Кибербезопасность 2.0:

переход от эффективного SIEM к проактивному SOC

Андрей Безверхий
CEO & co-founder | SOC Prime
SOC-Forum v.2.0 | 2016

О нас

Международный вендор

Компания основана в 2014 г.

170+ 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

Наши клиенты

MSSP

SOLAR JSOC

mo1iv

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

Переход от SIEM к SOC

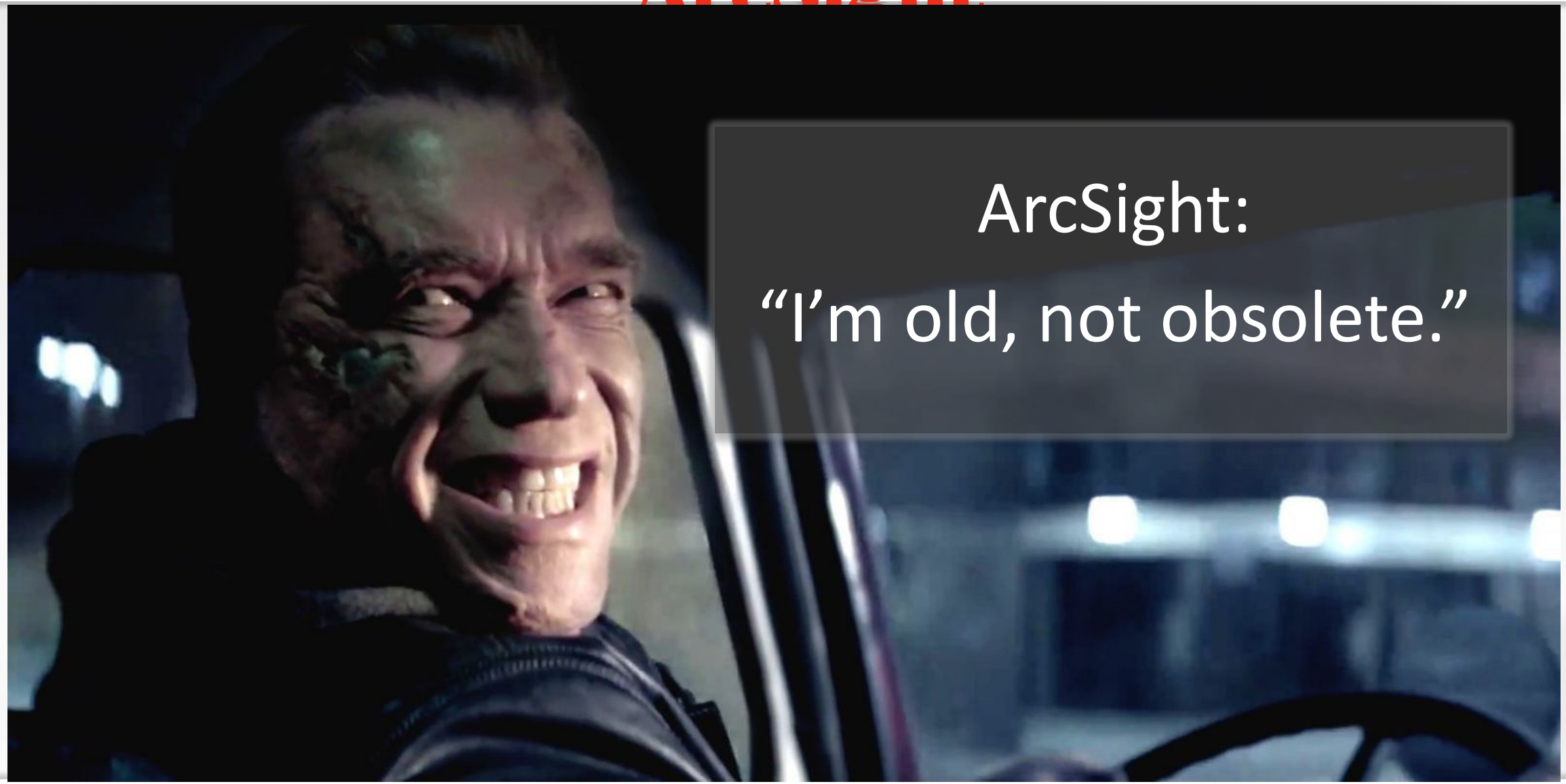
Сбор данных

Качество данных

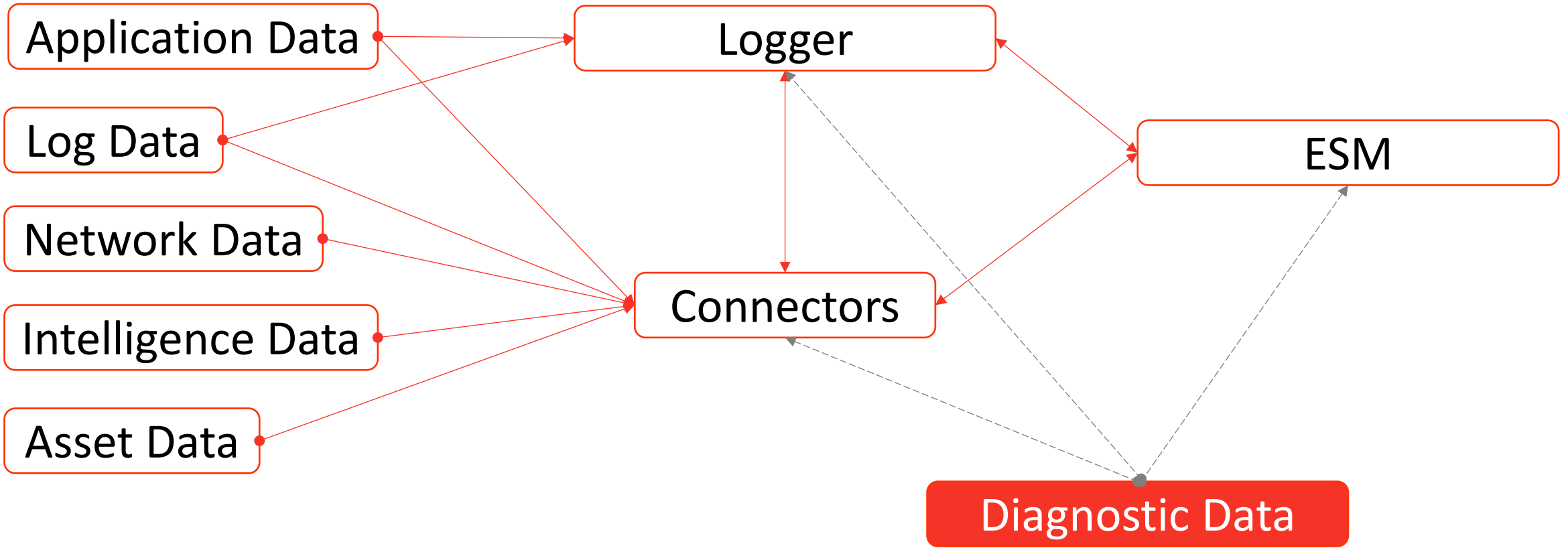
Безопасность & Производительность

Собираем все вместе ☺

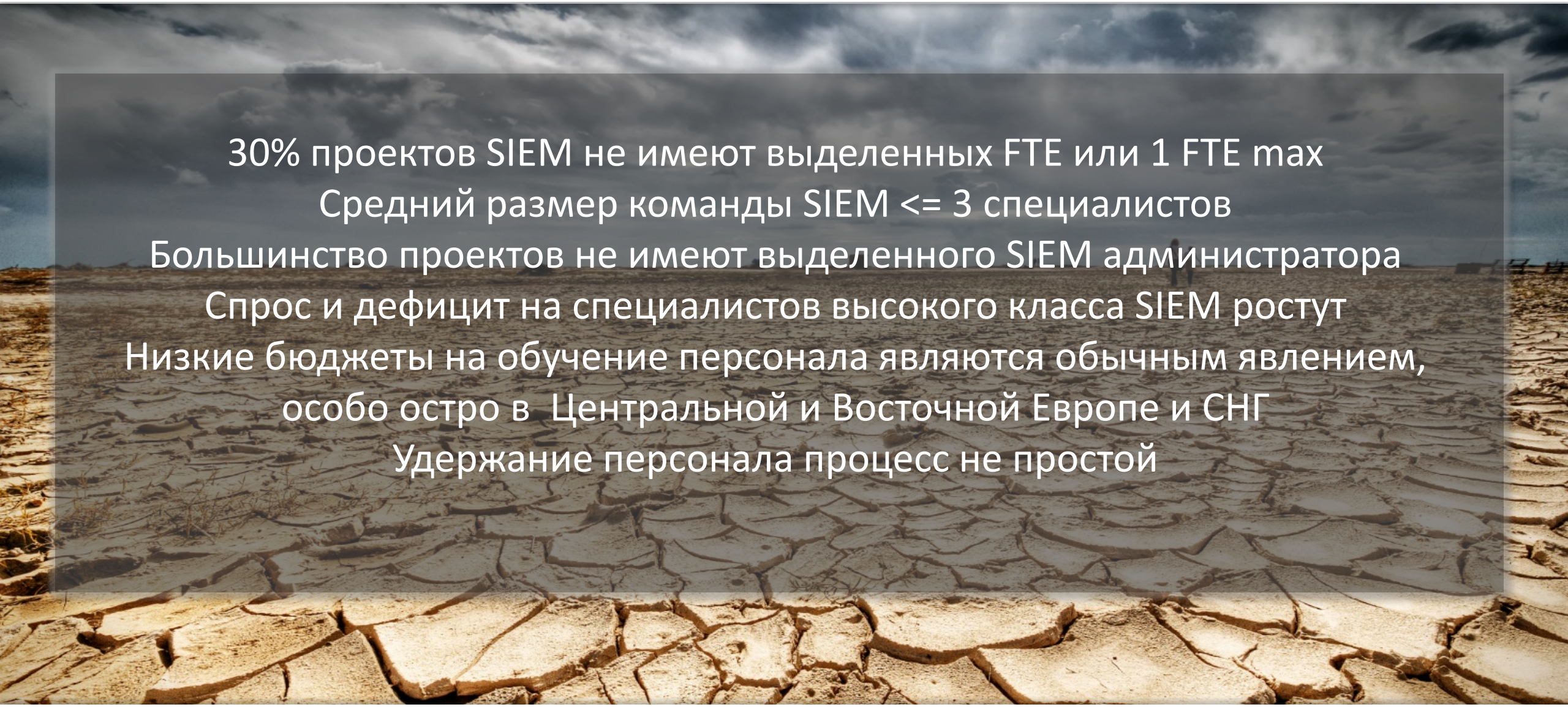
ОСТОРОЖНО: дальше примеры на ArcSight



Данные для SOC на примере ArcSight

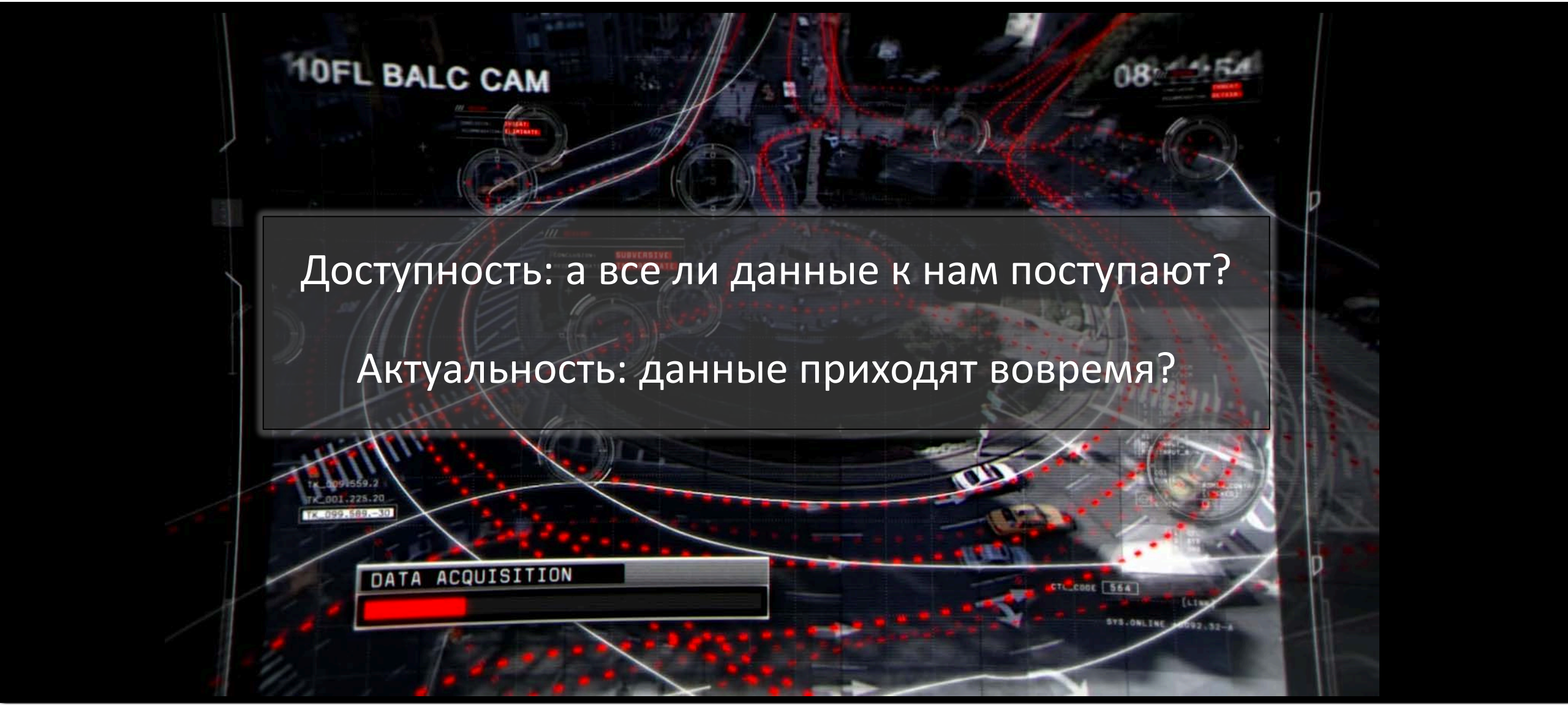


Тренды: SIEM =//= SOC



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

