

ФУНКЦИОНАЛЬНЫЕ ВОЗМОЖНОСТИ СОВРЕМЕННЫХ SIEM-СИСТЕМ

Чехарин Родион
Руководитель проектов
АО «ДиалогНаука»

О компании «ДиалогНаука»

- Создано в 1992 году СП «Диалог» и Вычислительным центром РАН
- Первыми и самыми известными отечественными продуктами, поставляемыми компанией, были ревизор ADinf, Doctor Web и Aidstest
- В настоящее время АО ДиалогНаука является системным интегратором в области информационной безопасности

- Общие сведения о SEM\SIEM ArcSight
- Архитектура сбора событий ArcSight
- ArcSight Quick Flex - быстрое подключение нестандартных источников
- ArcSight Logger - настраиваемое хранение журналов, быстрый поиск, отчёты и оповещения
- ArcSight ESM - модель сети, модель пользователя, корреляция - правила, реагирование, динамические списки
- Взаимодействие Logger и ESM
- ArcSight Marketplace - «кубики» для SIEM

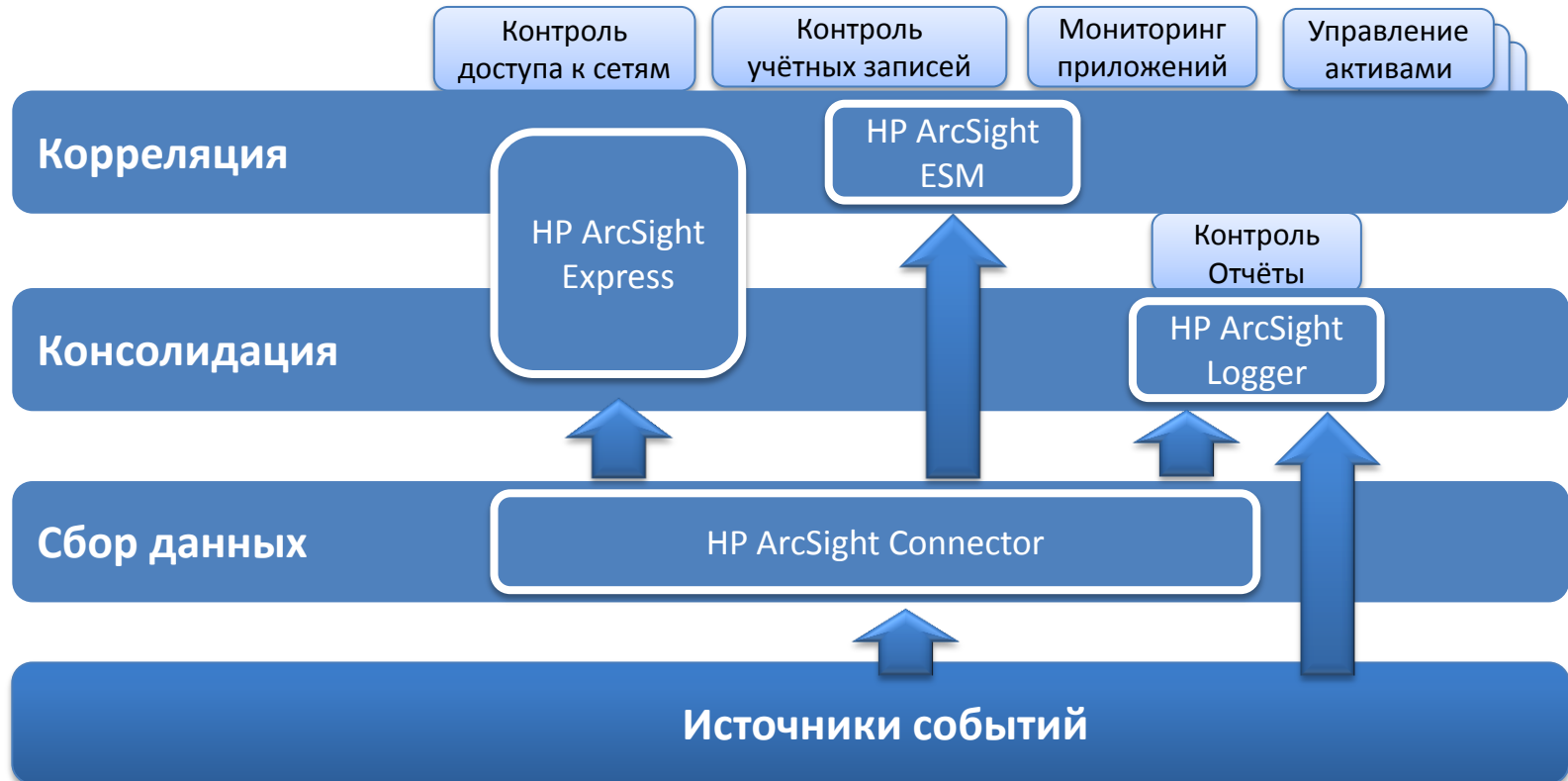
ОБЩИЕ СВЕДЕНИЯ О СИЕМ

- LMS "Система управления журналами" (Log Management System) – централизованная система сбора и хранения событий, предоставляющая единый интерфейс доступа к поученным и хранимым данным.
- SLM /SEM "Система управления событиями\журналами ИБ" (Security Log/Event Management) - по сути система управления журналами событий, но с минимальным анализом данных.
- SIM "Управление данными ИБ" - система управления активами, ориентированная на ИБ. Содержит сведения об уязвимостях хостов, результаты антивирусных сканирований и т.д.
- SEC "Корреляция событий ИБ" (Security Event Correlation) - Система для поиска и выявления шаблонов повторяющихся действий в журналах событий ИБ.
- SIEM "Система управления информационной безопасностью" (Security Information and Event Management) - Система, включающая в себя возможности всех перечисленных систем, предназначенная для централизованного управления событиями и данными ИБ.

