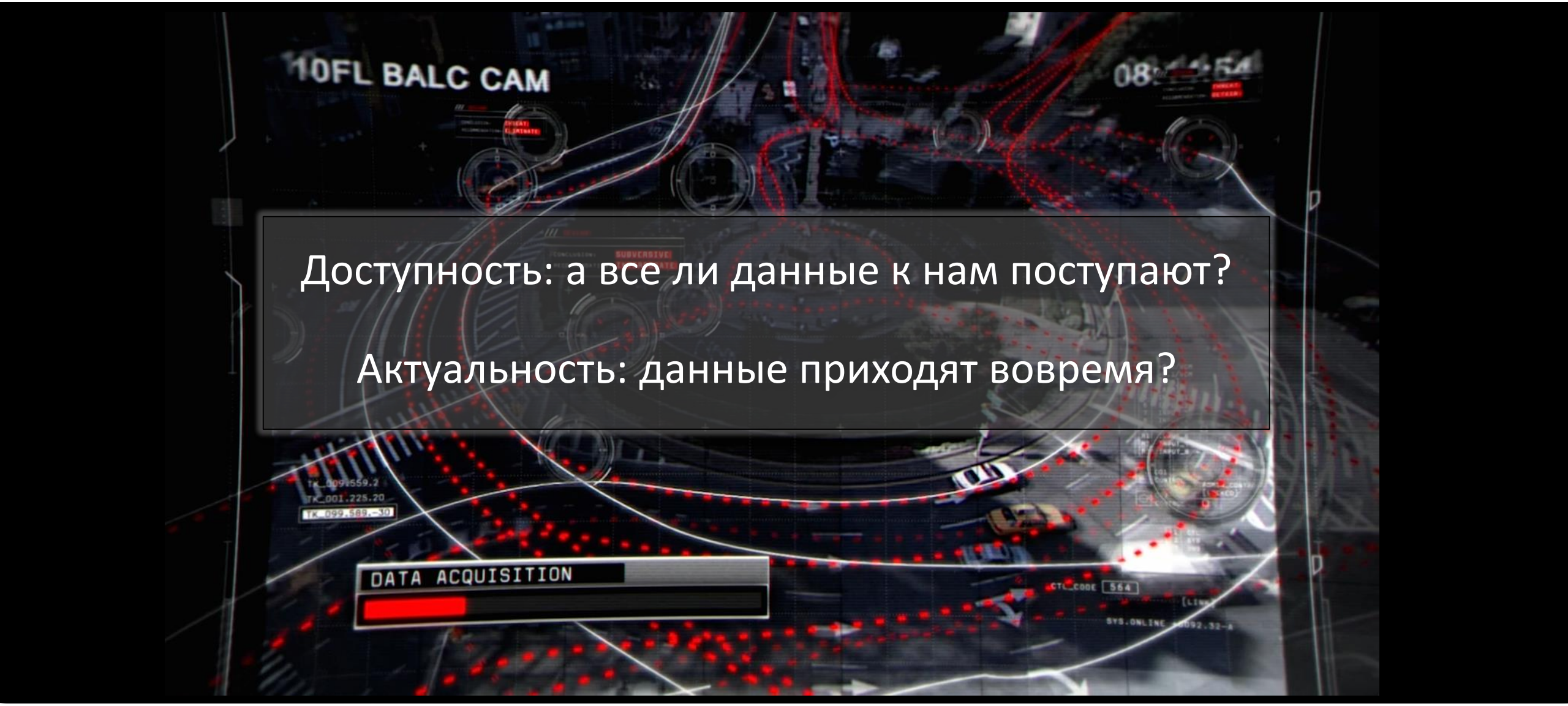


30% проектов SIEM не имеют выделенных FTE или 1 FTE max
Средний размер команды SIEM <= 3 специалистов
Большинство проектов не имеют выделенного SIEM администратора
Спрос и дефицит на специалистов высокого класса SIEM ростут
Низкие бюджеты на обучение персонала являются обычным явлением, особо остро в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



SOC PRIME
POWER ON SECURITY

# Сбор данных




Доступность: а все ли данные к нам поступают?

Актуальность: данные приходят вовремя?



SOC PRIME
POWER ON SECURITY

# 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

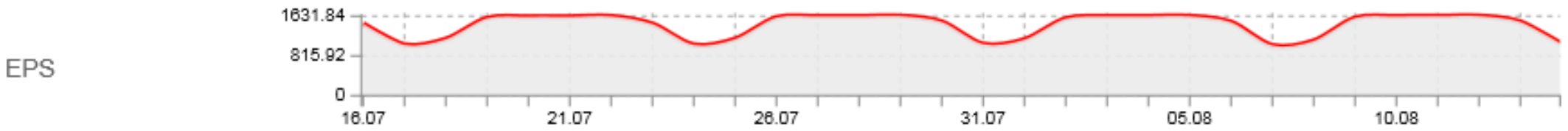
- Источник журналов
- «Коннектор»
- «Logger и ESM»

# 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 | | |
| 15 Aug 2016 09:16:45 BST | 15 Aug 2016 09:16:38 BST | Windows Domain Brute Force Logon | System Monitored | ArcSight | | |
| 15 Aug 2016 09:16:41 BST | 15 Aug 2016 09:16:36 BST | Windows Domain Brute Force Logon | System Monitored | ArcSight | | |
| 15 Aug 2016 09:16:39 BST | 15 Aug 2016 09:16:31 BST | Computer Account Changed | System Monitored | ArcSight | | |
| 15 Aug 2016 09:16:39 BST | 15 Aug 2016 09:16:31 BST | Computer Account Changed | System Monitored | ArcSight | | |
| 15 Aug 2016 09:16:35 BST | 15 Aug 2016 09:16:08 BST | Computer Account Changed | System Monitored | ArcSight | | |
| 15 Aug 2016 09:16:34 BST | 15 Aug 2016 09:16:27 BST | Windows Domain Brute Force Logon | System Monitored | ArcSight | | |
| 15 Aug 2016 09:16:22 BST | 15 Aug 2016 09:16:18 BST | Windows Domain Brute Force Logon | System Monitored | ArcSight | | |
| 15 Aug 2016 09:16:18 BST | 15 Aug 2016 09:16:12 BST | Windows Brute Force Logon | System Monitored | ArcSight | | |
| 15 Aug 2016 09:16:17 BST | 15 Aug 2016 09:16:01 BST | Computer Account Changed | System Monitored | ArcSight | | |

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



*Full list for 'Health Check' @ https://www.protect724.hpe.com/docs/DOC-11167*

# 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, AddrBasedUsrZonePopCusts=1, AddrBas
AddrBasedUsrZonePopRows=3, AddrBasedZonePopEvents=0, AddrBasedZonePopRows=136, AgentId=3CuQ2SFUBABCCFLtnXBHjyQ==, AgentLocation=, AgentName=CheckPoint_FW, CategorizerCount=4
CategorizerCountCustom=0, CommandResponses Processed=15162, Commands Processed=7, Comment=, Content Version (3CuQ2SFUBABCCFLtnXBHjyQ==)=2015-06-25-16-34-20_7475, Current Dro
[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|GRCApp] eventcount
[|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|Secu
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 20
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
Event Processed=Thu Aug 04 16:04:43 EEST 2016, Global events Processed=32947, GlobalCommandResponses Processed=15162, HostNameResolutionEnabled=false, Last Command Processed
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 1
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
M1CacheSize=0, ModifiedBy=bredikhin, NGCustomAdditionalDataMapper0=Generic mappings:(no mappings), NGCustomAdditionalDataMapper1=Mappings for Check_Point\Compliance_Blade:(n
NGCustomAdditionalDataMapper2=Mappings for Check_Point\GRCApp:(no mappings), NGCustomAdditionalDataMapper3=Mappings for Check_Point\HTTPS_Inspection:(no mappings), NGCustomA
for Check_Point\Security_Gateway_Management:(no mappings), NGCustomAdditionalDataMapper5=Mappings for Check_Point\Security_Management_Server:(no mappings), NGCustomAdditiona
Check_Point\SmartDefense:(no mappings), NGCustomAdditionalDataMapper7=Mappings for Check_Point\Unknown:(no mappings), NGCustomAdditionalDataMapper8=Mappings for Check_Point\
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
Post-Aggregation Events/Sec=0.023744285283851297, Post-Aggregation Events/Sec(SLC)=0.1, Post-Filtering Event rate LTC=Mon Aug 15 07:26:09 EEST 2016, Post-Filtering Events Pr
Events Processed(SLC)=6, Post-Filtering Events/Sec=0.023744233628726727, Post-Filtering Events/Sec(SLC)=0.1, RawEventCount=14168, RawEventLen=7115073, Resolver.hAdded=2, Res
Resolver.hQBlocked=0, Resolver.hQRejected=0, Resolver.hQSize=0, Resolver.hSize=2, Resolver.iAdded=4816, Resolver.iEvicted=0, Resolver.iQBlocked=0, Resolver.iQRejected=0, Res
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 07:26:0
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

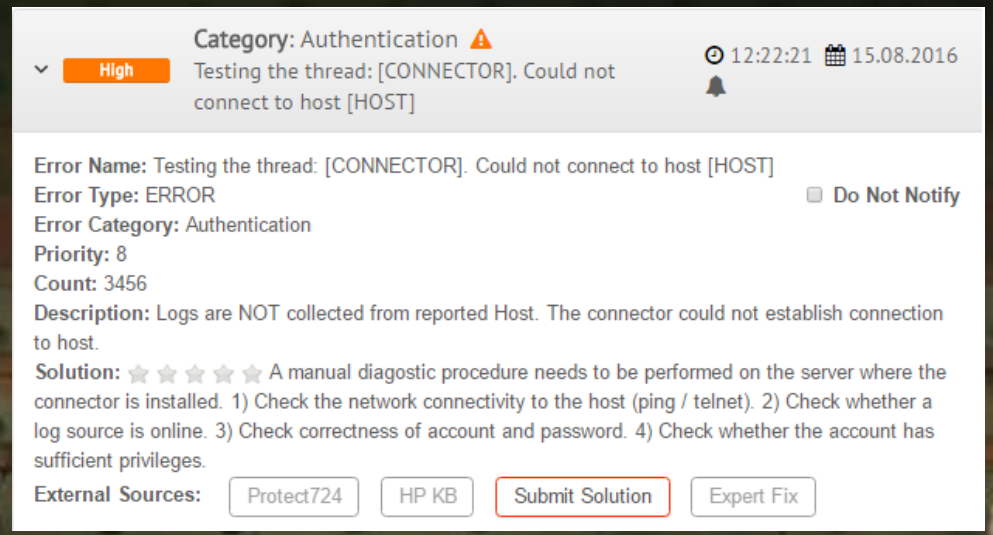
```
    at com.arcsight.agent.transport.fb.a(fb.java:638)
    at com.arcsight.agent.transport.fb.a(fb.java:389)
    at com.arcsight.agent.transport.fb.a(fb.java:349)
    at com.arcsight.agent.transport.fb.a(fb.java:307)
    at com.arcsight.agent.transport.t.onSingleEvent(t.java:101)
    at com.arcsight.agent.transport.a.m.onSingleEvent(m.java:45)
```