поговорим о сборе 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»

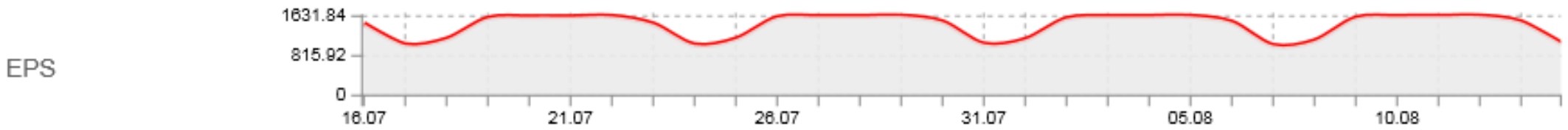
«Logger и ESM»

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		
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

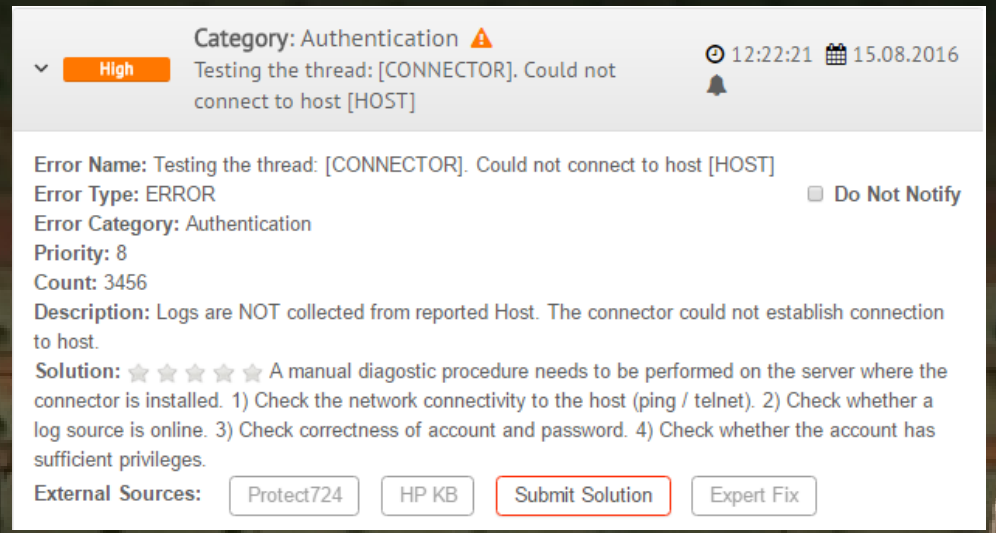
```
    at com.arcsight.agent.transport.fb.a(fb.java:638)
    at com.arcsight.agent.transport.fb.a(fb.java:389)
    at com.arcsight.agent.transport.fb.a(fb.java:349)
    at com.arcsight.agent.transport.fb.a(fb.java:307)
    at com.arcsight.agent.transport.t.onSingleEvent(t.java:101)
    at com.arcsight.agent.transport.a.m.onSingleEvent(m.java:45)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

Доступность: люди против машин

Данные для машин