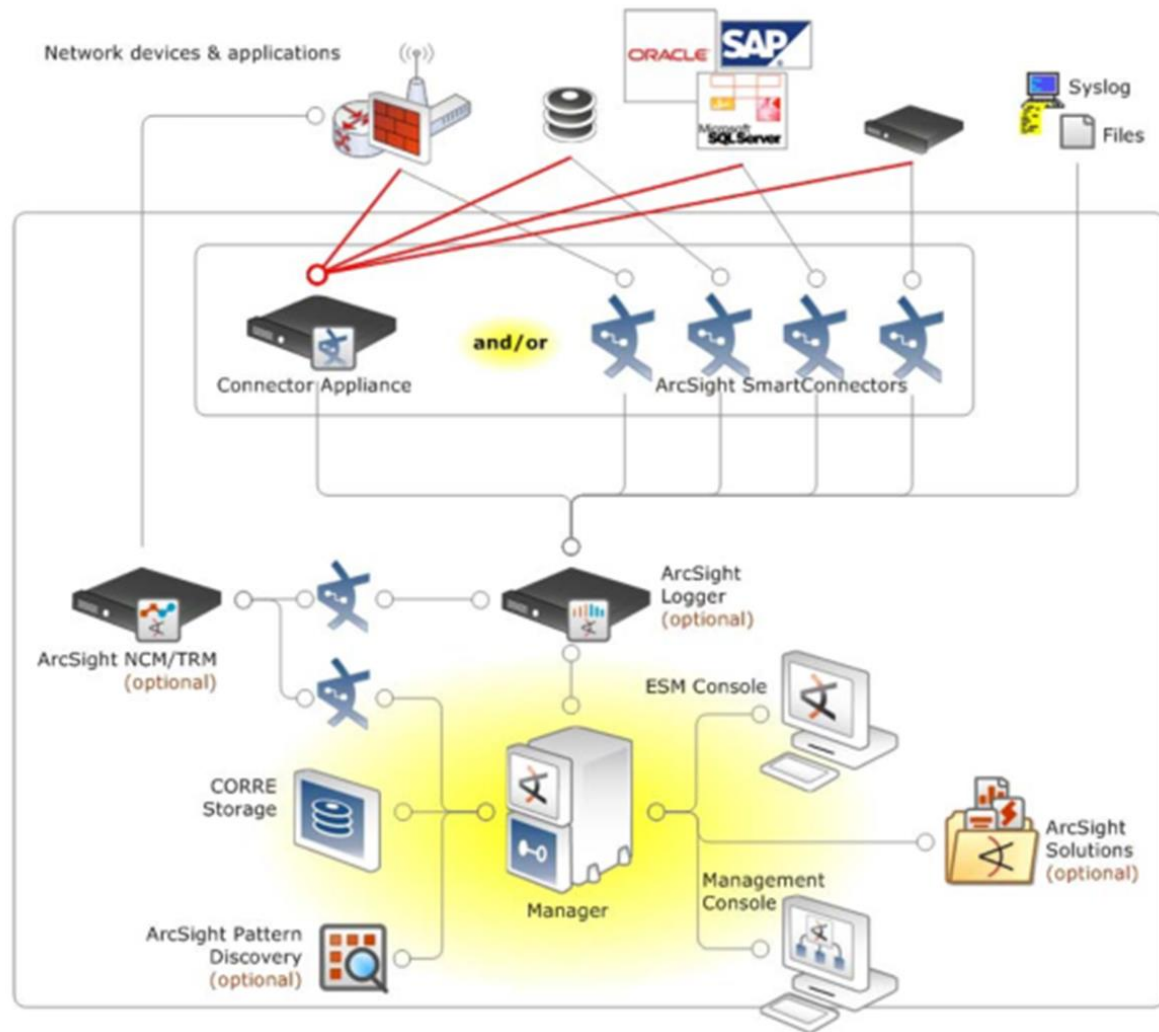
ОСНОВНЫЕ ТРЕБОВАНИЯ К SIEM СИСТЕМАМ

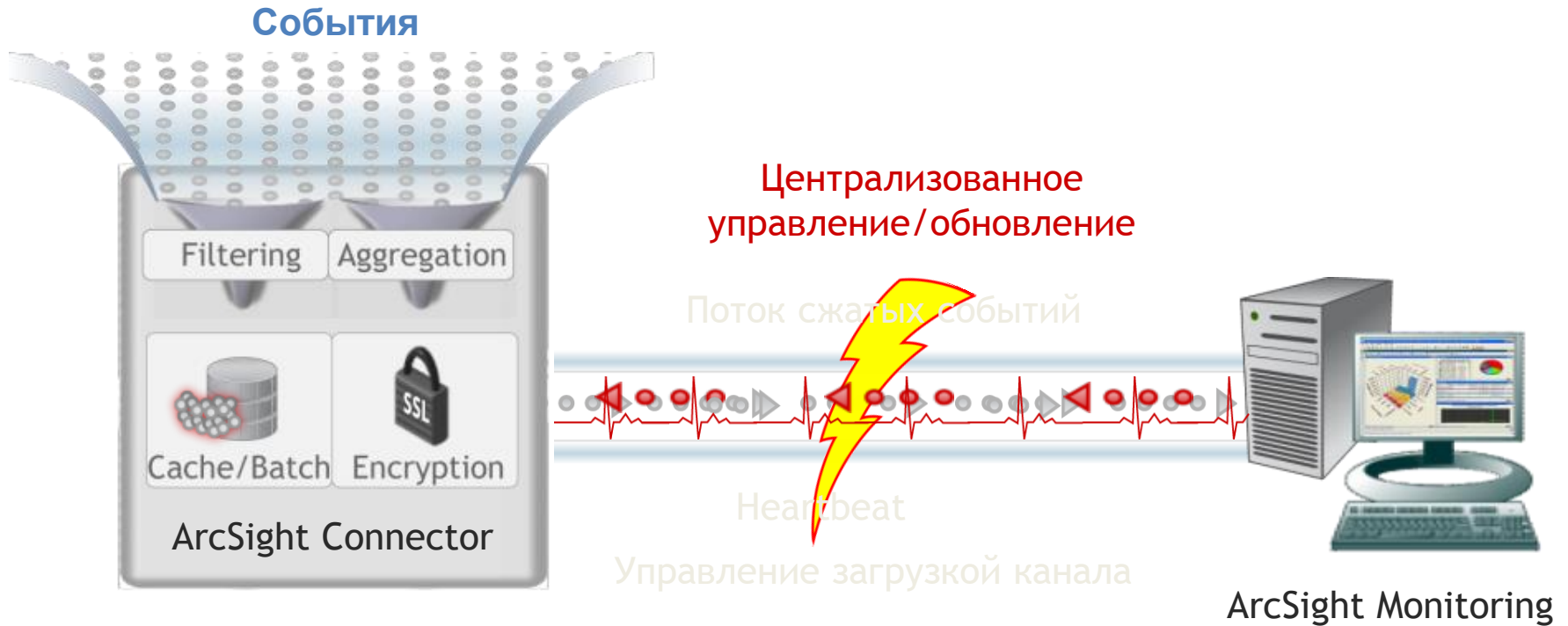
1. Сбор событий и получение сведений и контексте событий
2. Нормализация полученных данных
3. Корреляция
4. Приоритезация
5. Оповещения
6. Отчетность и визуализация
7. Документооборот