# Доступность: люди против машин

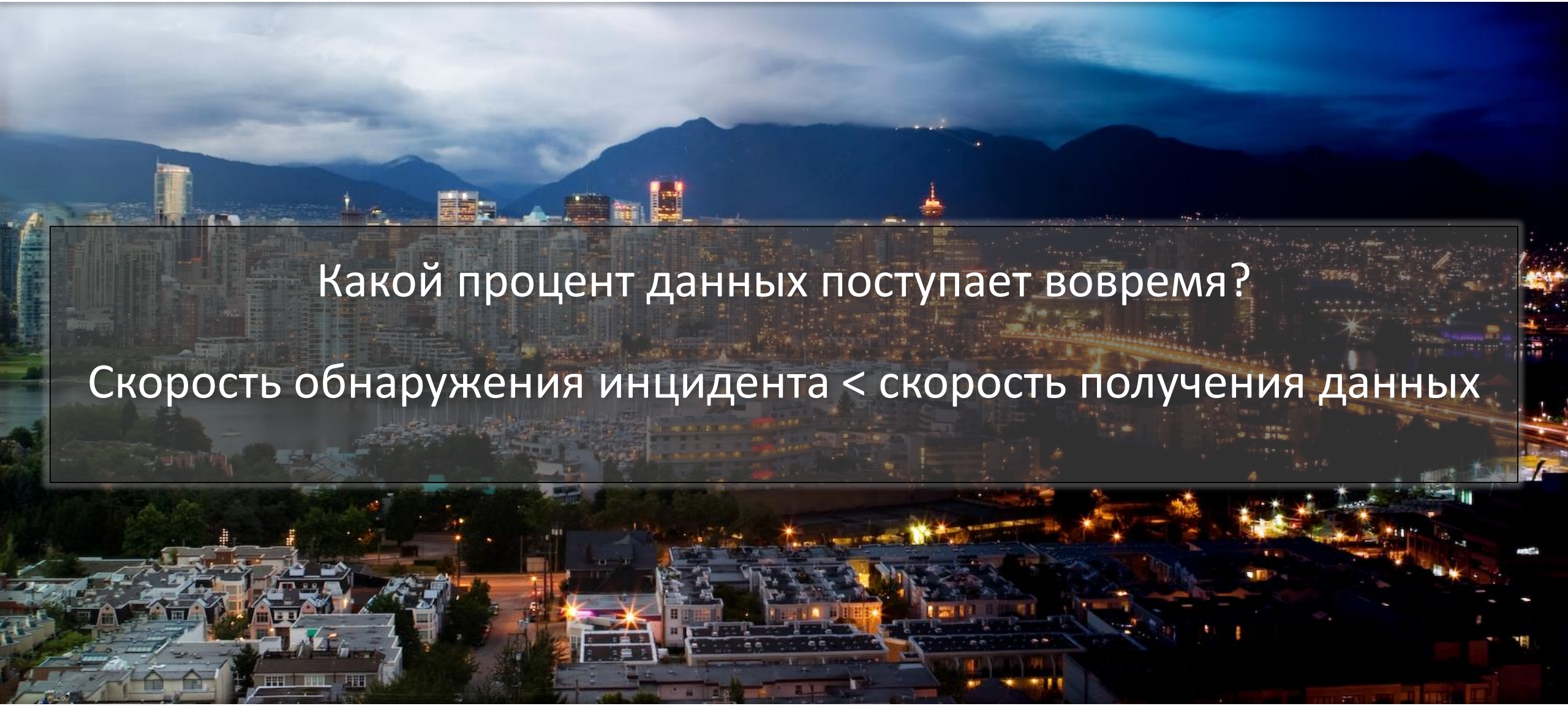
данные для машин

инфомация для людей

```
[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)
```