```
[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)
```

Данные для людей

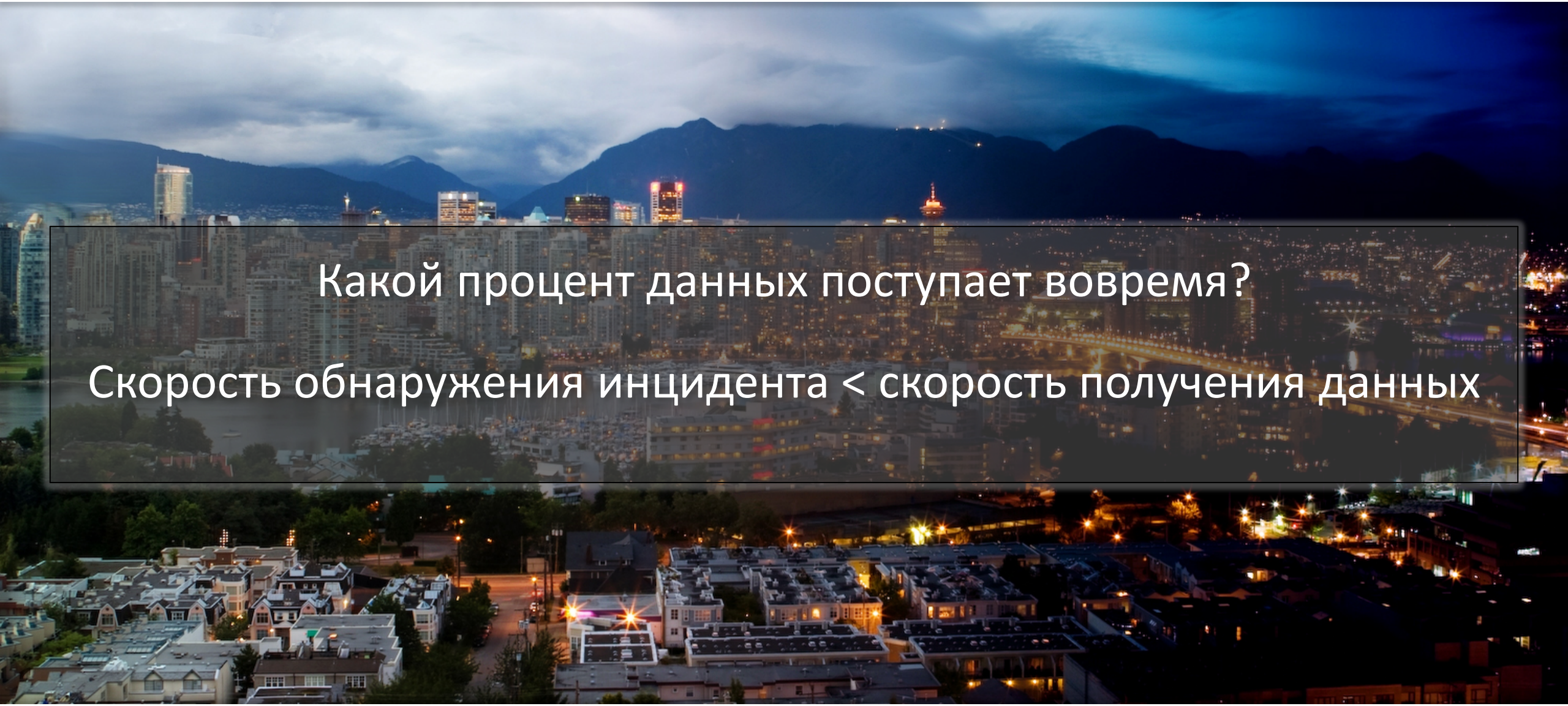


Сбор данных: доступность

Search in: All | not collected | Search

Component	Type	Error Name	Category	Description	Protect724	HP KB
Connector	ERROR	Tried version [N]. ERROR: [NAME]	Database	The Logs are NOT collected - the connection was not established. Connector was unable to determine database version.	Protect724	HP KB
Recommendations: A manual diagostic procedure needs to be performed. 1) Check network connectivity to the DB: make sure specified IP address is correct and DNS resolvable, check that port is open using TELNET, check that DB Listener is up and is bound on correct network interface and allows connections from connector IP. 2) Check whether the connector supports this version of the DB if necessary upgrade connector to the latest version or change/upgrade JDBC driver. 3) Check if account has enough privileges to make queries to the DB. 4) Make sure that all services were restarted after changing audit settings in the DB otherwise settings may not apply.						
Connector	ERROR	Testing the thread: [CONNECTOR]. Could not connect to host [HOST]	Authentication	Logs are NOT collected from reported Host. The connector could not establish connection to host.	Protect724	HP KB
Recommendations: A manual diagostic 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.						
Connector	ERROR	Could not connect to host [HOSTNAME] with configured username [USERNAME]	Authentication	Logs are NOT collected from reported Host. The connector could not establish connection to host with predifined authentication record for username it reports in error.	Protect724	HP KB
Recommendations: Please assure that authentication record defined in connector has correct spelling for username and password. Additionally verify that specified account has enough privileges to connect and collect data, try authneticating from the account manually.						