Семейство продуктов HP ArcSight



Потоки данных





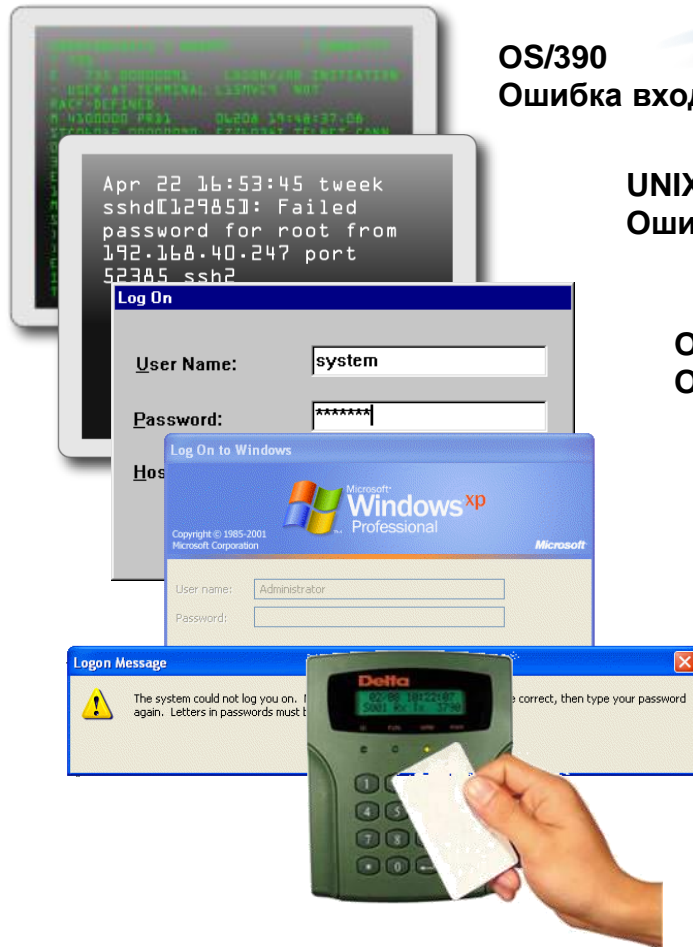
Оригинал...

```
Mar 17 2017 12:16:03: %PIX-6-106015: Deny TCP (no connection) from
10.50.215.102/15605 to 204.110.227.16/443 flags FIN ACK on interface outside
Mar 17 2017 14:53:16 drop gw.foobar.com >eth0 product VPN-1 & Firewall-1 src
xxx.xxx.146.12 s_port 2523 dst xxx.xxx.10.2 service ms-sql-m proto udp rule 49
```

Результат

Time (Event Time)	name	Device Vendor	deviceProduct	Category Behavior	Category DeviceGroup	Category Outcome	Category Significance
3/17/2017 12:16:03	Deny	Cisco	PIX	/Access	/Firewall	/Failure	/Informational/Warning
3/17/2017 14:53:16	Drop	Checkpoint	Firewall-1/VPN-1	/Access/Start	/Firewall	/Failure	/Informational/Warning

Выгода: Быстрый анализ и поиск независимо от производителя источника событий



OS/390
Ошибка входа

UNIX
Ошибка входа

Oracle
Ошибка входа

Windows
Ошибка входа

HID-карты
Вход запрещён

The image shows a security event log interface with multiple event details windows. The main window displays the following normalized event data:

Name	Value
Event	
Name	Rejected Badge In
Start Time	8 Jul 2008 13:16:53 CDT
End Time	8 Jul 2008 13:16:53 CDT
Aggregated Event Count	1
Correlated Event Count	0
Category	
Category Significance	/Informational/Warning
Category Behavior	/Authentication/Verify
Category Device Group	/Physical Access System
Category Outcome	/Failure
Category Object	/Location
Threat	
Priority	9
Device	
Device Address	10.1.1.253
Device Vendor	PAS
Device Product	Badge Reader
Device Custom	
Device Custom String1.Location	Lobby
Attacker	
Attacker ...	desktop27.ny2.east.arcnet.com
Attacker ...	10.0.113.27
Target	
Target H...	hrweb01.hr.east.arcnet.com
Target A...	172.16.1.10
Device Cust...	

Новый способ создания парсеров для Flex-агентов с возможностями:

- Быстрая разработка
- Корректность
- Гибкость
- Упрощение обслуживания и сопровождения
- Снижения порогового уровня для начала работы

Quick Flex Parser Tool представляет следующие возможности для анализа файлов:

- Подсветка текста сообщений в окнах `Base Regex` и `Token Filter Manager` для оценки правильности разбора сообщения токенами
- Подсветка текста сообщений в окне `Log View` для отображения логики разбора сообщения токенами и фильтрами токенов
- Графическая статистика покрытия сообщений созданными токенами в окне `Log View`
- Тестирования работоспособности токенов и детальное описание выявленных ошибок

QuickFlex: начало работы

Quick Flex [Aruba / Mobility Controller / Version: 1] File | Base Regex Editor | Token Filter Editor | Token Manager | Token Filter Manager | Help

Total Logs: **177** Base Parsed: 0 Base Unparsed: **177** Complete: 0 Incomplete: **177** Next Unparsed > Go to # Line number > Search by Log 🔍 Generate Parser ⚙️