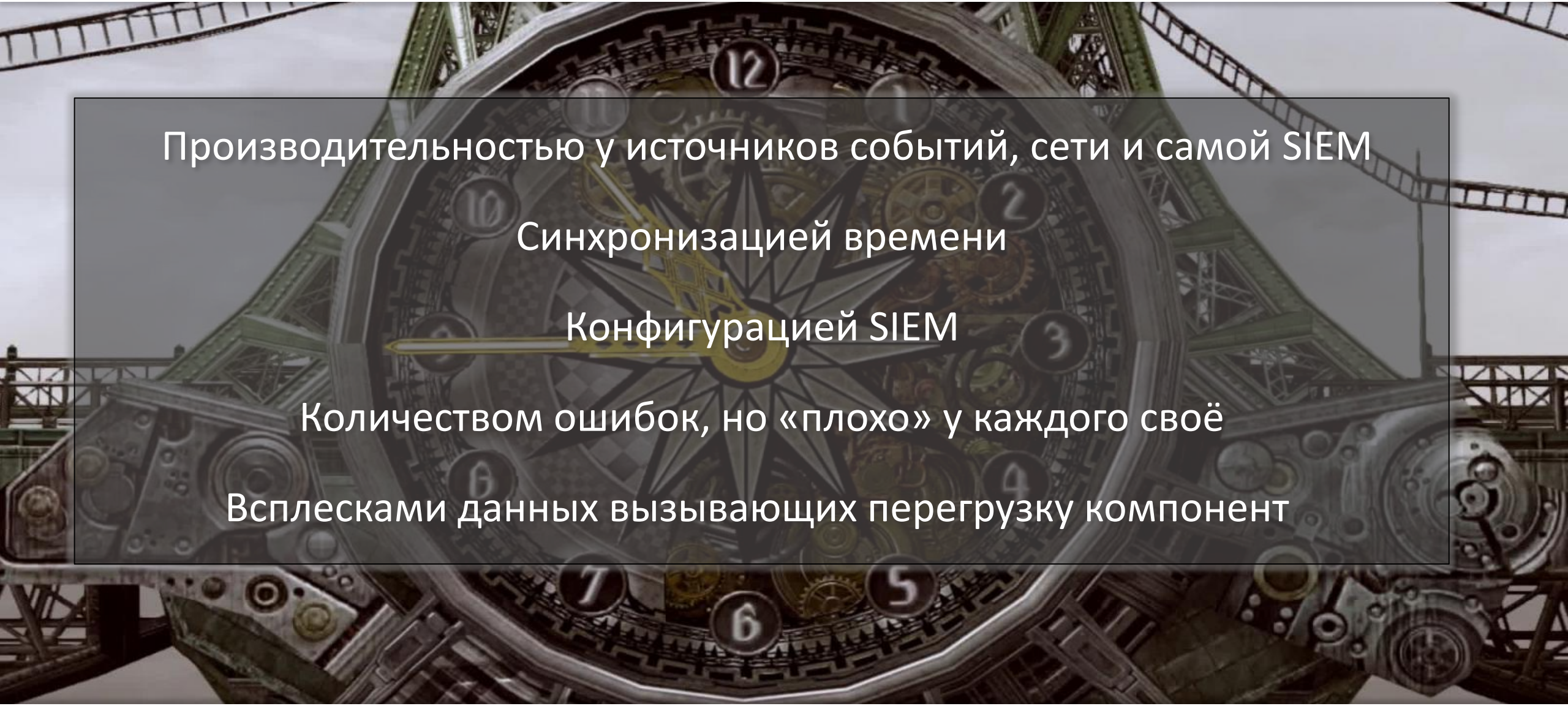
# Сбор данных: Актуальность



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

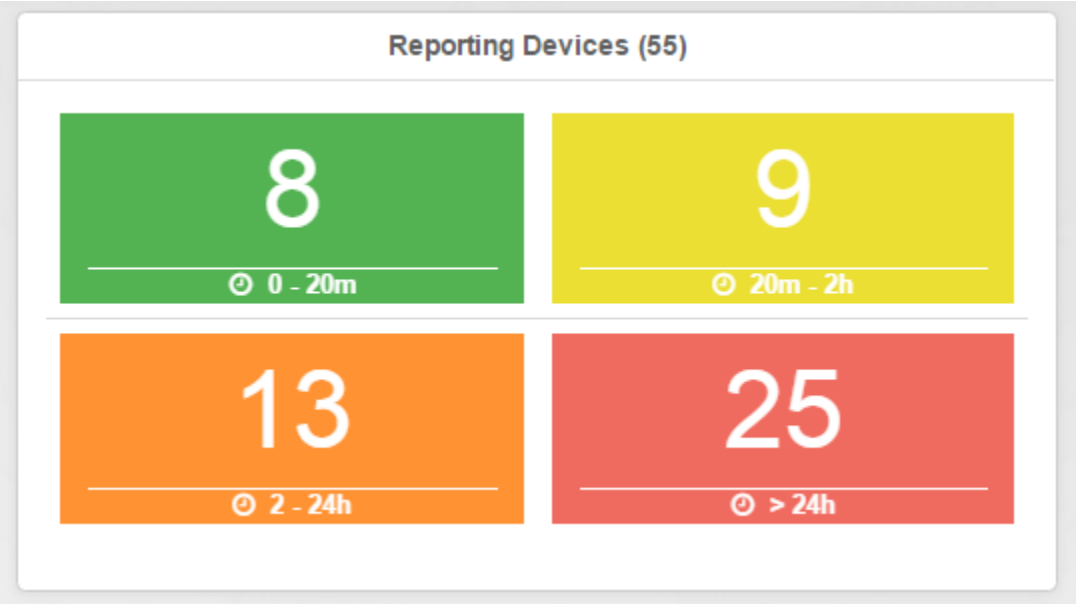
Конфигурацией SIEM

Количеством ошибок, но «плохо» у каждого своё

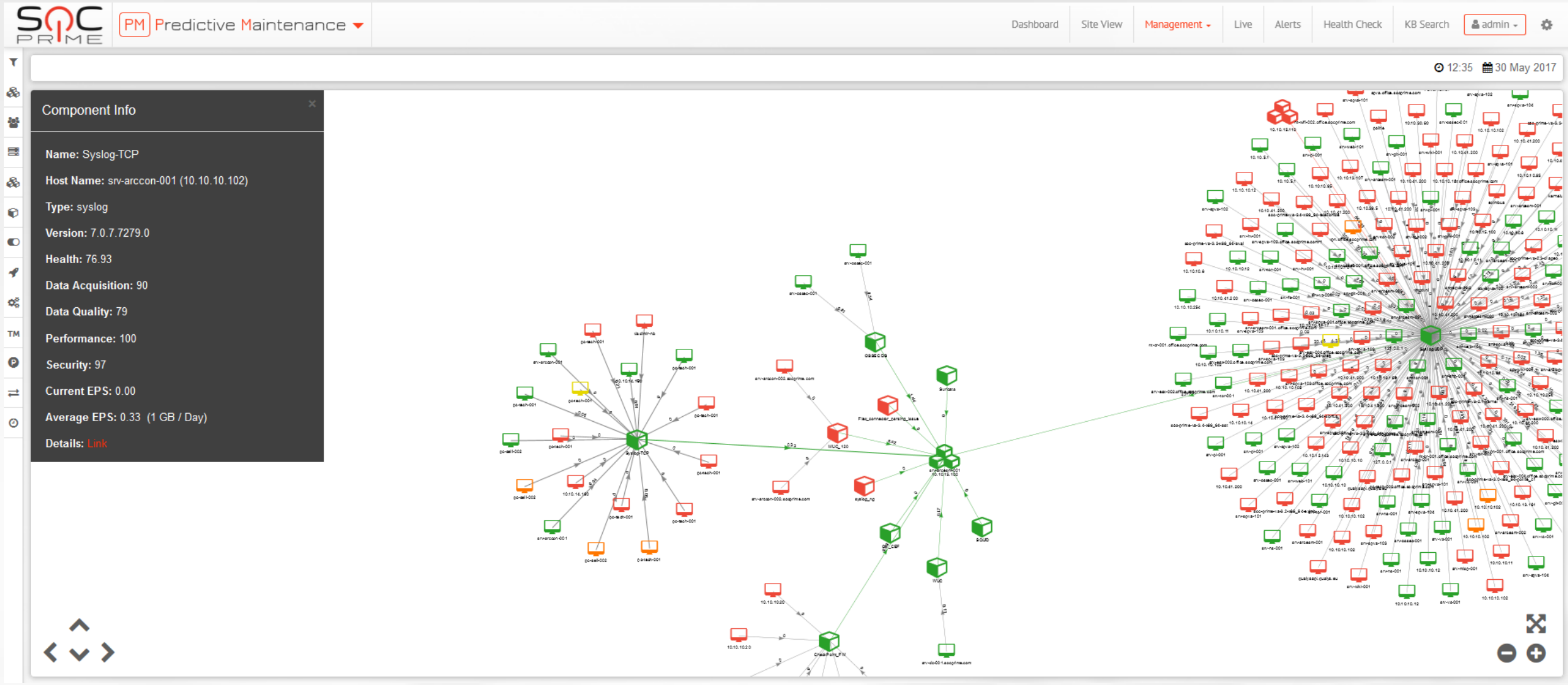
Всплесками данных вызывающих перегрузку компонент

# Сбор данных: актуальность

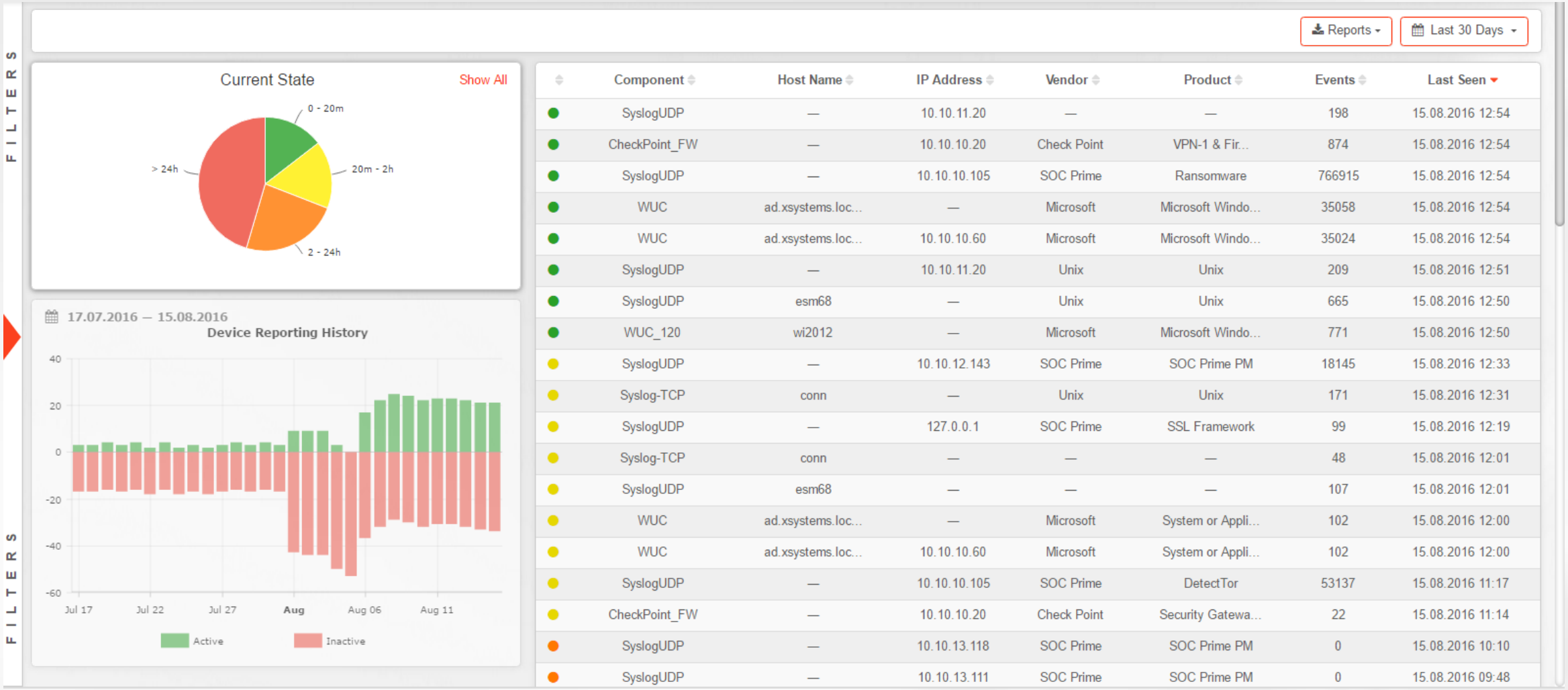
Формула: время получения менеджером - время генерации на источнике