Connector	WARN	Waiting [N] to retry database detection for [NAME]	Database	Logs are NOT collected - detection and connection to the database failed. The connection was not established.	Protect724	HP KB
Recommendations: A manual diagnostics needs to be performed. 1) Check the network access to the host with database. 2) Check the correctness of the authentication credentials and whether there are all necessary privileges for the account. 3) Check whether there is necessary JDBC driver in a directory /Connector Home/current/user/agent/lib if necessary upgrade to a more stable version.						
Connector	WARN	Stored password did not work for [INSTANCE NAME]	Authentication	Logs are NOT collected - incorrect login or password. Connector can not communicate with the remote host.	Protect724	HP KB
Recommendations: It is necessary to validate the login and password by connecting to DB host with an external SQL client to connect to host (DB). Possibly account password has been changed.						
Connector	WARN	Tried version [N]. ERROR: [NAME]	Configuration	The Logs are NOT collected - the connection was not established. Connector was unable to determine database version.	Protect724	HP KB
Recommendations: A manual diagostic procedure needs to be performed. 1) Check network connectivity to the DB: make sure specified IP address is correct and DNS resolvable, check that port is open using TELNET, check that DB Listener is up and is bound on correct network interface and allows connections from connector IP. 2) Check whether the connector supports this version of the DB if necessary upgrade connector to the latest version or change/upgrade JDBC driver. 3) Check if account has enough privileges to make queries to the DB. 4) Make sure that all services were restarted after changing audit settings in the DB otherwise settings may not apply.						