#	Total "177" Log Lines	Refresh	Matched Token Filters
1	Oct 21 07:43:48 172.16.0.254 aaa[452]: <125022> <WARN> aaa Authentication failed for User admin, Logged in from 172.16.0.87 port 20817, Connecting to 172.16.0.254 port 4343 connection type HT...	🔄	0
2	Oct 21 07:43:53 172.16.0.254 aaa[452]: <125024> <NOTI> aaa Authentication Succeeded for User admin, Logged in from 172.16.0.87 port 20818, Connecting to 172.16.0.254 port 4343 connection typ...	🔄	0
3	Oct 28 02:19:07 172.16.0.254 aaa[452]: <125025> <INFO> aaa Radius Authentication is disabled	🔄	0
4	Oct 28 02:19:07 172.16.0.254 aaa[452]: <125032> <NOTI> aaa Authentication Succeeded for User admin, Logged in from 172.16.0.87 port 13875, Connecting to 172.16.0.254 port 22 connection type S...	🔄	0
5	Oct 17 08:40:03 172.16.0.254 authmgr[486]: <132023> <ERRS> authmgr 802.1x authentication is disabled in profile Station 00:0c:f1:28:99:60 00:0b:86:aaa8:70	🔄	0
6	Oct 17 08:40:03 172.16.0.254 authmgr[486]: <132030> <ERRS> authmgr Dropping EAPOL packet sent by Station 00:0c:f1:28:99:60 00:0b:86:aaa8:70	🔄	0

Base Regex Token Filter

Token Filter Coverage

177 Total

No Token Filter Match 177

Token Filter Stats

No Data Available

Hewlett Packard Enterprise HPE Security Quick Flex v1.0.0 | © 2016 Hewlett Packard Enterprise Company, L.P.

QuickFlex: основное регулярное выражение

The screenshot shows the 'Base Regex Editor' window. At the top, there are menu items: 'Log View', 'Token Filter Editor', 'Token Manager', 'Token Filter Manager', and 'Help'. The main area is divided into two sections:

- Raw Log:** Contains a log line: "Oct 21 07:43:48 172.16.0.254 aaa[452]: <125022> <WARN> |aaa| Authentication failed for User admin, Logged in from 172.16.0.87 port 20817, Connecting to 172.16.0.254 port 4343 connection type HTTPS". A status indicator at the top right says "Valid Regex and Matched entire Log Line" with a green checkmark.
- Base Regex:** Contains a complex regular expression: `(?:\d{4}\s+)?(?:\[?(\[w\J*\.[w\J]*)\]?)?s*(?:\[^\[\]]+\(?:\[[0-9a-fA-F][0-9a-fA-F]\;]{5}[0-9a-fA-F][0-9a-fA-F]@\d+\.\d+\.\d+\.\d+.*?@\d+\.\d+\.\d+\.\d+)\)?\[(\d{1,4})\]:\s*<(\d{5,6})>\s*<(DEBUG|INFO|NOTICE|WARN|ERR|SICRITIALRT)>\s*(?:\s*(?:\[^\[\]]*\s*)\D)?(?:\s*<?:\s+)\s+(?:\d+\.\d+\.\d+\.\d+)\s+>)\s+(.*)`

At the bottom, there is a note: "(*): The regex must be valid and match the entire log line." and three buttons: "Matching details", "Tokenize", and "Save".

QuickFlex: этапы работы

List of New Tokens Used in Base Regex

1. Token0 ((\w\j*\.[\w\j]*)
2. Token1 ([^\[\]\+)
3. Token2 ((?:[0-9a-fA-F][0-9a-fA-F])\{5\}[0-9a-fA-F][0-9a-fA-F]@\d+\.\d+\.\d+\.\d+.*@\d+\.\d+\.\d+\.\d+)
4. Token3 (\d{1,4})
5. Token4 (\d{5,6})
6. Token5 (DEBUG|INFO|NOTI|WARN|ERR|SICRITIAL|RT)
7. Token6 ([^\|]*)
8. Token7 (*)

Cancel **Save**

Base Regex Editor

Log View Token Filter Editor Token Manager Token Filter Manager Help

Matching details Tokenize **Save**

Message ID Token Token0 Message Token Token0 Data Capturing Setting Additional Data

Base Token List

- Token0 ((\w\j*\.[\w\j]*)
- Token1 ([^\[\]\+)
- Token2 ((?:[0-9a-fA-F][0-9a-fA-F])\{5\}[0-9a-fA-F][0-9a-fA-F]@\d+\.\d+\.\d+\.\d+.*@\d+\.\d+\.\d+\.\d+)

Token Details

Token Name * Hostname

Type

Regex ((\w\j*\.[\w\j]*)

Description

Assignment

Save Token

Mapping List

+ New X Delete

Assignment *	Device Process Name	Description	Operation	Arguments *	Process
event.deviceProcessName			None	Operation: None	Arguments: token_name

Save Mapping

Flex-агент: дополнительные возможности

- Обработка событий, состоящих из нескольких разных строк:

```
Mon 2013-09-16 00:07:38: -----
Mon 2013-09-16 00:10:11: SecurityPlus AntiVirus processing c:\mdaemon\queues\local\md50003493074.msg...
Mon 2013-09-16 00:10:11: * Message return-path: bushurovavn@baltech.ru
Mon 2013-09-16 00:10:11: * Message from: bushurovavn@baltech.ru
Mon 2013-09-16 00:10:11: * Message to: moskin.a@comp.ru
Mon 2013-09-16 00:10:11: * Message subject: Компания "Балтех" Новый курс "Трибодиагностика. Основы смазывания машин и оборудования."
Mon 2013-09-16 00:10:11: * Message ID: <d041a922-1e42-11e3-fc8c-001e8c490aad@tgci.ru>
Mon 2013-09-16 00:10:11: Start SecurityPlus AntiVirus results
Mon 2013-09-16 00:10:11: * Attachment t1.rar is infected by Trojan.Horse.d1
Mon 2013-09-16 00:10:11: * Total attachments scanned      : 6 (including multipart/alternatives and message body)
Mon 2013-09-16 00:10:11: * Total attachments infected      : 1
Mon 2013-09-16 00:10:11: * Total attachments disinfected: 1
Mon 2013-09-16 00:10:11: * Total errors while scanning    : 0
Mon 2013-09-16 00:10:11: * Total attachments removed     : 0
Mon 2013-09-16 00:10:11: End of SecurityPlus AntiVirus results
Mon 2013-09-16 00:10:11: -----
```