# Сбор данных: актуальность

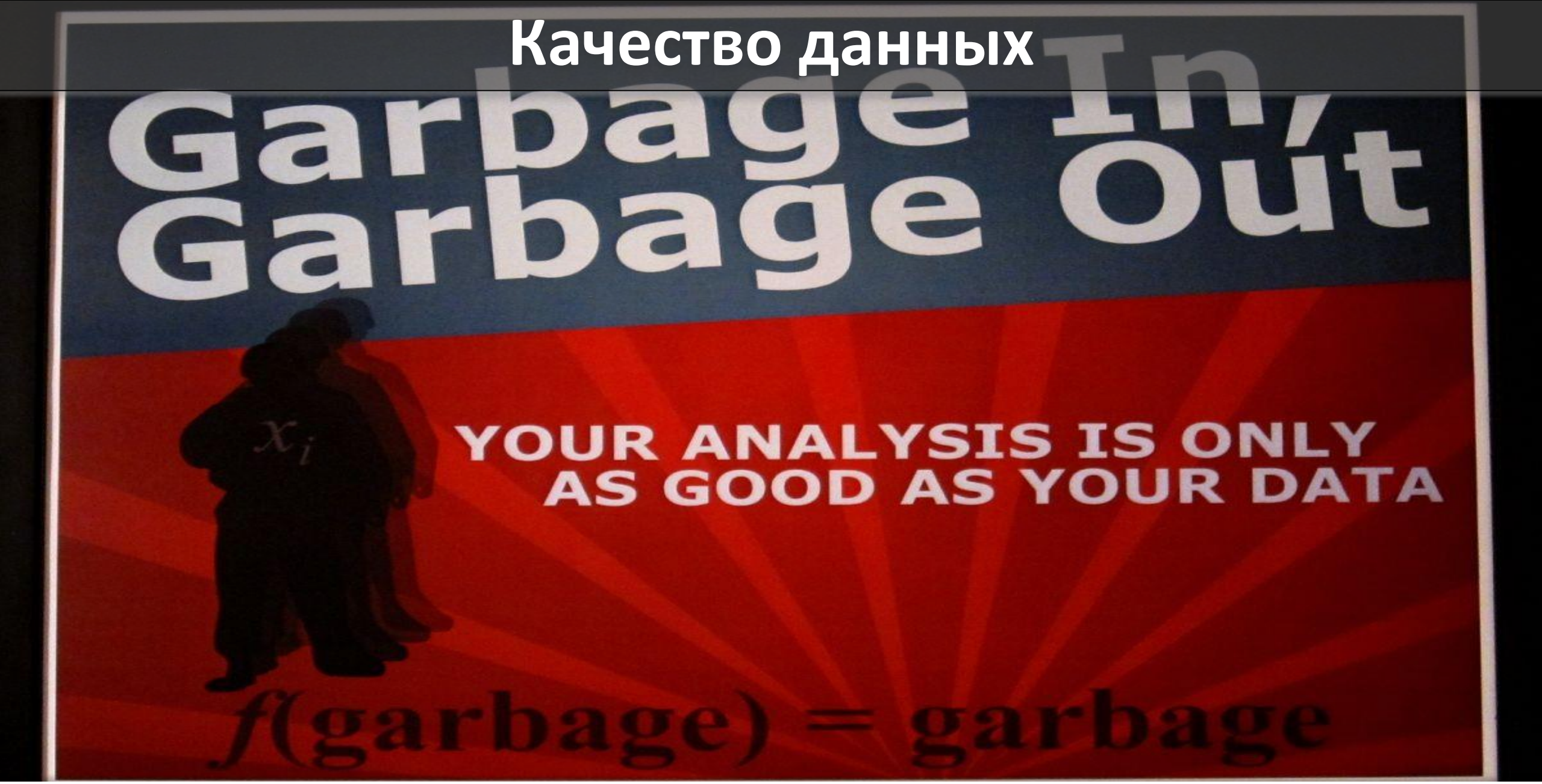


# Сбор данных: актуальность




| Component | Host Name | IP Address | Vendor | Product | Events | Last Seen |
|---|---|---|---|---|---|---|
| SyslogUDP | — | 10.10.11.20 | — | — | 198 | 15.08.2016 12:54 |
| CheckPoint_FW | — | 10.10.10.20 | Check Point | VPN-1 & Fir... | 874 | 15.08.2016 12:54 |
| SyslogUDP | — | 10.10.10.105 | SOC Prime | Ransomware | 766915 | 15.08.2016 12:54 |
| WUC | ad.xsystems.loc... | — | Microsoft | Microsoft Windo... | 35058 | 15.08.2016 12:54 |
| WUC | ad.xsystems.loc... | 10.10.10.60 | Microsoft | Microsoft Windo... | 35024 | 15.08.2016 12:54 |
| SyslogUDP | — | 10.10.11.20 | Unix | Unix | 209 | 15.08.2016 12:51 |
| SyslogUDP | esm68 | — | Unix | Unix | 665 | 15.08.2016 12:50 |
| WUC_120 | wi2012 | — | Microsoft | Microsoft Windo... | 771 | 15.08.2016 12:50 |
| SyslogUDP | — | 10.10.12.143 | SOC Prime | SOC Prime PM | 18145 | 15.08.2016 12:33 |
| Syslog-TCP | conn | — | Unix | Unix | 171 | 15.08.2016 12:31 |
| SyslogUDP | — | 127.0.0.1 | SOC Prime | SSL Framework | 99 | 15.08.2016 12:19 |
| Syslog-TCP | conn | — | — | — | 48 | 15.08.2016 12:01 |
| SyslogUDP | esm68 | — | — | — | 107 | 15.08.2016 12:01 |
| WUC | ad.xsystems.loc... | — | Microsoft | System or Appli... | 102 | 15.08.2016 12:00 |
| WUC | ad.xsystems.loc... | 10.10.10.60 | Microsoft | System or Appli... | 102 | 15.08.2016 12:00 |
| SyslogUDP | — | 10.10.10.105 | SOC Prime | DetectTor | 53137 | 15.08.2016 11:17 |
| CheckPoint_FW | — | 10.10.10.20 | Check Point | Security Gatewa... | 22 | 15.08.2016 11:14 |
| SyslogUDP | — | 10.10.13.118 | SOC Prime | SOC Prime PM | 0 | 15.08.2016 10:10 |
| SyslogUDP | — | 10.10.13.111 | SOC Prime | SOC Prime PM | 0 | 15.08.2016 09:48 |

# Качество данных






SOC PRIME
POWER ON SECURITY

# 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

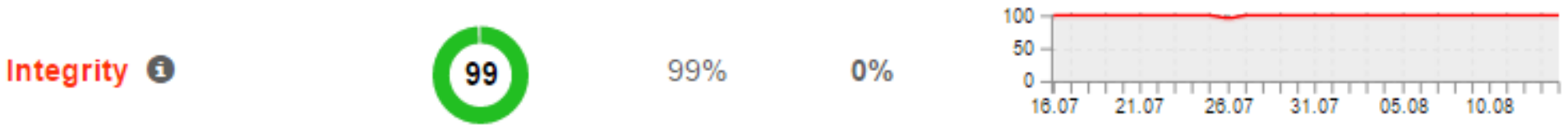
PCI, SOX, ISO 27K = хранить данные в «формате без изменений»

# Качество данных: целостность

«Парсинг» необходимо контролировать непрерывно

| | | | | | |
|---|---|---|---|---|---|
| Too many devices being created - possible parsing problem | | | 8 | ArcSight | ArcSight |
| //hotline.ua/img/s/v3/arr_adapt_footer_title.png - HIER_DIRECT/77.222.150.22 image/png | | 10.10.11.20 | 7 | Unix | Unix |
| CMD | | | 3 | 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... | | | 2 | | |
| 1471264367.096 240114 10.10.32.45 TCP_TUNNEL/200 127593 CONNECT www.google.com.ua:443 - HIER_DIRECT/216.58.209.1... | | | 2 | | |
| Ransomware Update Entry | | 82.94.251.220 | 3 | SOC Prime | Ransomware |