Connector	WARN	Failed to process query [QUERY] on database URL	Database	Logs are NOT collected - connector failed to process query on database.	Protect724	HP KB

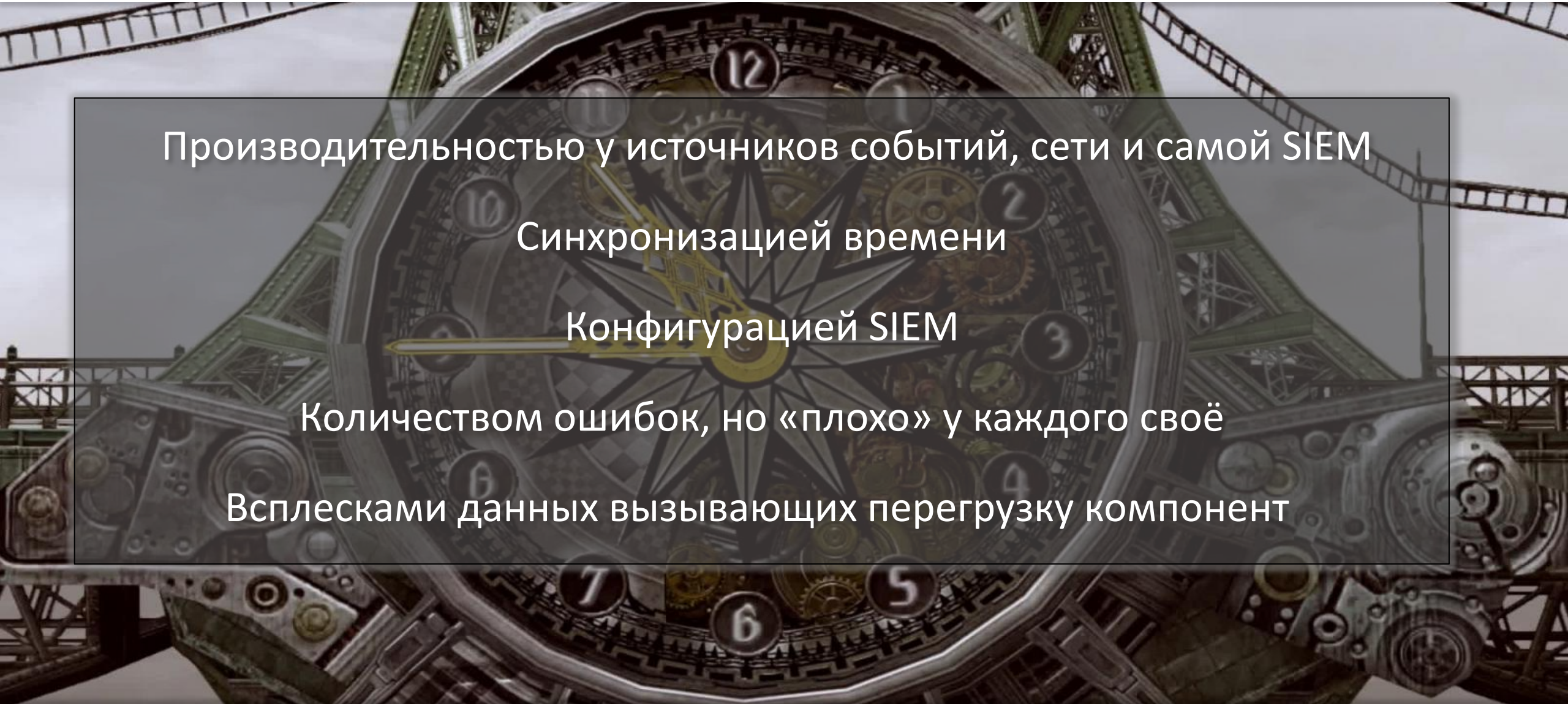
Сбор данных: Актуальность



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

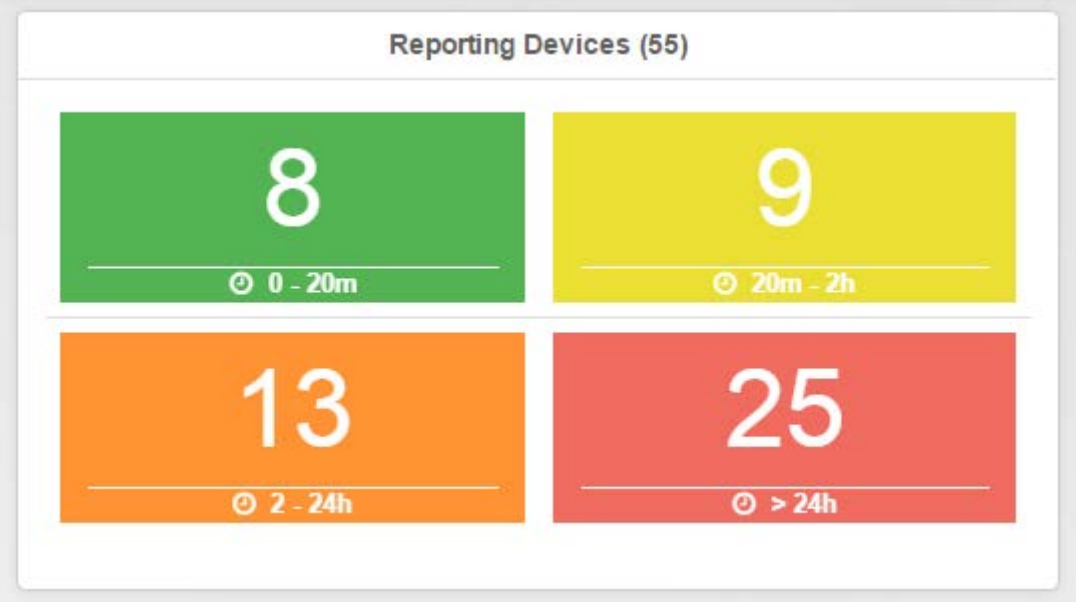
Конфигурацией SIEM

Количеством ошибок, но «плохо» у каждого своё

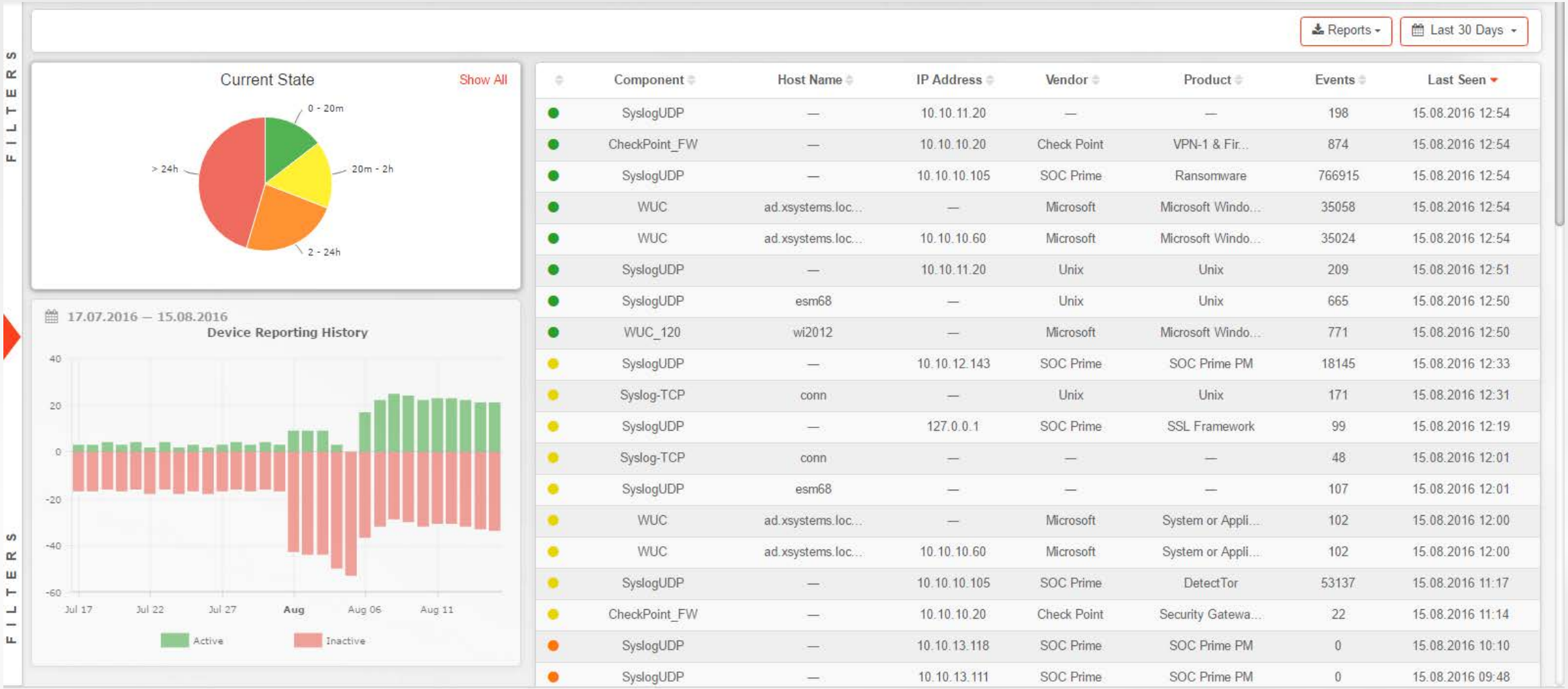
Всплесками данных вызывающих перегрузку компонент

Сбор данных: актуальность

Формула: время получения менеджером - время генерации на источнике



Сбор данных: актуальность



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: Целостность

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

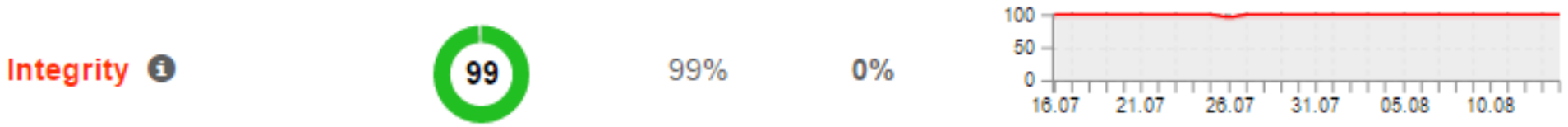
PCI, SOX, ISO 27K = хранить данные в «формате без изменений»

Качество данных: целостность

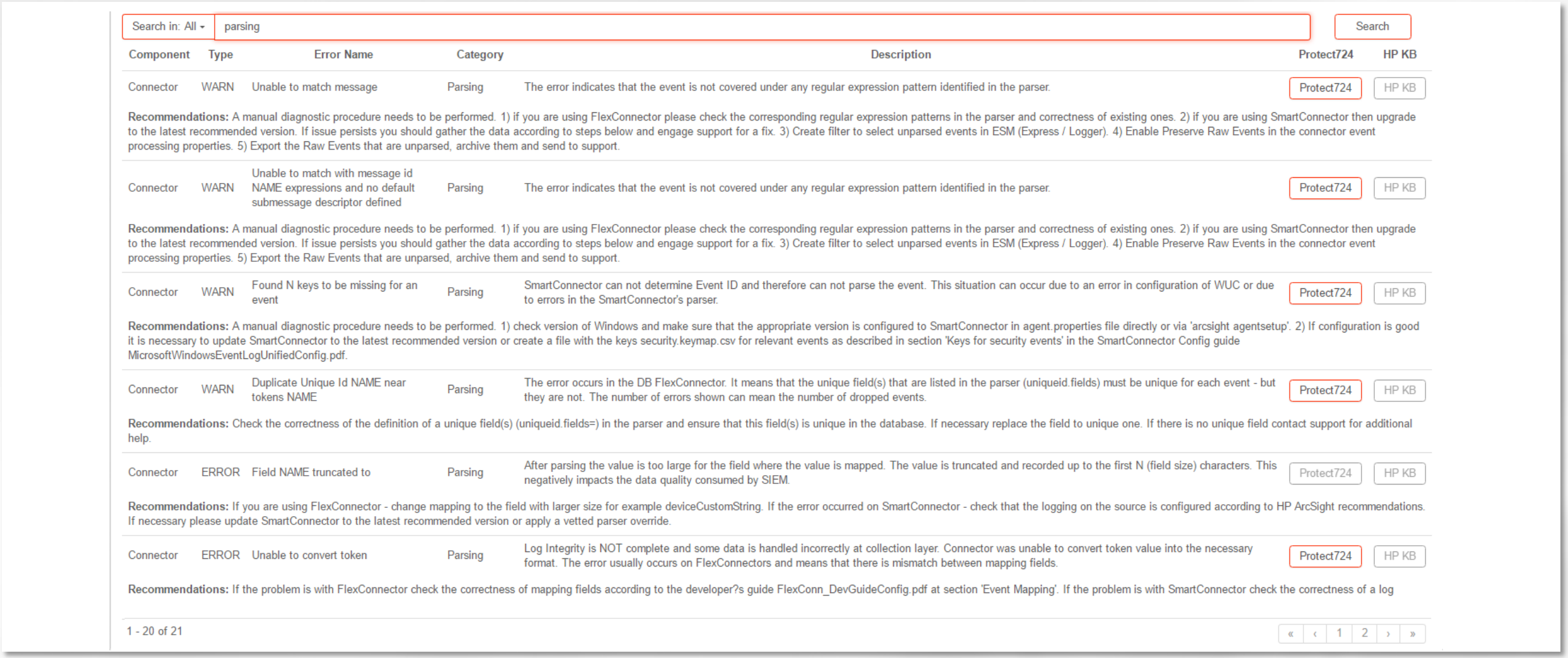
«Парсинг» необходимо контролировать непрерывно

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: целостность



Search in: All | parsing | Search

Component	Type	Error Name	Category	Description	Protect724	HP KB
Connector	WARN	Unable to match message	Parsing	The error indicates that the event is not covered under any regular expression pattern identified in the parser.	Protect724	HP KB
Recommendations: A manual diagnostic procedure needs to be performed. 1) if you are using FlexConnector please check the corresponding regular expression patterns in the parser and correctness of existing ones. 2) if you are using SmartConnector then upgrade to the latest recommended version. If issue persists you should gather the data according to steps below and engage support for a fix. 3) Create filter to select unparsed events in ESM (Express / Logger). 4) Enable Preserve Raw Events in the connector event processing properties. 5) Export the Raw Events that are unparsed, archive them and send to support.						