- Получение данных об одном событии из разных строк журнала:

```
[18/Jul/2005:12:30:20 -0400] conn=8 op=0 msgId=82 - BIND uid=admin
[18/Jul/2005:12:30:25 -0400] conn=7 op=-1 msgId=-1 - LDAP connection from 10.0.20.122
to 10.0.20.122
[18/Jul/2005:12:30:30 -0400] conn=8 op=0 msgId=82 - RESULT err=0
```

Flex-агент: дополнительные возможности

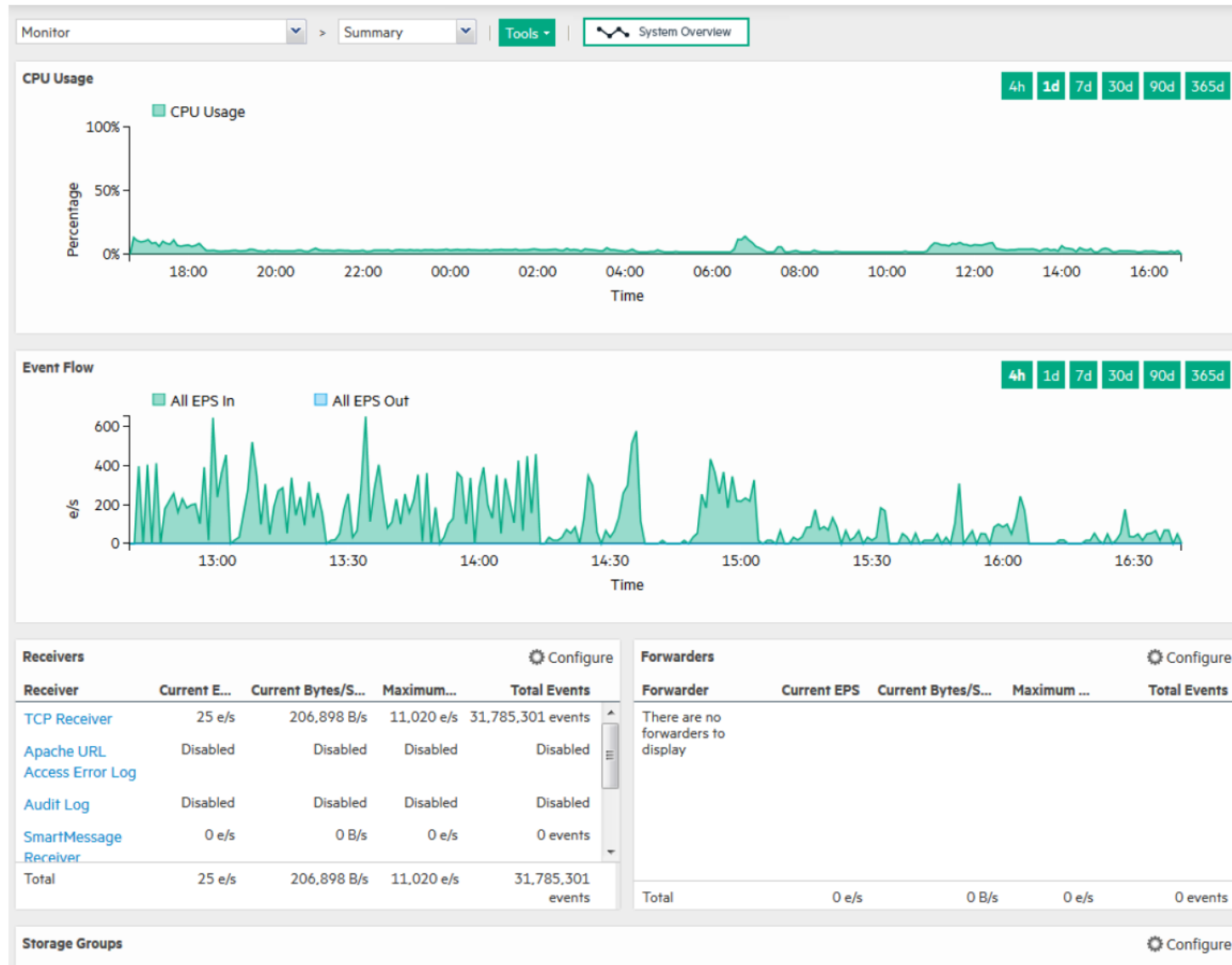
- Запрос данных из внешних источников:

```
type=sql
field.addr.as.numbers=true
field.getter=oldFileHash
field.setter.count=2
field.setter[0]=targetUserPrivileges
field.setter[1]=oldFilePermission
jdbc.class=org.gjt.mm.mysql.Driver
jdbc.url=jdbc:mysql://localhost:3306/arcsight
jdbc.username=root
jdbc.password=OBFUSCATE.4.0.2:HT1WgEnTJ3sqlCb7jQ3PRA==
jdbc.query=select inn,name,nameshort from "ARCSIGHT"."egr" where inn in (?\u0000?)
```

- Табличное соответствие:

```
event.externalId,event.deviceSeverity,set.event.deviceExternalId,set.event.message,set.event.priority,set.event.deviceFacility,
553,Audit_success,WN_03S_0553S,Обнаружена атака с повторением пакетов,6,Access,PCIDSS10
672,Audit_failure,WN_03S_0672F,Неудачная попытка выдачи билета проверки подлинности,4,Access,PCIDSS10
672,Audit_success,WN_03S_0672S,Выдан билет проверки подлинности,2,Access,PCIDSS10
673,Audit_failure,WN_03S_0673F,Неудачная попытка выдачи билета службы,4,Access,PCIDSS10
673,Audit_success,WN_03S_0673S,Удачная попытка выдачи билета службы,2,Access,PCIDSS10
674,Audit_success,WN_03S_0674S,Выданный билет обновлен,2,Access,PCIDSS10
675,Audit_failure,WN_03S_0675F,Ошибка предварительной проверки,4,Access,PCIDSS10
678,Audit_success,WN_03S_0678S,Учетная запись сопоставлена для входа в систему,2,Access,PCIDSS10
679,Audit_failure,WN_03S_0679F,УЗ не удалось сопоставить для входа в систему,4,Access,PCIDSS10
680,Audit_failure,WN_03S_0680F,Контроллер домена неудачно пытался проверить данные для входа в аккаунт ,4,Access,PCIDSS10
680,Audit_success,WN_03S_0680S,Контроллер домена удачно пытался проверить данные для входа в аккаунт,2,Access,PCIDSS10
682,Audit_success,WN_03S_0682S,Сеанс переподключен к станции,2,Access,PCIDSS10
683,Audit_success,WN_03S_0683S,Сеанс отключен от станции ,2,Access,PCIDSS10
640,Audit_success,WN_03S_0640S,Изменение общей базы данных УЗ ,2,Account,PCIDSS8
643,Audit_success,WN_03S_0643S,Изменение политики для домена,6,Privileges,PCIDSS7
```