Статус по каждому устройству



# Качество данных: категоризация

Знать все коды событий

Для всех систем в вашей организации

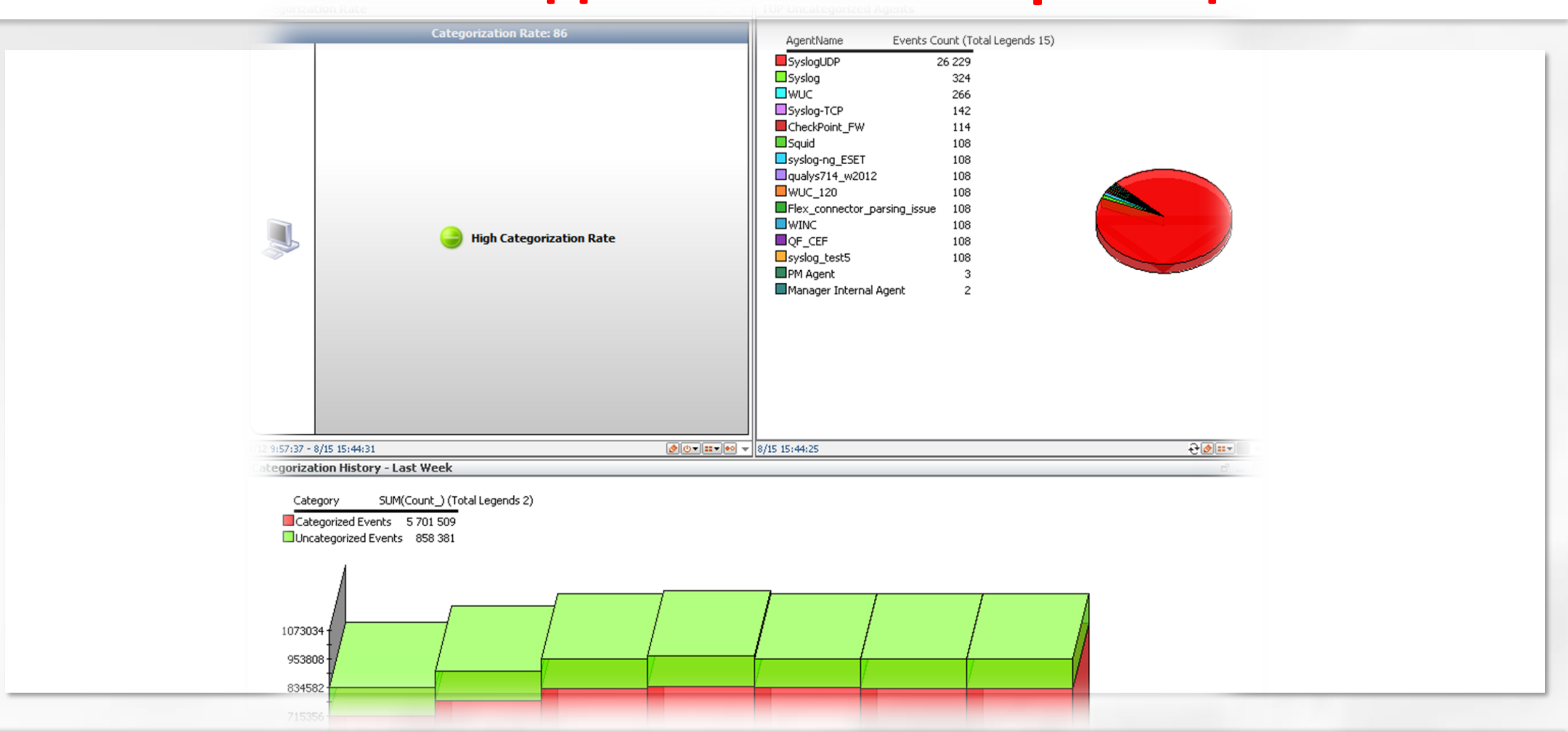
Быть в курсе всех изменений

Ежедневно следить и проводить обновление SIEM

**VS**

Довериться категоризации и универсальному контенту

# Качество данных: категоризация



# Качество данных: инвентаризация

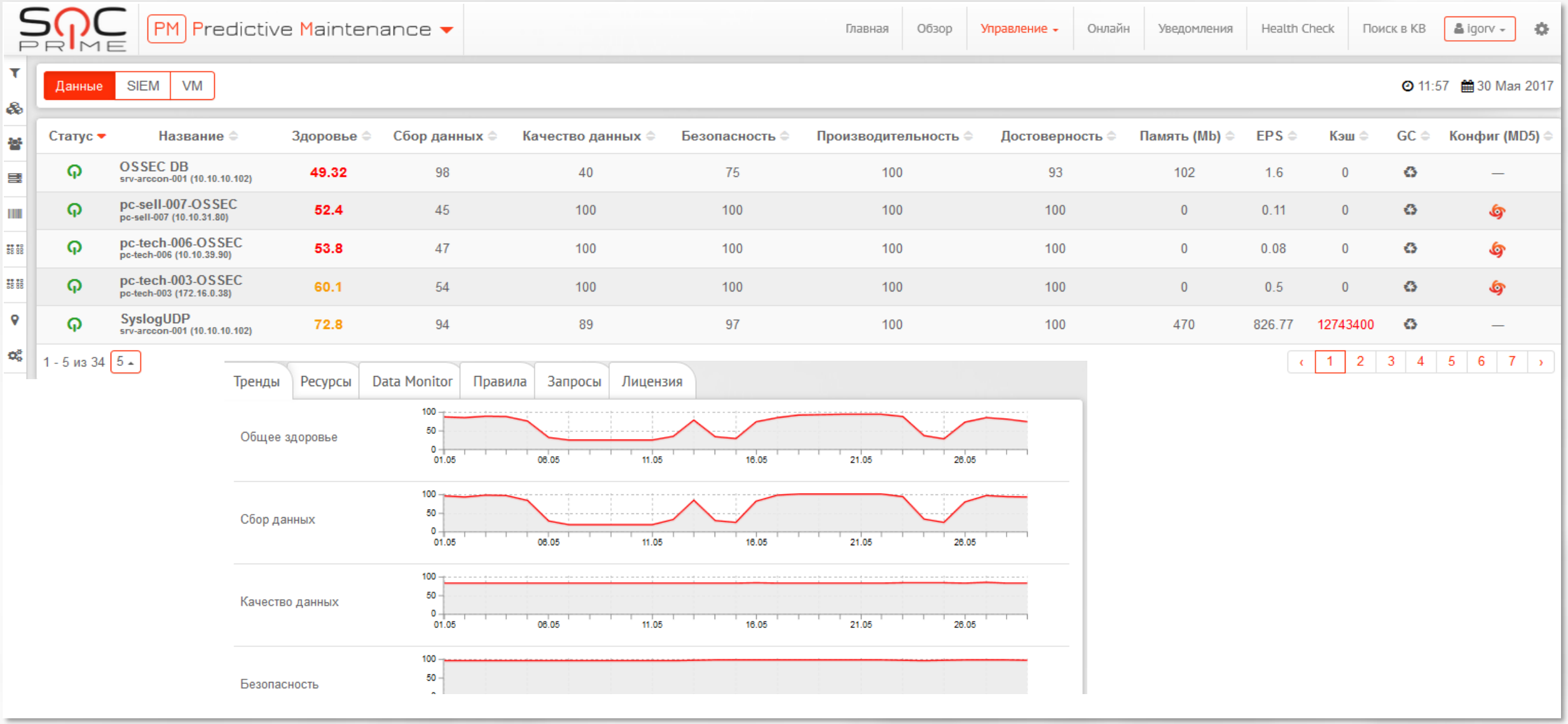
Инвентарная модель – это важно

Инвентаризация = более точная корреляция & расставление приоритетов

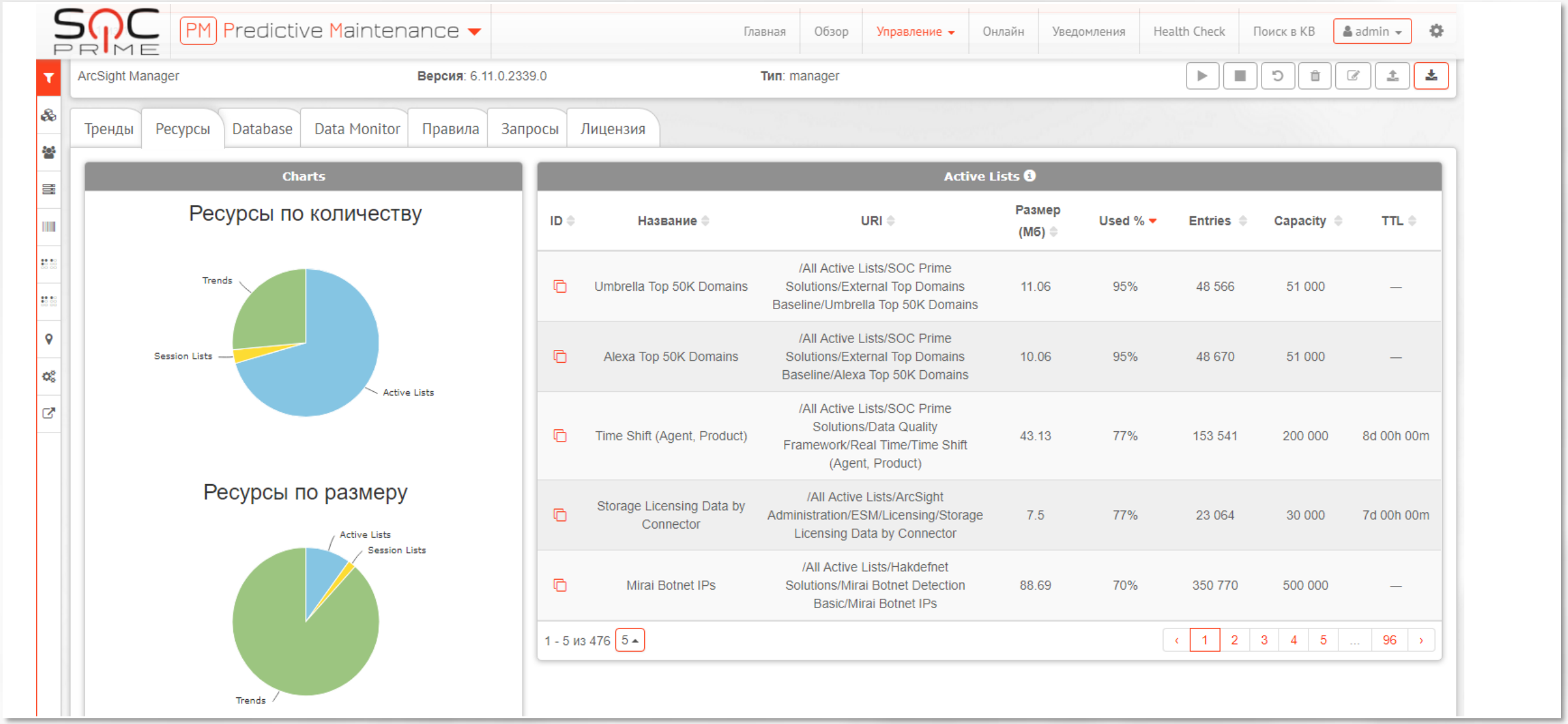
Необходимо создавать & обновлять на ESM уровне

Формула: Общее кол-во IP-адресов с инвентарной моделью / Общее кол-во IP-адресов

# Производительность



# Производительность



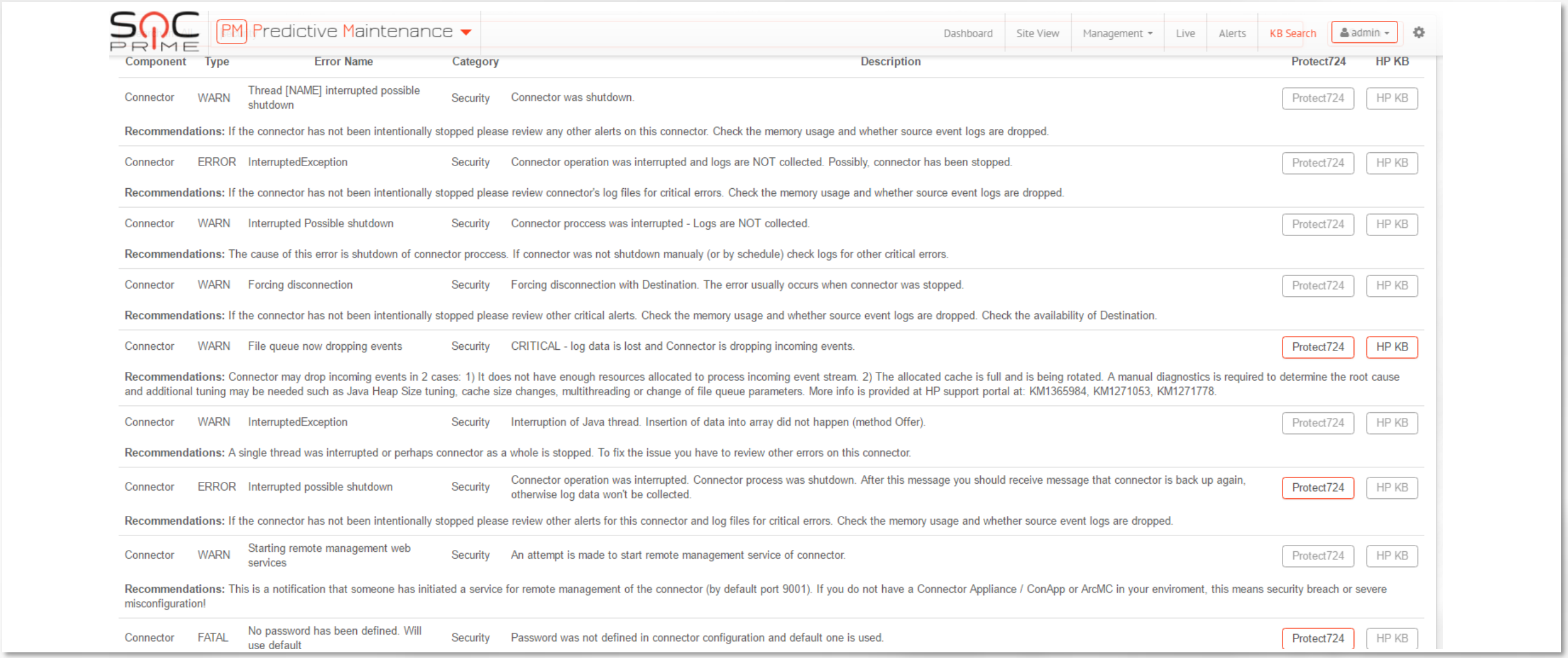
# Безопасность

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

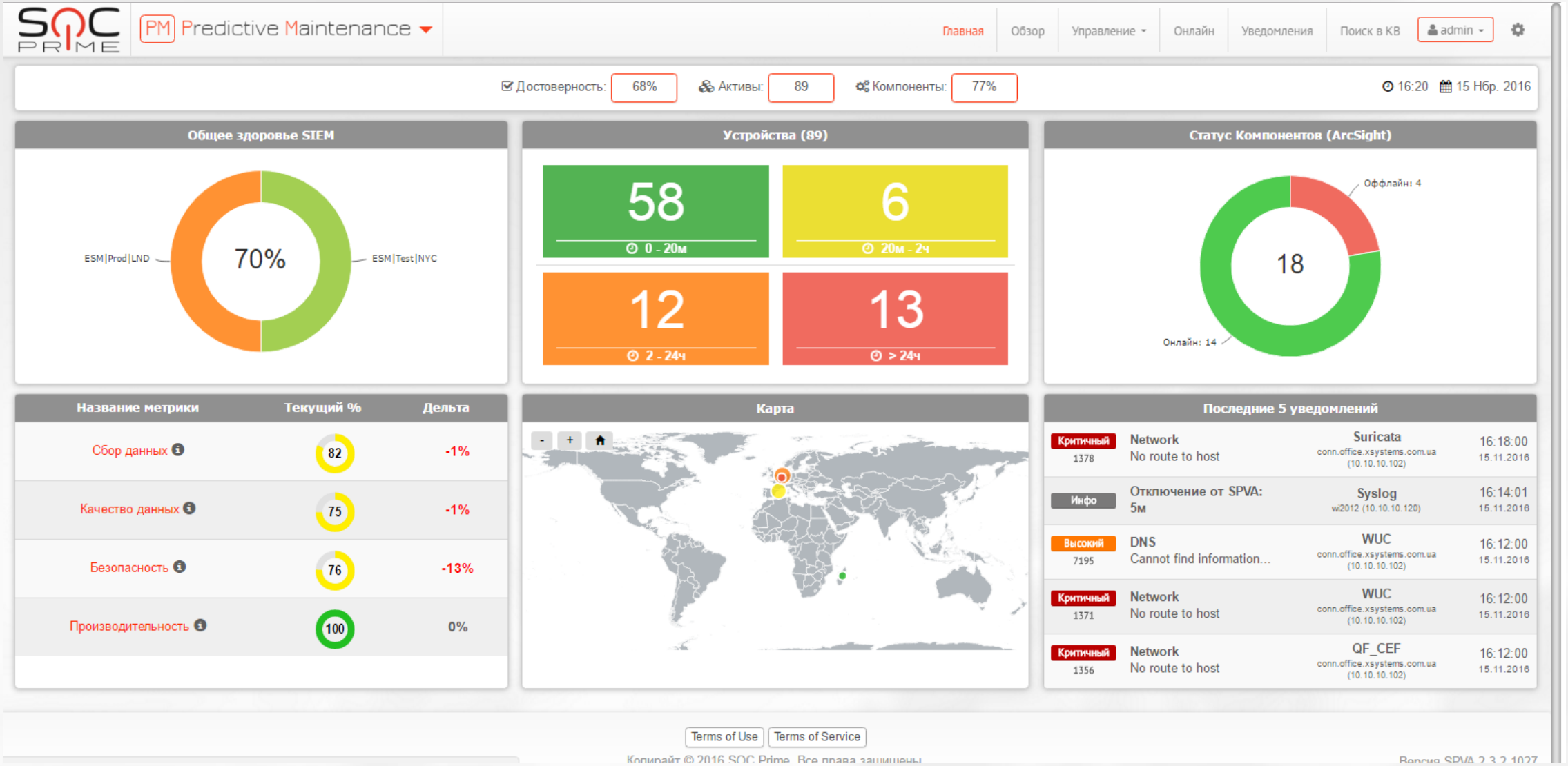
Компоненты Endpoint Security и контроля целостности часто не устанавливаются на SIEM