Connector	WARN	Unable to match with message id NAME expressions and no default submessage descriptor defined	Parsing	The error indicates that the event is not covered under any regular expression pattern identified in the parser.	Protect724	HP KB
Recommendations: A manual diagnostic procedure needs to be performed. 1) if you are using FlexConnector please check the corresponding regular expression patterns in the parser and correctness of existing ones. 2) if you are using SmartConnector then upgrade to the latest recommended version. If issue persists you should gather the data according to steps below and engage support for a fix. 3) Create filter to select unparsed events in ESM (Express / Logger). 4) Enable Preserve Raw Events in the connector event processing properties. 5) Export the Raw Events that are unparsed, archive them and send to support.						
Connector	WARN	Found N keys to be missing for an event	Parsing	SmartConnector can not determine Event ID and therefore can not parse the event. This situation can occur due to an error in configuration of WUC or due to errors in the SmartConnector's parser.	Protect724	HP KB
Recommendations: A manual diagnostic procedure needs to be performed. 1) check version of Windows and make sure that the appropriate version is configured to SmartConnector in agent.properties file directly or via 'arcsight agentsetup'. 2) If configuration is good it is necessary to update SmartConnector to the latest recommended version or create a file with the keys security.keymap.csv for relevant events as described in section 'Keys for security events' in the SmartConnector Config guide MicrosoftWindowsEventLogUnifiedConfig.pdf.						
Connector	WARN	Duplicate Unique Id NAME near tokens NAME	Parsing	The error occurs in the DB FlexConnector. It means that the unique field(s) that are listed in the parser (uniqueid.fields) must be unique for each event - but they are not. The number of errors shown can mean the number of dropped events.	Protect724	HP KB