Хранение и поиск: ArcSight Logger



Хранение и поиск: ArcSight Logger

The screenshot displays the ArcSight Logger web interface. At the top, there is a navigation bar with tabs for Summary, Analyze, Dashboards, Reports, Configuration, and System Admin. The current view is the 'Analyze' section, showing a search filter for 'Logger and deviceEventClassId = memory:100' and a time range of 'Current week'. A bar chart shows 7,455 events scanned over a 24-hour period. Below the chart is a table of event details with columns for Time (Event Time) and a list of 9 events.

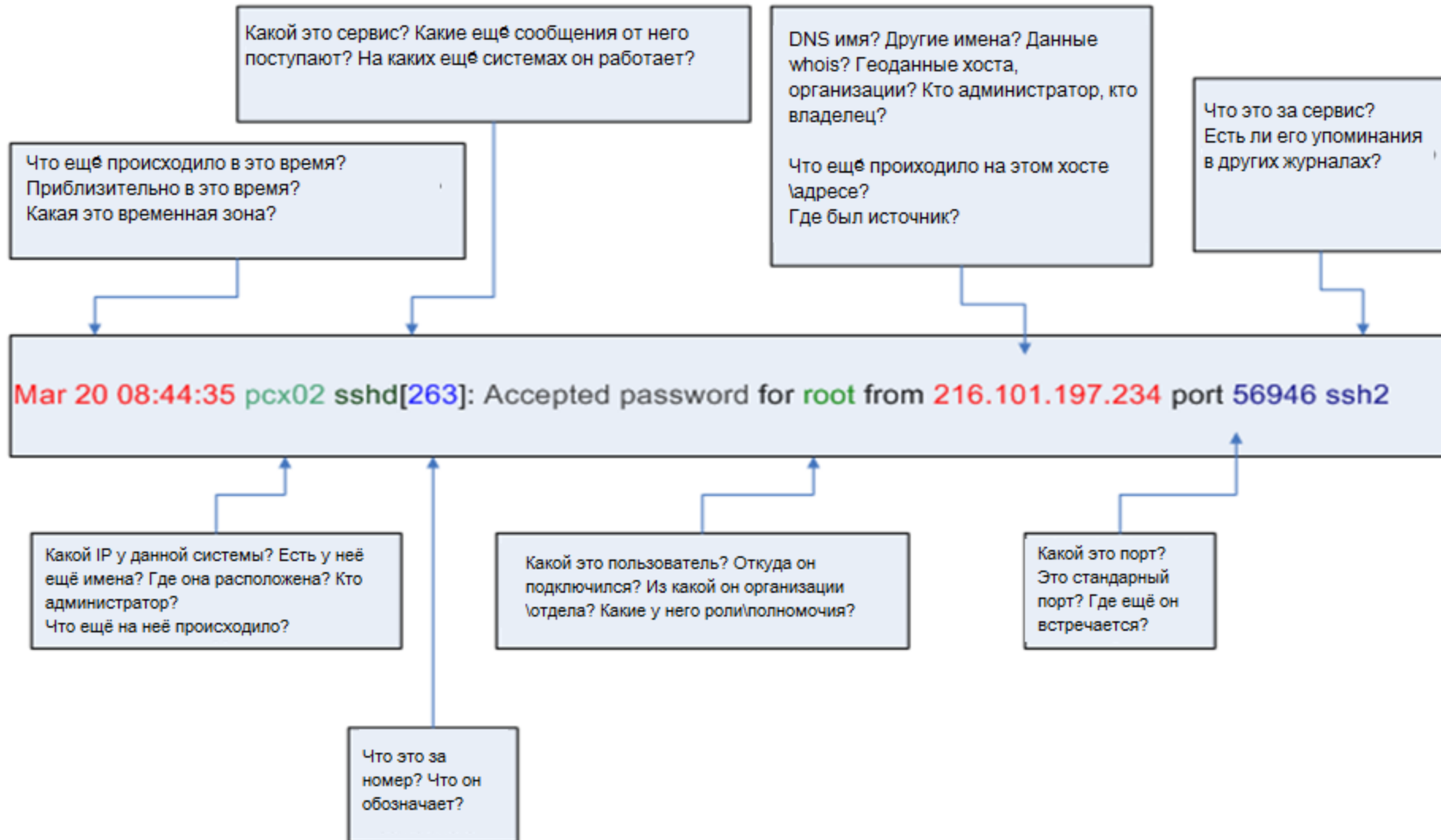
The main area shows a search for 'Logger | chart count by name' with a 'Go!' button. Below this, a bar chart displays 27 events scanned, with a chart showing counts for CPU Usage, Disk Space Remaining, and Disk bytes read. A tree view on the right lists various system components like Anti-Virus, CrossDevice, Database, Firewall, etc.