# Безопасность




| Component | Type | Error Name | Category | Description | Protect724 | HP KB |
|---|---|---|---|---|---|---|
| Connector | WARN | Thread [NAME] interrupted possible shutdown | Security | Connector was shutdown. | Protect724 | HP KB |
| **Recommendations:** 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 |
| **Recommendations:** 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 proccess was interrupted - Logs are NOT collected. | Protect724 | HP KB |
| **Recommendations:** The cause of this error is shutdown of connector proccess. If connector was not shutdown manualy (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 |
| **Recommendations:** 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 |
| **Recommendations:** 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 |
| **Recommendations:** 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 |
| **Recommendations:** 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 |
| **Recommendations:** 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 enviroment, 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






SOC PRIME
POWER ON SECURITY

# Преимущества для бизнеса с Predictive Maintenance

Контроль качества и простое управление сервисом SOC

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

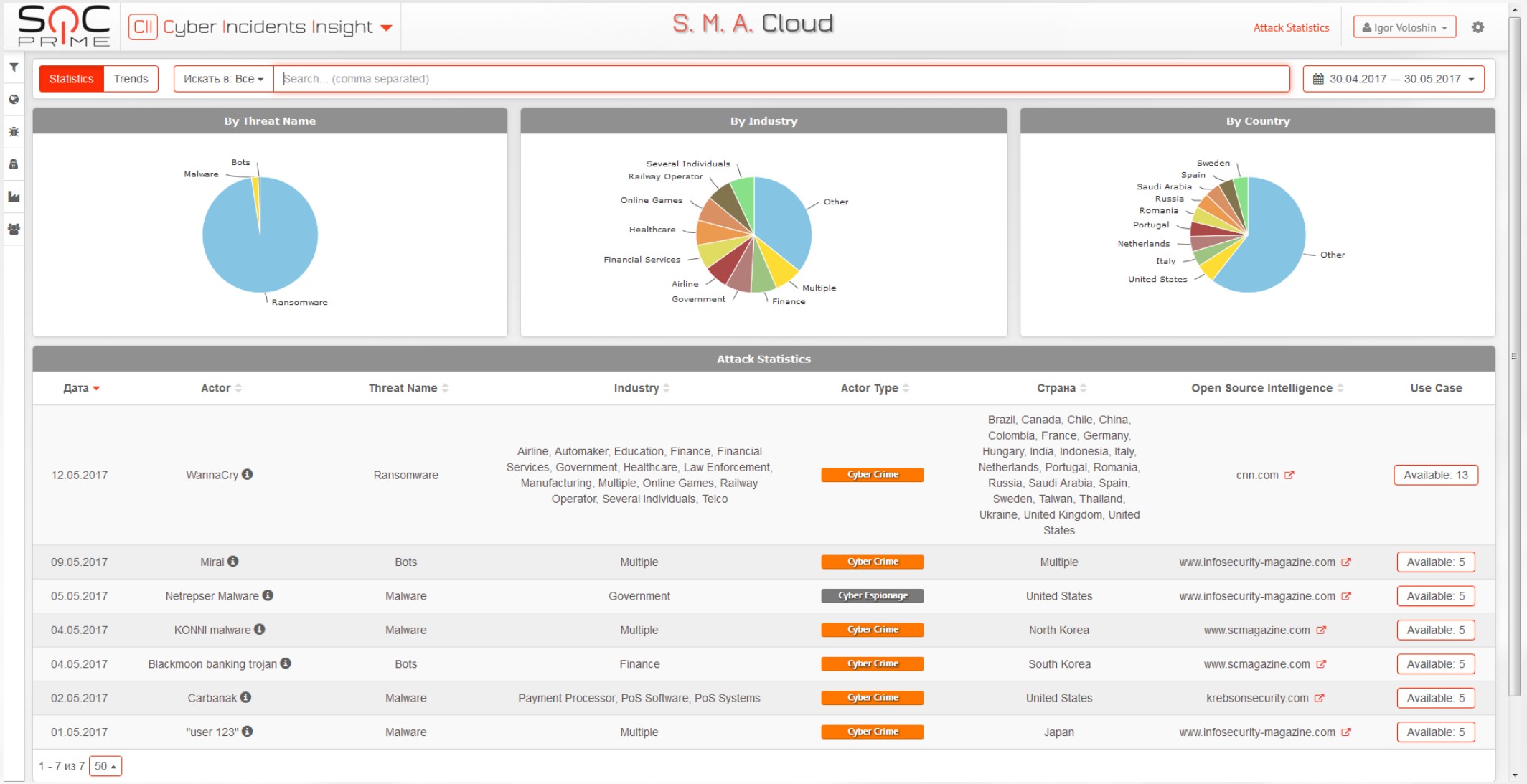
Возможность прогнозировать аномалии в работе SIEM и устранять ошибки, до того как они перерастут в критичные сбои системы