Recommendations: Check the correctness of the definition of a unique field(s) (uniqueid.fields=) in the parser and ensure that this field(s) is unique in the database. If necessary replace the field to unique one. If there is no unique field contact support for additional help.						
Connector	ERROR	Field NAME truncated to	Parsing	After parsing the value is too large for the field where the value is mapped. The value is truncated and recorded up to the first N (field size) characters. This negatively impacts the data quality consumed by SIEM.	Protect724	HP KB
Recommendations: If you are using FlexConnector - change mapping to the field with larger size for example deviceCustomString. If the error occurred on SmartConnector - check that the logging on the source is configured according to HP ArcSight recommendations. If necessary please update SmartConnector to the latest recommended version or apply a vetted parser override.						
Connector	ERROR	Unable to convert token	Parsing	Log Integrity is NOT complete and some data is handled incorrectly at collection layer. Connector was unable to convert token value into the necessary format. The error usually occurs on FlexConnectors and means that there is mismatch between mapping fields.	Protect724	HP KB
Recommendations: If the problem is with FlexConnector check the correctness of mapping fields according to the developer?s guide FlexConn_DevGuideConfig.pdf at section 'Event Mapping'. If the problem is with SmartConnector check the correctness of a log						

1 - 20 of 21 « ‹ 1 2 › »

SOC PRIME
POWER ON SECURITY

Качество данных: категоризация

Знать все коды событий

Для всех систем в вашей организации

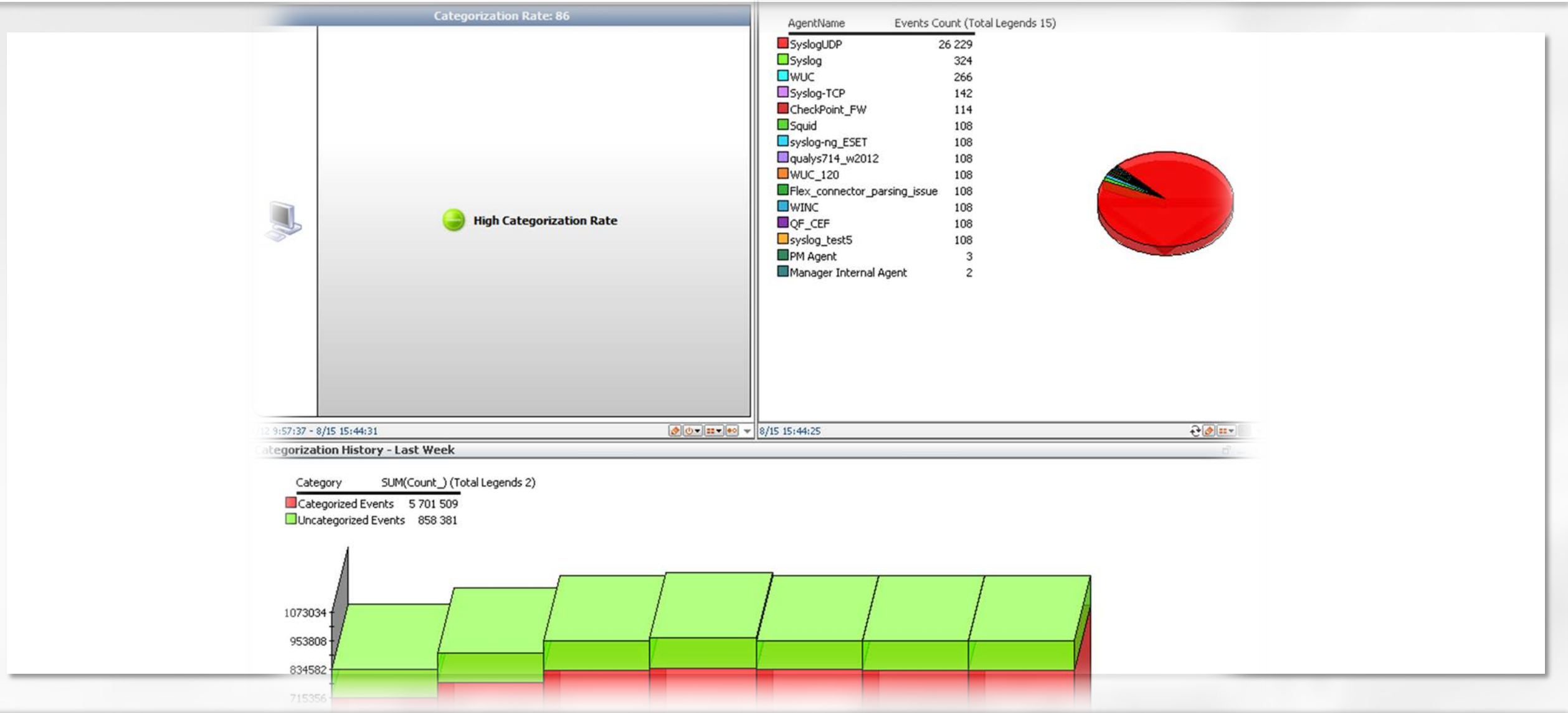
Быть в курсе всех изменений

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