At the bottom, a table lists event names and their counts:

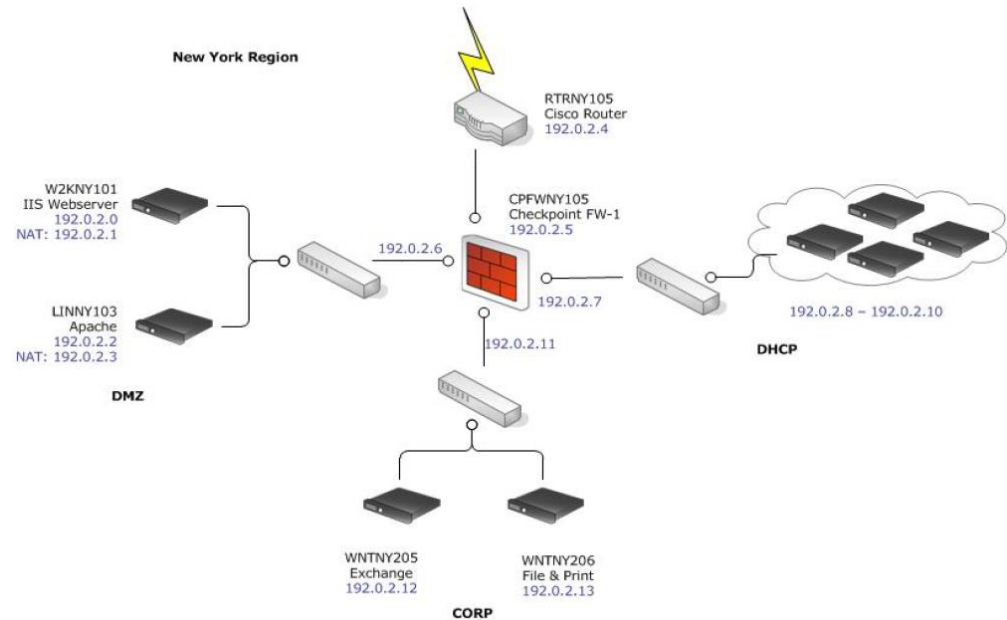
name	_count
Root Disk Space Remaining	1
Storage Group Space Used	64
Successful login	1
TCP_CLIENT_REFRESH	1

On the right side, there are 'Chart Settings' and 'Actions' panels. The 'Actions' panel includes options like 'Quick Run with default options', 'Run In Background', 'Run Report', 'List Published Outputs', 'Create Dashboard Widget', 'Customize Report', 'Copy Report', 'Copy Report as Link', 'Cut Report', 'Download Report', 'View Description', 'Add to Favorites', and 'Delete Report'. The 'Properties' panel shows details for 'Top Infected Systems', including Name, Type (Adhoc), and Format (HTML).

Вопросы, вопросы...



Сетевая модель



Модель пользователя

Сопоставление

Кто стоит за данным логином?

Политики

Каково влияние события на бизнес?

Роль

Соответствует ли активность роли сотруднику?

Профиль пользователя

С чем обычно работает данный пользователь?

The screenshot shows the 'Inspect/Edit' window for 'Actor:User1'. It displays various attributes and account information.

Actor	
* U U I D	User1
* Full Name	User1
First Name	Иванов
Last Name	Иван
Middle Initial	Федотович
IDM Identifier	
D N	
Employee Type	Штат
Status	
Title	Ведущий экономист
Company	
Org	
Department	Отдел анализа финансовых показателей
Manager	Сидоров И.Е.

(Name)
(Description)

Account Attributes	
Authenticator	Account ID
Oracle	user1
ABS	I.Ivanov
Docs	Ivanov.fin
Windows	IvanovIF

Role Attributes		
Role Name	Resource Name	Role Type
Analist	ABS	User

Модель пользователя \ модель ресурса \ сетевая МОДЕЛЬ

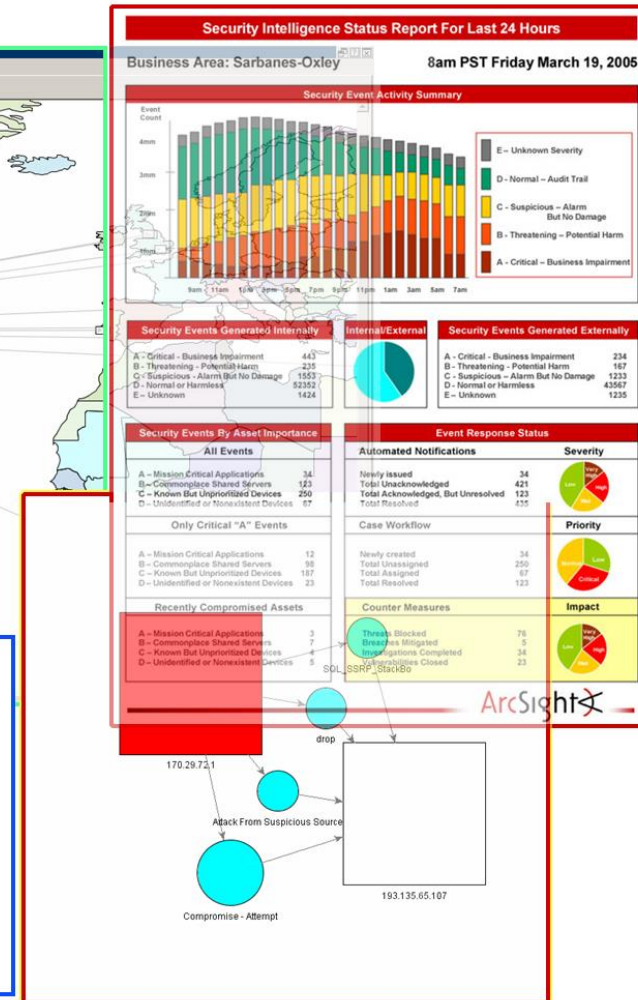
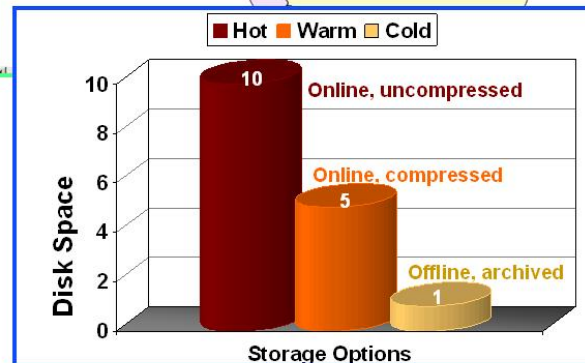
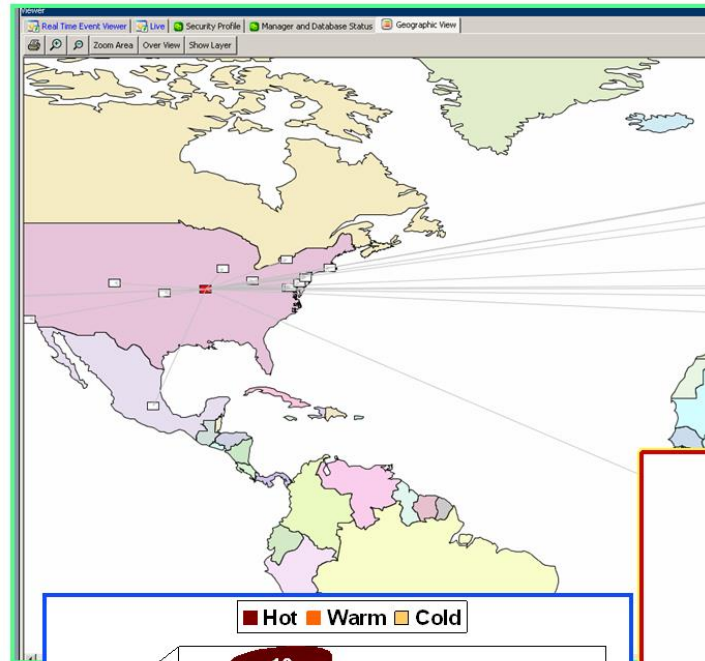
Модель ресурса