# Use Case Cloud

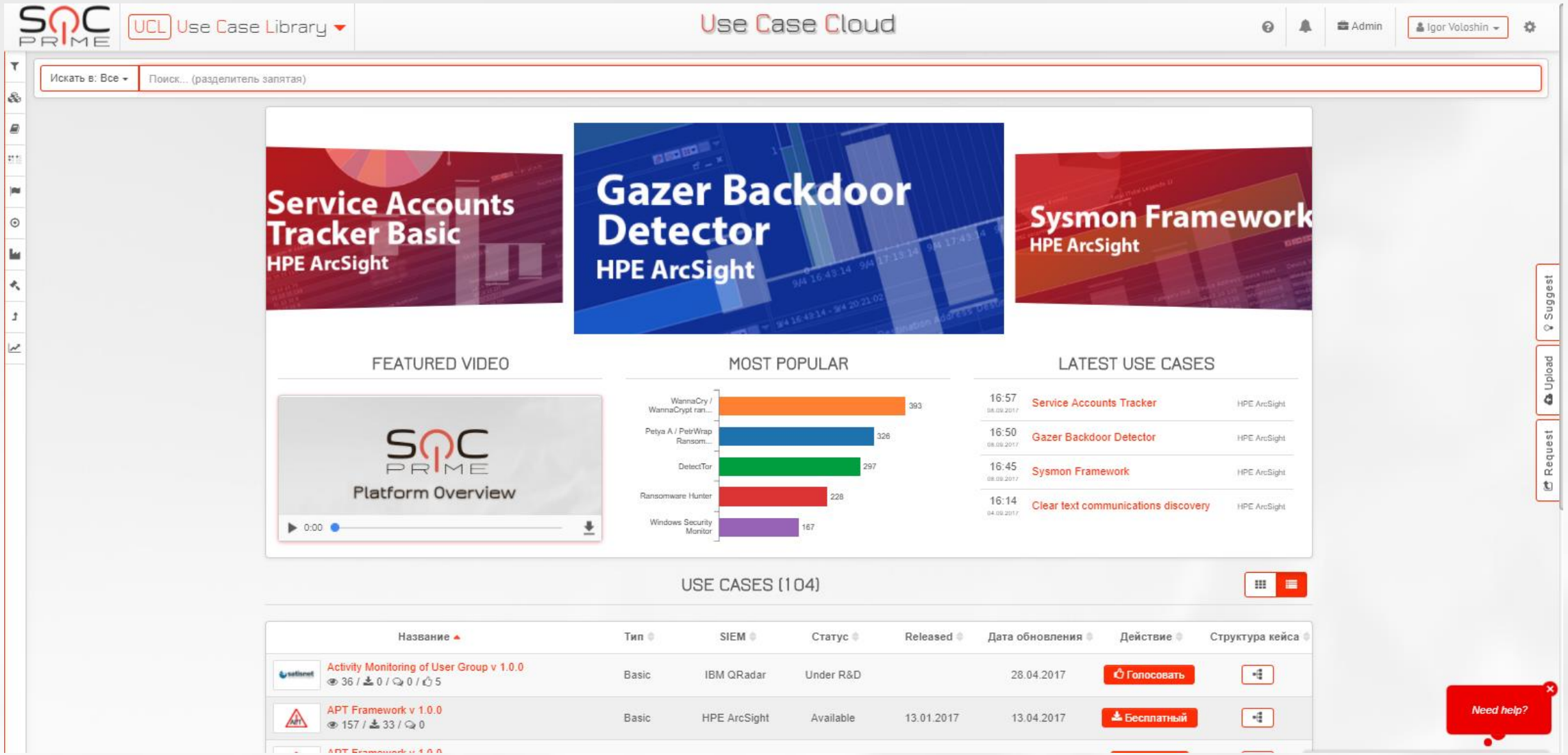



SOC PRIME
POWER ON SECURITY

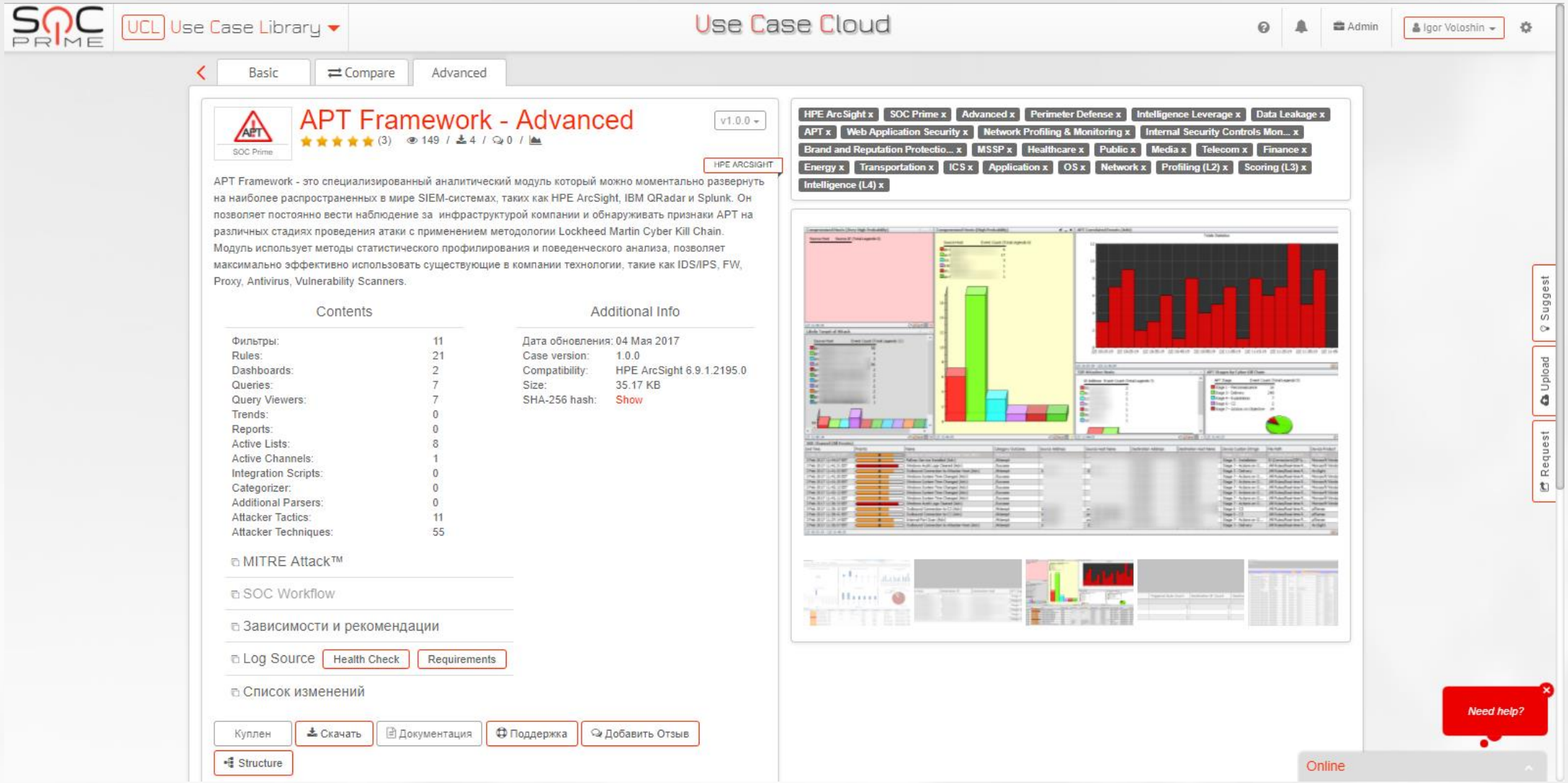
# Cyber Incidents Insight



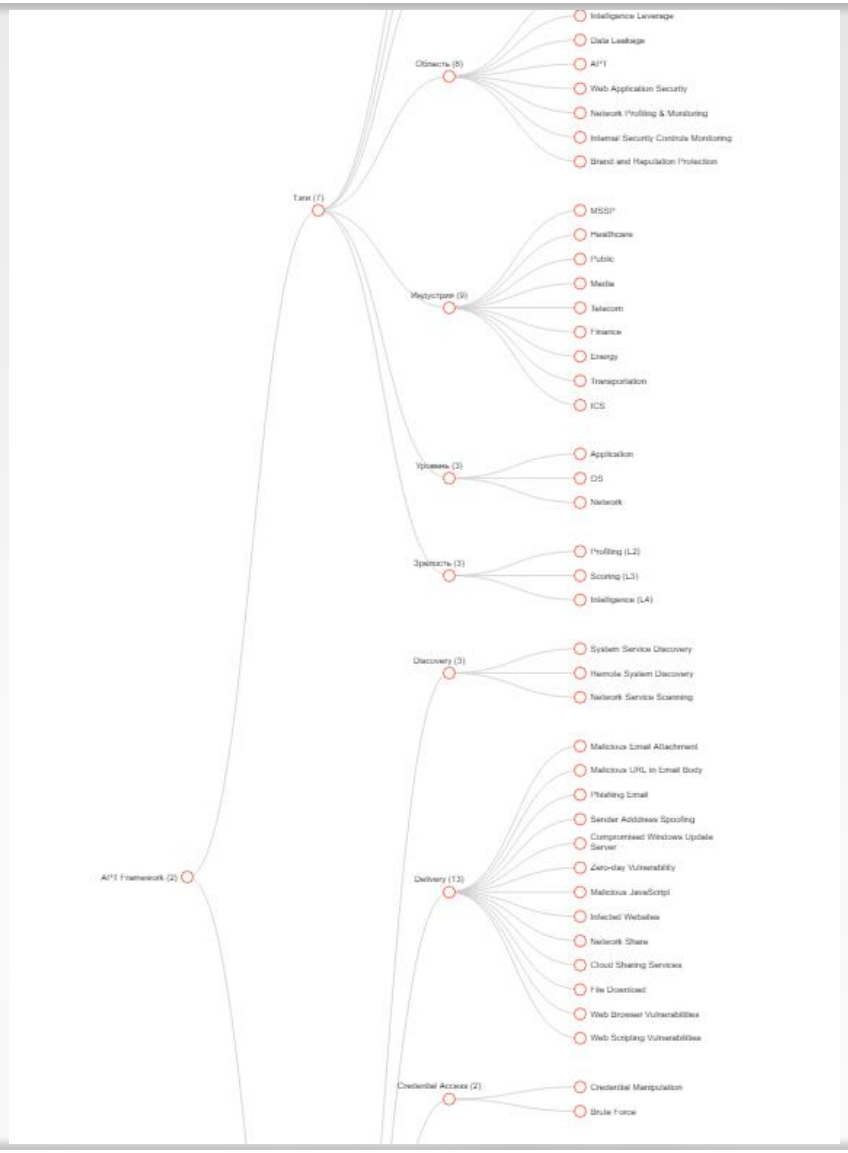
# Use Case Library



# Use Case Library



# Use Case Library



MITRE Attack™ - APT Framework - Basic

| | | | | |
|---|---|---|---|---|
| Recon<br>3 Techniques | Deliver<br>13 Techniques | Creds<br>2 Techniques | Escalate<br>3 Techniques | Evade<br>7 Techniques |
| Persist<br>4 Techniques | C&C<br>14 Techniques | Lateral<br>7 Techniques | Execute<br>3 Techniques | Collect<br>1 Techniques |
| Extract<br>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**.