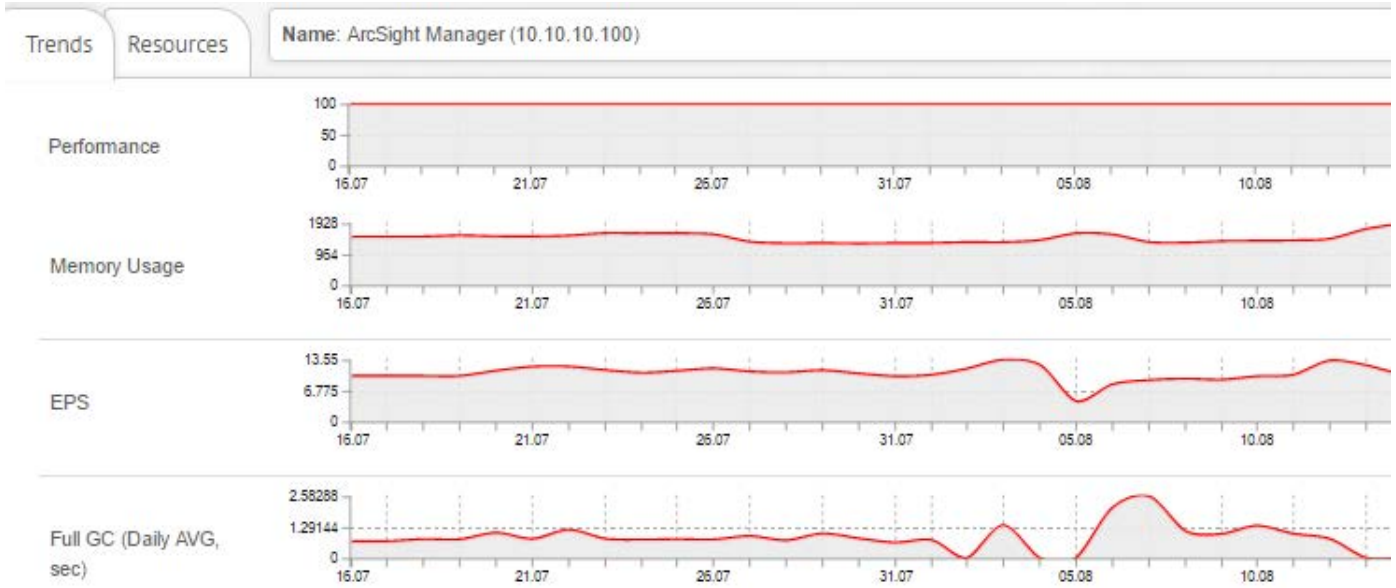
Формула: Общее кол-во IP-адресов с инвентарной моделью / Общее кол-во IP-адресов

Производительность

Status	Name	Health	Performance	Categorization	Realtime	Memory (Mb)	EPS	GC	UCL
	WUC	38.47	100	97	95	167	0.48		
	ArcSight Manager (10.10.10.100)	45.71	100	86	99	1407	10.28		
	Flex_connector_parsing_issue	74.15	100	0					
	QF_CEF	74.15	100	0					
	WINC	74.85	100	0					
	qualys714_w2012	74.85	100	0	—	160	0.01		—

AVG FGC: Before 846432; After 725806; Max 4132352; Spent Time 0.889827

	Date	Before(B)	After(B)	Max(B)	Time(s)
Last 5 Events:	15.08.2016 15:57:13;	840517;	716445;	4112384;	0.926981
	15.08.2016 14:57:12;	860367;	728595;	4146176;	0.679785
	15.08.2016 13:57:11;	848921;	723080;	4115456;	0.706961
	15.08.2016 12:57:11;	858491;	731113;	4145152;	0.63965
	15.08.2016 11:57:09;	851094;	729041;	4140032;	1.10221



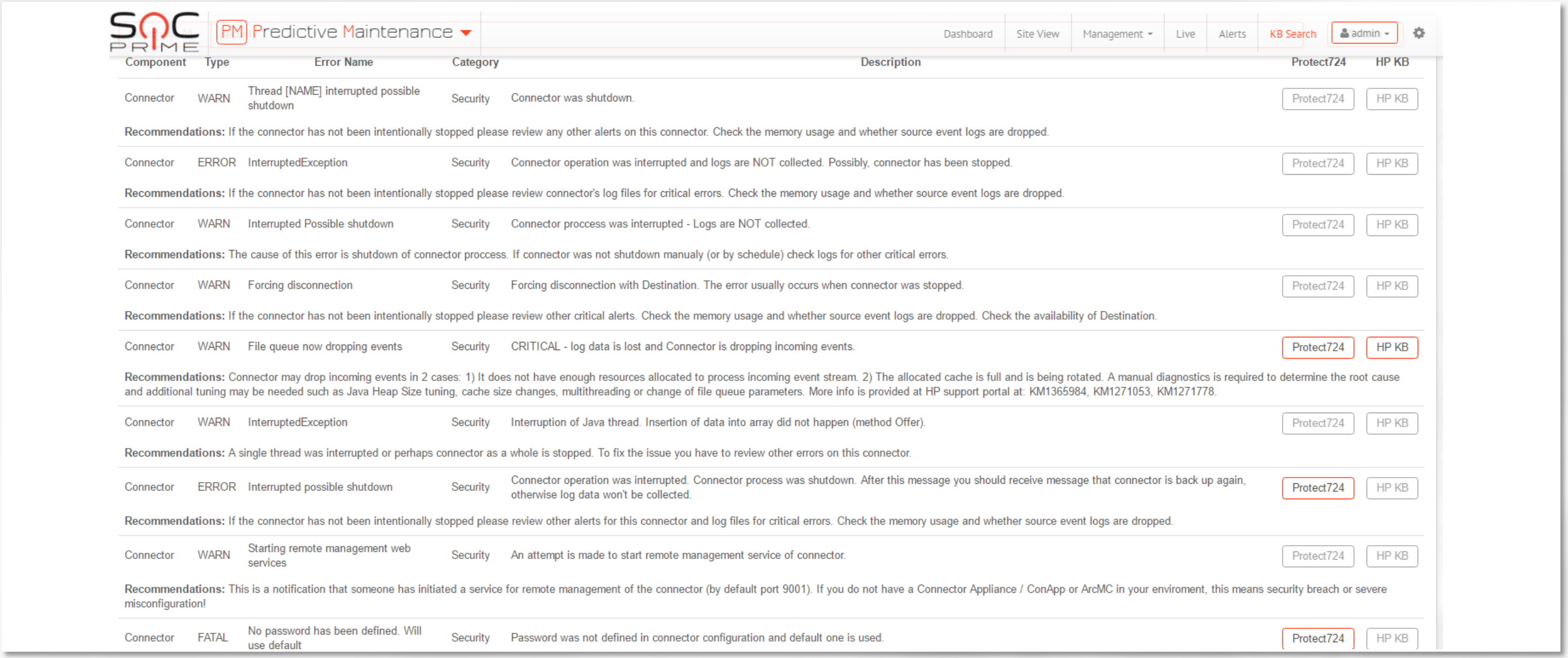
Безопасность

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

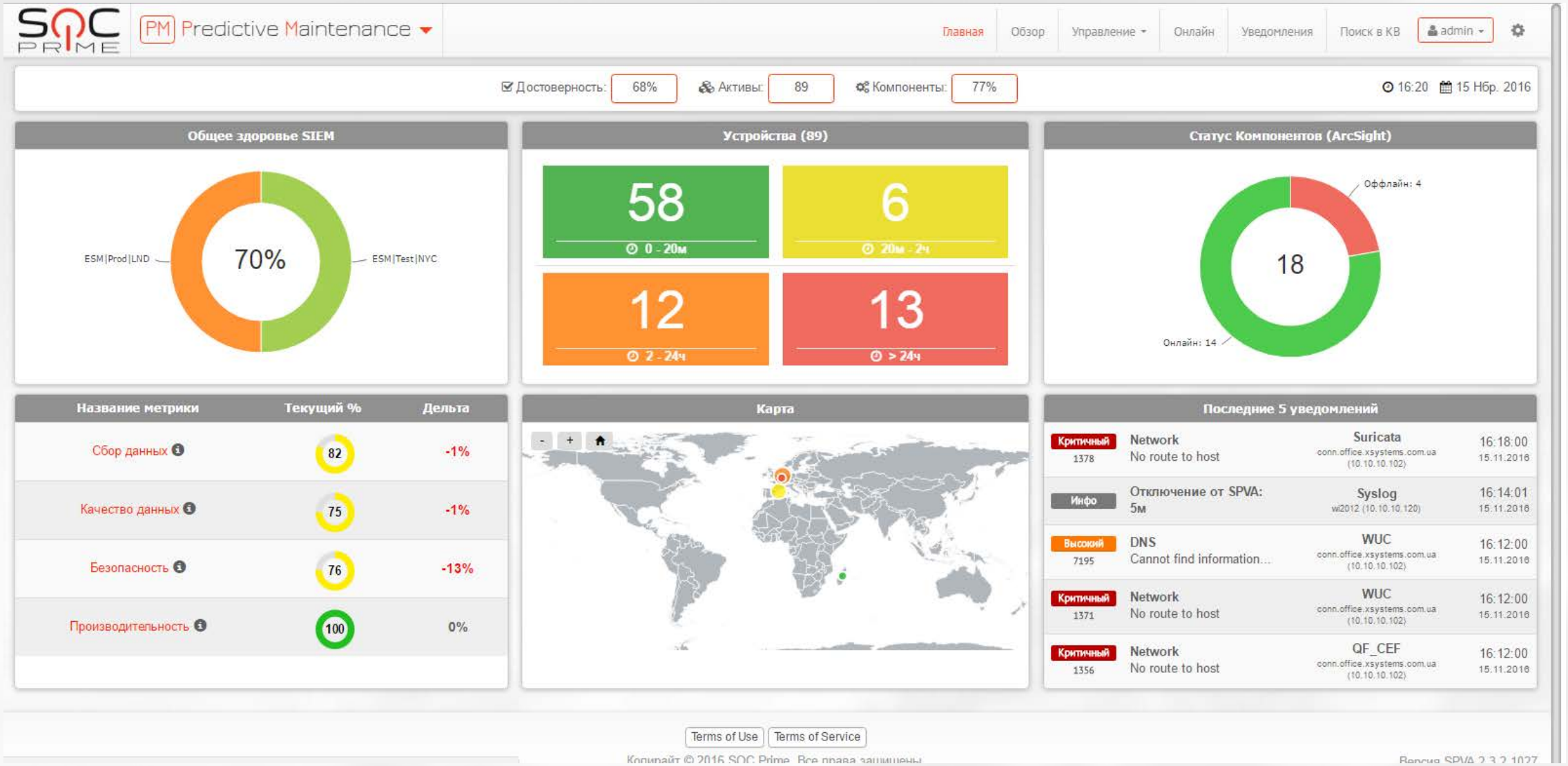
Безопасность



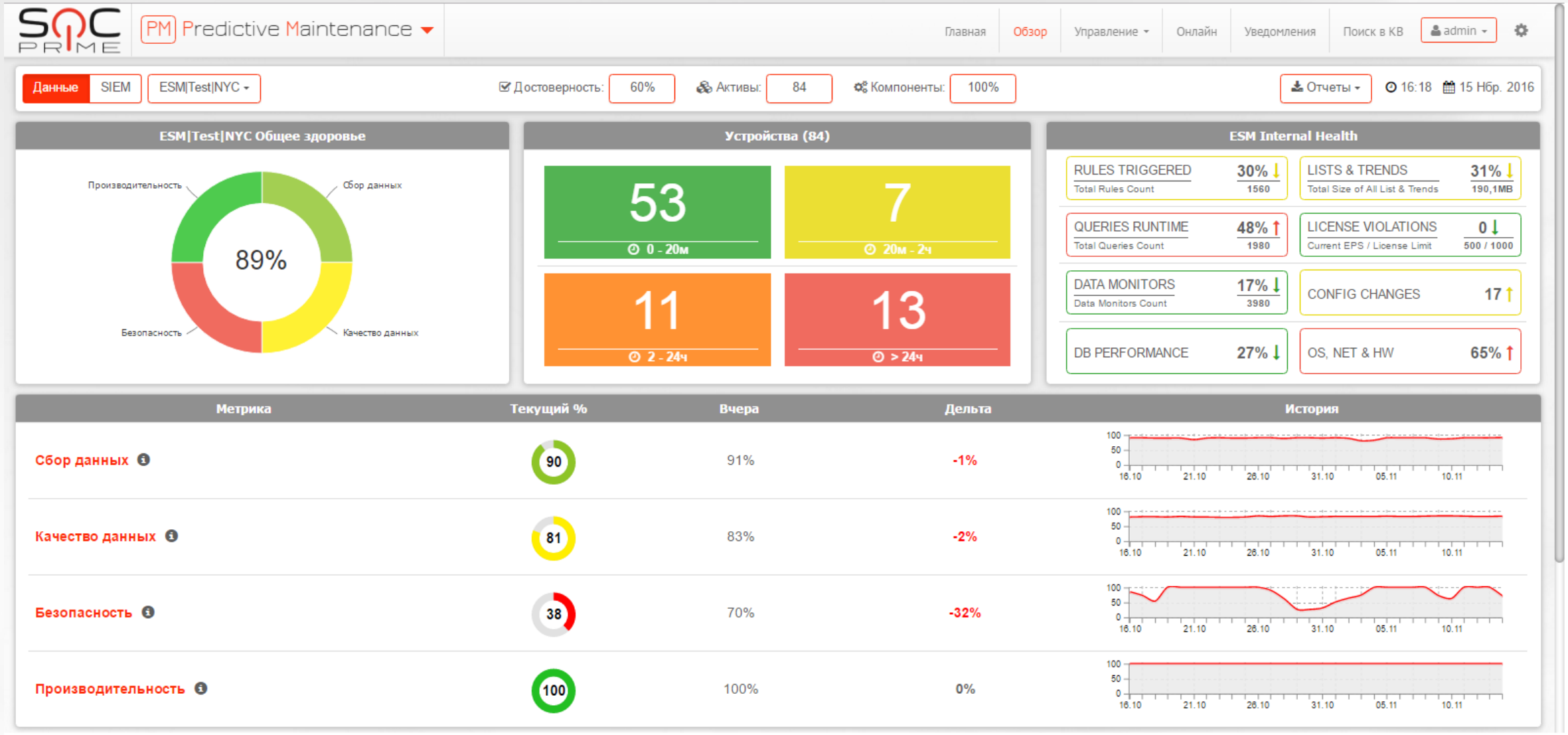
SOC PRIME | PM Predictive Maintenance | Dashboard | Site View | Management | Live | Alerts | KB Search | admin

Component	Type	Error Name	Category	Description	Protect724	HP KB
Connector	WARN	Thread [NAME] interrupted possible shutdown	Security	Connector was shutdown.	Protect724	HP KB
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

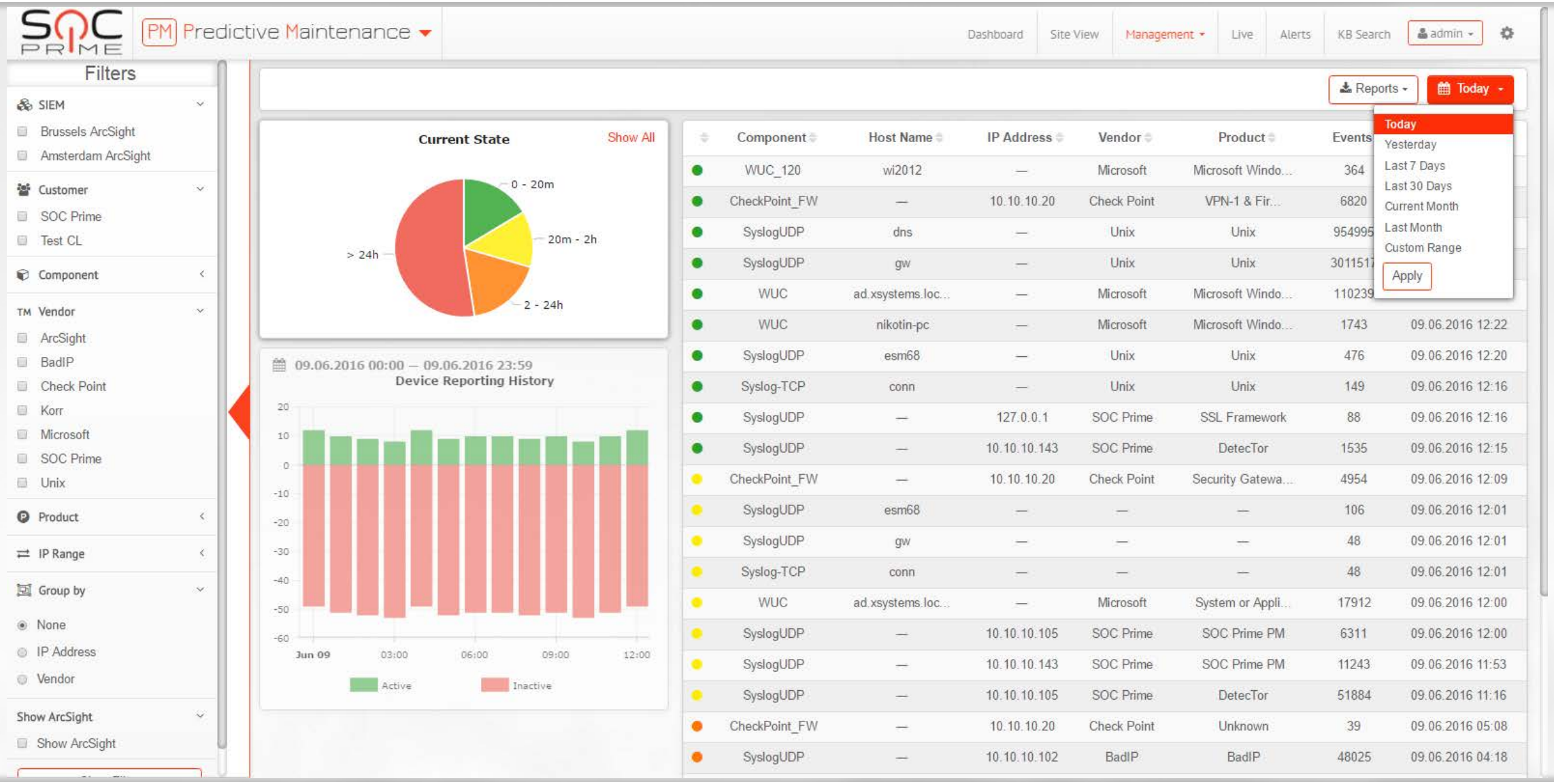


Метрики и обзор устройств



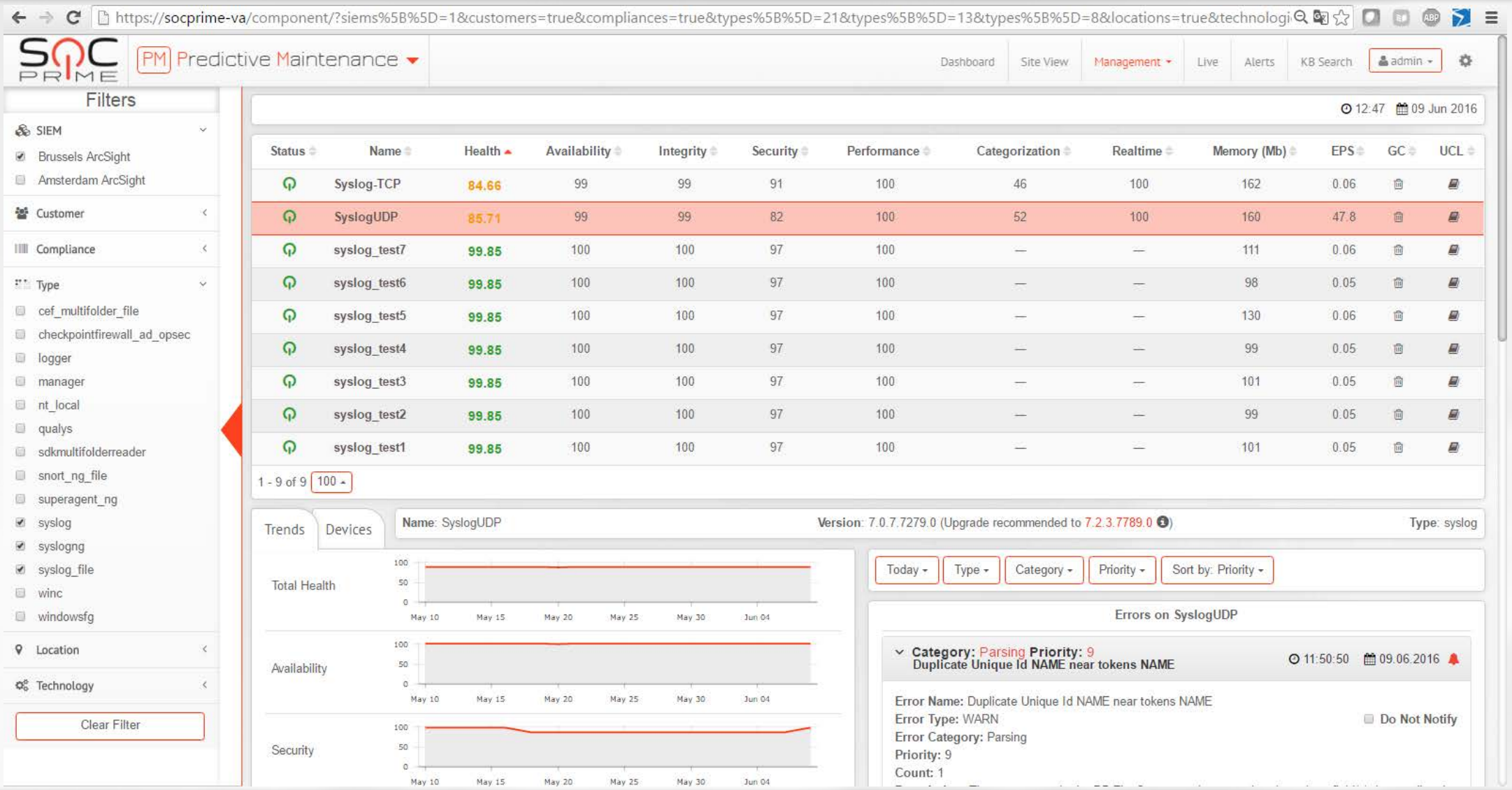
SOC PRIME
POWER ON SECURITY

Отчетность по устройствам и актуальности



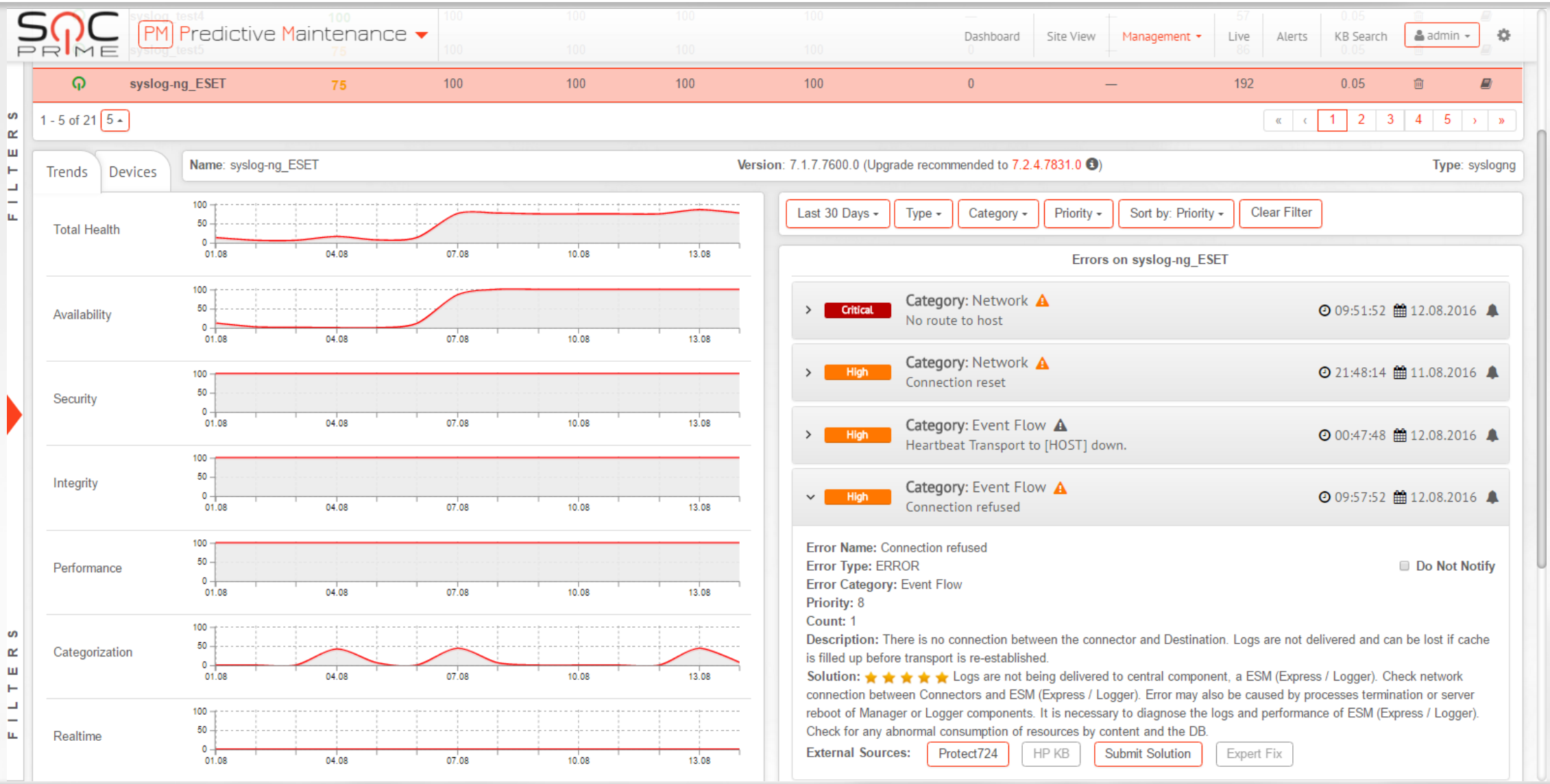
SOC PRIME
POWER ON SECURITY

Комплексная диагностика

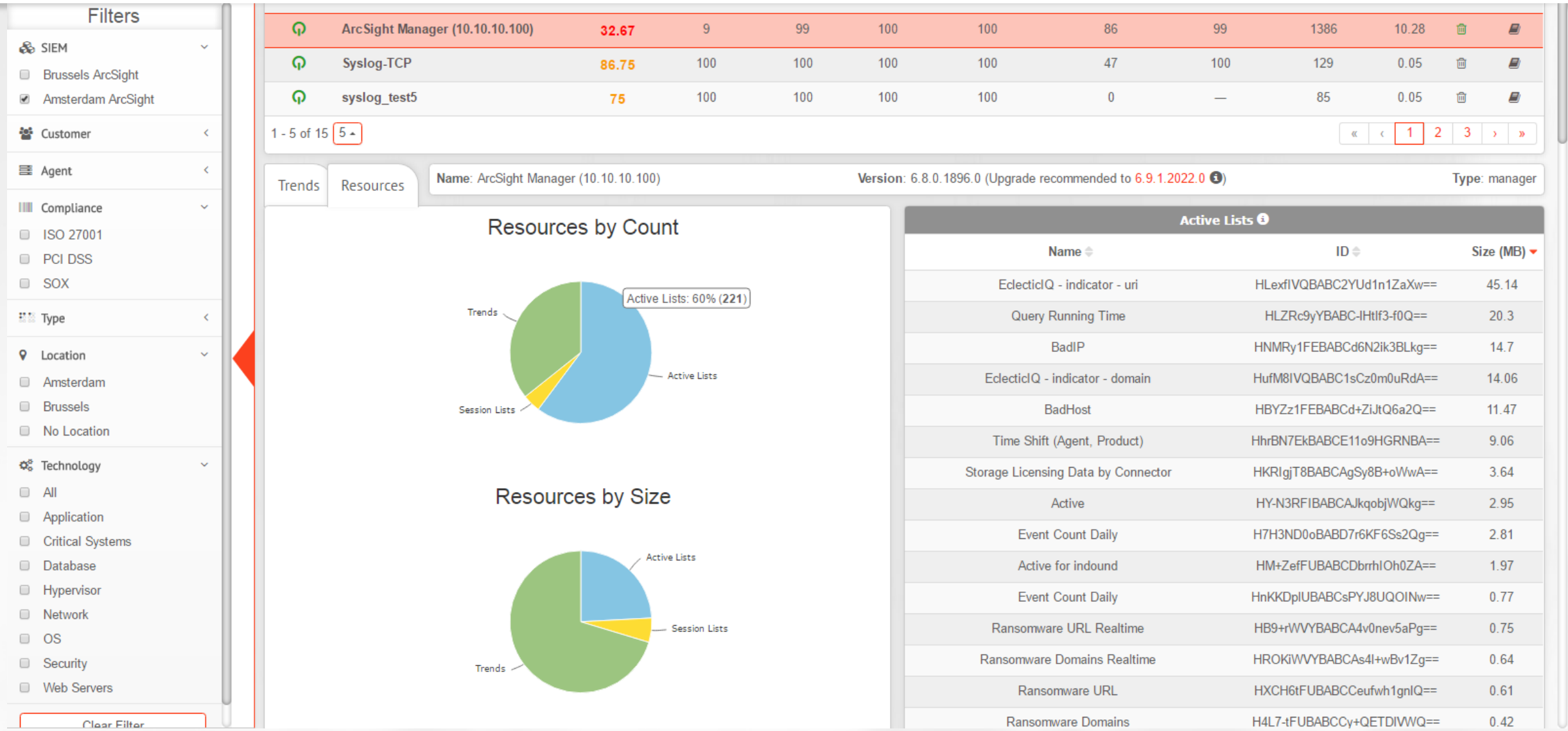


SOC PRIME
POWER ON SECURITY

Вся информация о здоровье с описанием



Отслеживание потребления ресурсов ESM



Predictive Maintenance: сохранит время для более важных дел!

Берегите себя!

sales@socprime.com