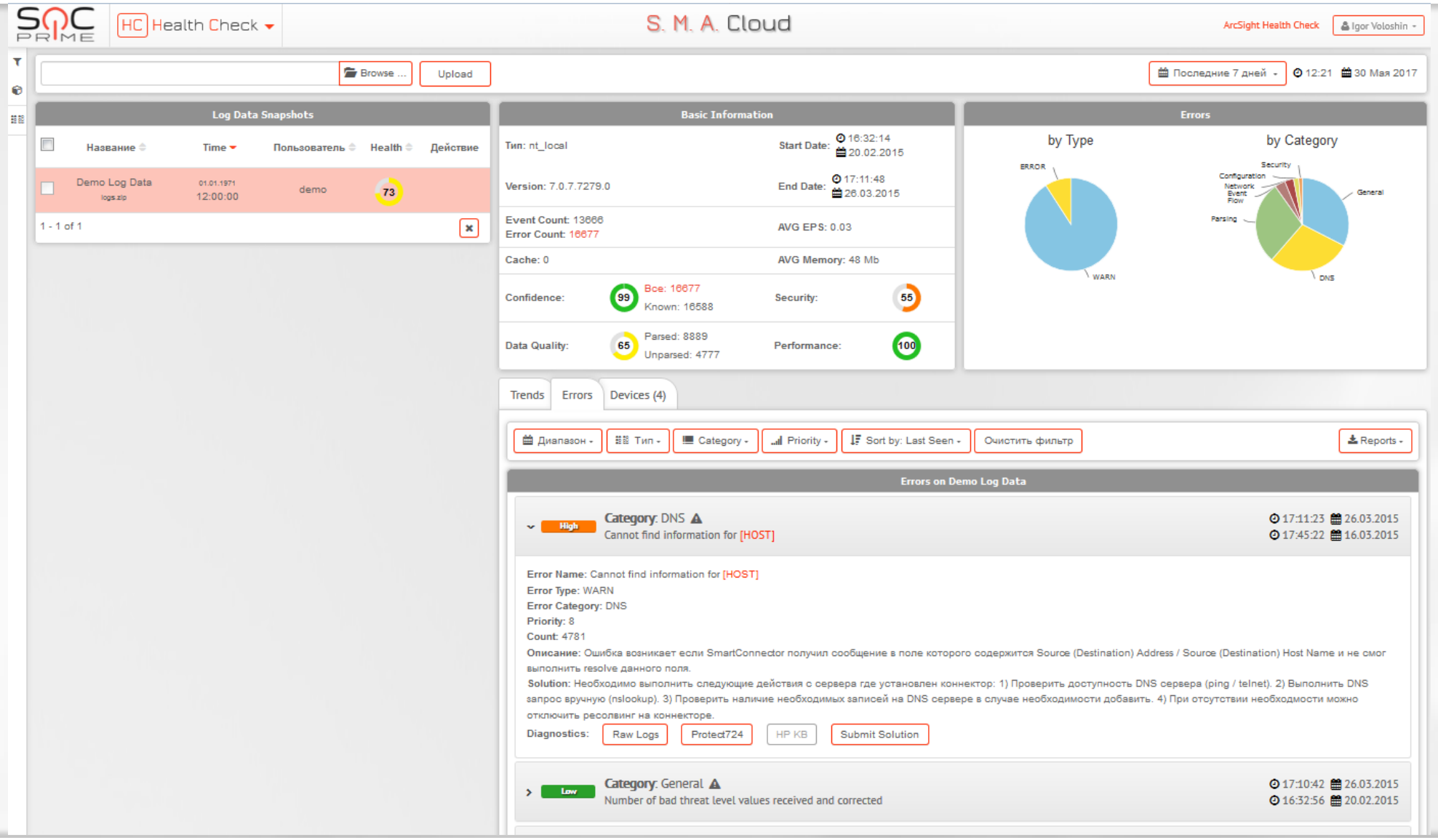
Detection | Examples | **Mitigations**

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
POWER ON SECURITY

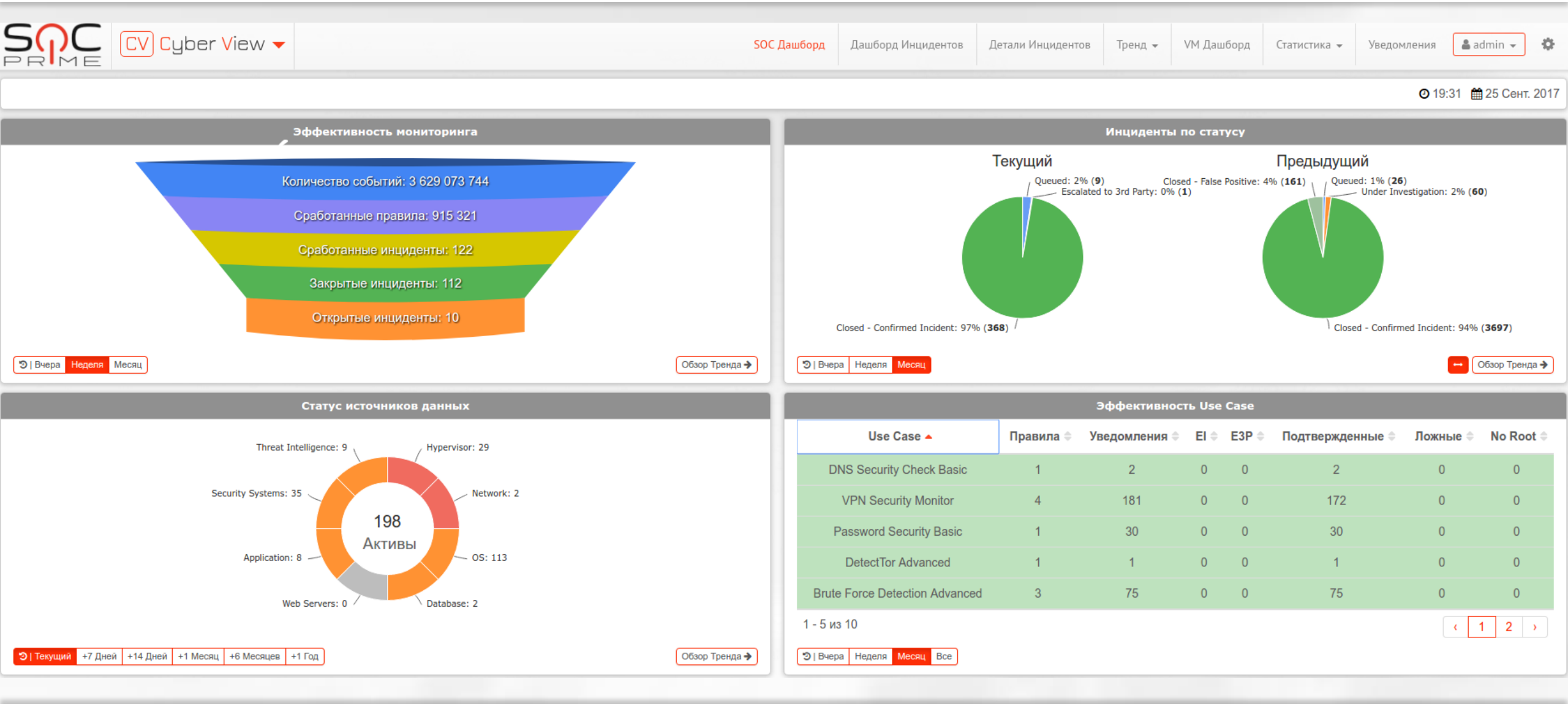
# Преимущества для бизнеса с Use Case Library

Передовые технологии для вашей команды по борьбе с киберугрозами

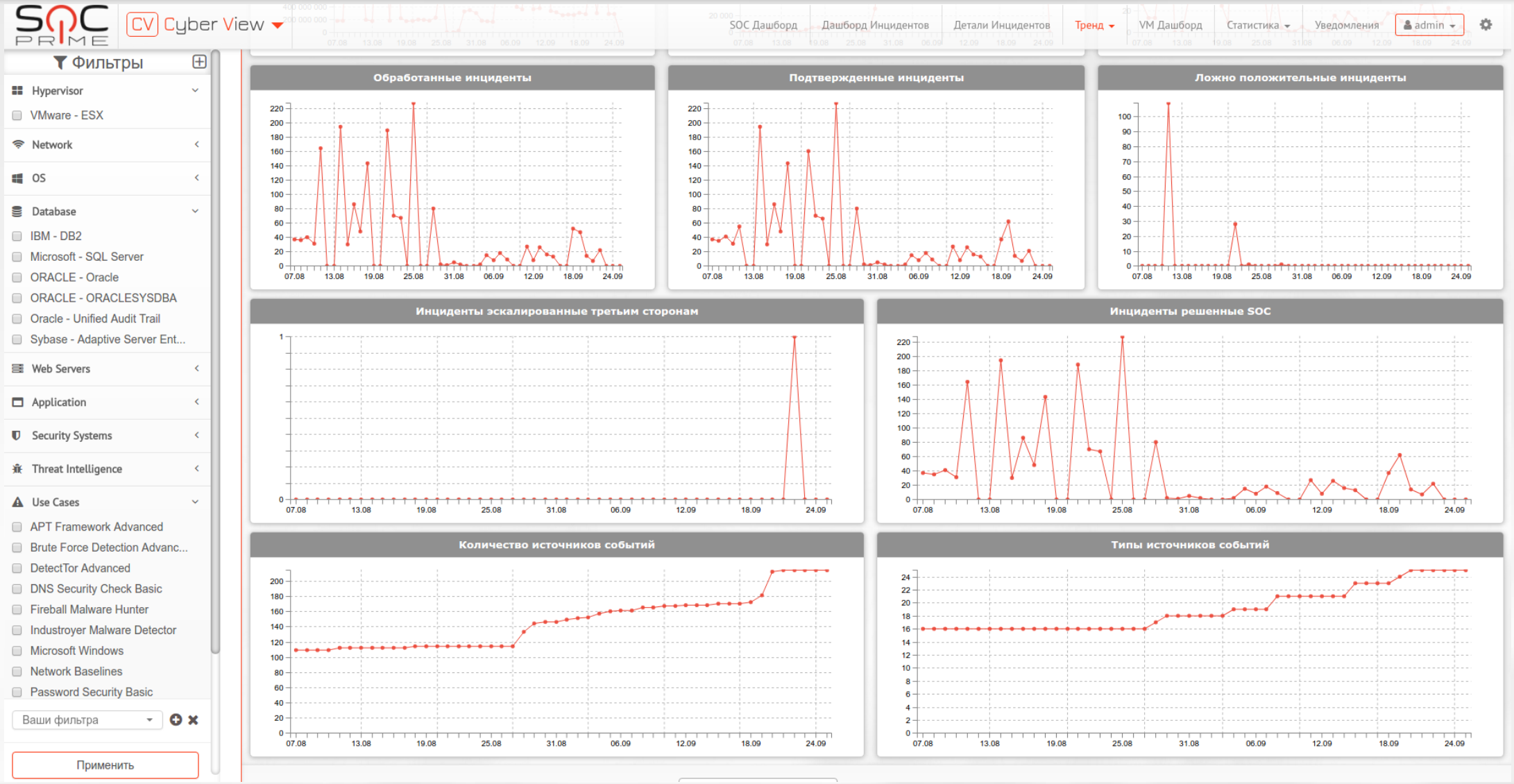
Онлайн доступ к глобальной экспертизе в отрасли кибербезопасности

Сделайте вашу SIEM умнее, выявляйте и расследуйте инциденты быстрее

# CyberView SOC мониторинг



# CyberView SOC мониторинг







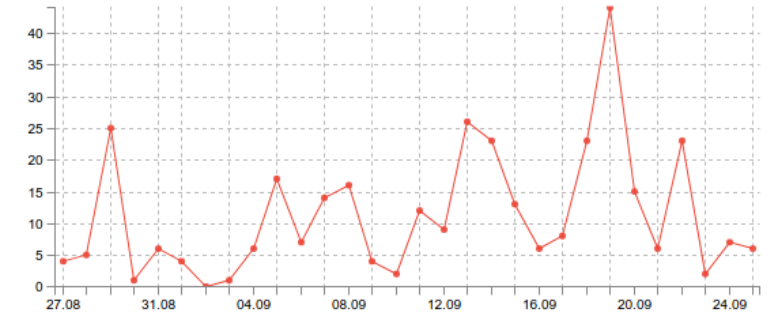

SOC PRIME
POWER ON SECURITY

# CyberView SOC мониторинг

SOC PRIME | CV Cyber View | SOC Дашборд | Дашборд Инцидентов | Детали Инцидентов | Тренд | VM Дашборд | Статистика | Уведомления | admin

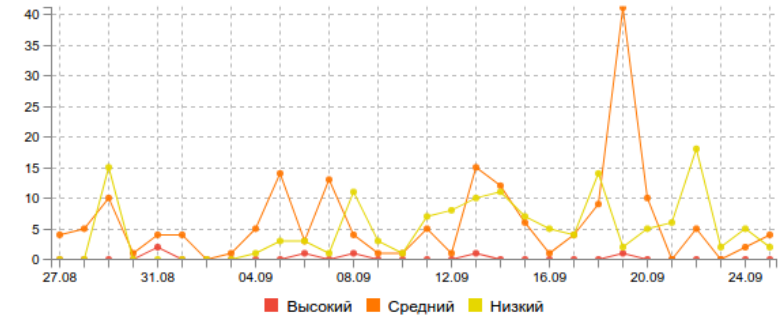
19:39 25 Сент. 2017

## Инциденты



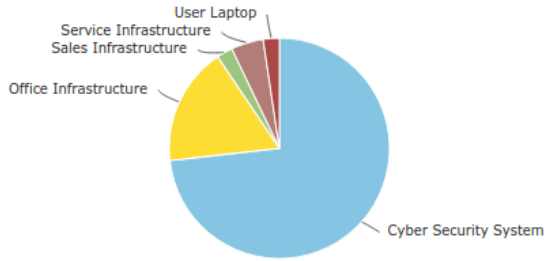

| День | Неделя | Месяц | Вид

## Инциденты по приоритету



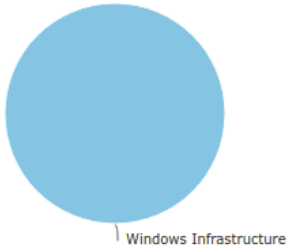

| День | Неделя | Месяц | Вид

## Инциденты по категории ассета



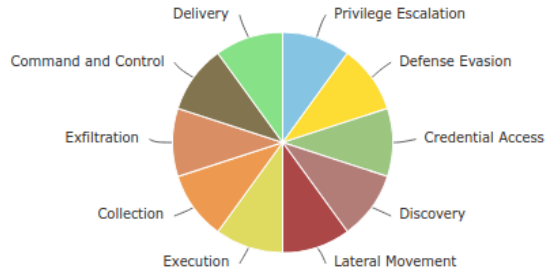

| День | Неделя | Месяц | Вид

## Инциденты по технологии




| День | Неделя | Месяц | Вид

## Инциденты по тактике




| День | Неделя | Месяц | Вид

## ТОП 5 инцидентов по владельцу ассета

| Владелец | Подразделение | Количество |
|---|---|---|
| Oleksandr Bredikhin | R&D | 96 |
| Eugeniy Samborskyi | DevOps | 28 |
| Oleksandr Verbnyak | R&D | 3 |

| День | Неделя | Месяц | Вид





SOC PRIME POWER ON SECURITY

# 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



SOC PRIME
POWER ON SECURITY