The screenshot displays a network management interface with the following sections:

- Asset Details:** Shows attributes for an asset with Name 10.31.38.12 - MAIL01, IP Address 10.31.38.12, MAC Address 00:50:56:a7:05:55, and Host Name MAIL01.
- Local Asset Categories:** A list of categories including Wireshark 1.10.0 (64-bit), Microsoft Exchange Client Language Pack, Microsoft Pragmatic General Multicast, VMware Tools, and Microsoft Office Proof (English) 2010.
- Vulnerabilities:** A list of CVE identifiers such as CVE-2005-1794, CVE-2009-0217, CVE-2009-1532, CVE-2009-1917, CVE-2009-1918, CVE-2009-1919, CVE-2009-2510, CVE-2009-2511, CVE-2009-3555, CVE-2009-3671, CVE-2009-3673, CVE-2009-3674, CVE-2009-3676, CVE-2009-3678, CVE-2009-4074, CVE-2010-0017, CVE-2010-0018, CVE-2010-0020, CVE-2010-0021, and CVE-2010-0022.

- Интерфейс реального времени с географическим расположением объектов и представлением отклонений в параметрах безопасности
- Отображение событий по подразделениям или устройствам
- Выбор между опасностью события или его категорией
- Интуитивно понятный инструментальный интерфейс для подготовки табличных и графических отчетов о безопасности или показ карты нарушений безопасности



The screenshot displays the ArcSight Console interface with several active windows:

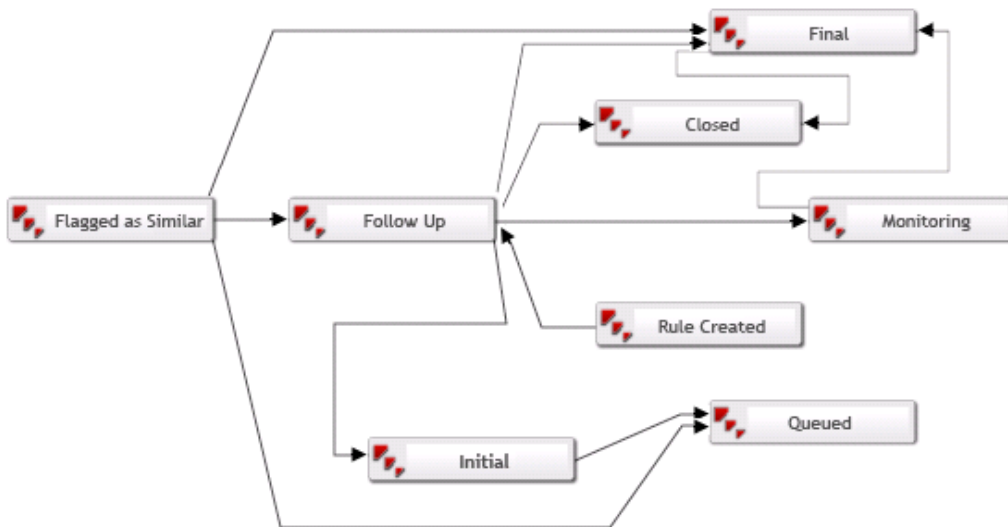
- Section 11 Overview:** Shows a 'Violation' status with a red arrow icon.
- Rules Attackers and Targets:** A network diagram showing nodes and connections. A large blue square highlights a central node.
- Last 20 Rules Fired:** A list of rules with their names and counts.
- Top 20 Rules Fired:** A table showing the most frequent rules.
- Top 20 Targets in Rule Firings:** A bar chart showing the number of firings for various target addresses.
- Information Systems:** A network diagram showing various systems and their relationships.

Name
Same User Using Different User Names to Log-on
Same User Using Different User Names to Log-on
Same User Using Different User Names to Log-on
Same User Using Different User Names to Log-on
Same User Using Different User Names to Log-on
User Logged in from Two Locations
Same User Using Different User Names to Log-on
Same User Using Different User Names to Log-on
Same User Using Different User Names to Log-on
User Logged in from Two Locations
Same User Using Different User Names to Log-on
Same User Using Different User Names to Log-on
User Logged in from Two Locations
Same User Using Different User Names to Log-on
User Logged in from Two Locations
Same User Using Different User Names to Log-on
User Account Deletion
Access Rights Removed

Name	Total
Malicious Code Detected	83
Application Brute Force Logins	2
Vulnerabilities Found in Information System	1
Successful Attack - Brute Force	1

Target Address	Total
Unknown	13021
10.0.112.203	400
192.91.254.205	300
192.91.254.209	200
192.91.254.201	200
10.0.112.211	200
10.0.112.205	200
10.0.112.207	100
10.0.112.213	100

- Этапы: обработка инцидентов в соответствии с заранее заданным, предназначенном для совместной работы процессом
- Аннотирование инцидентов для более полного анализа
- Интеграция со сторонними системами документооборота



Stage:Final

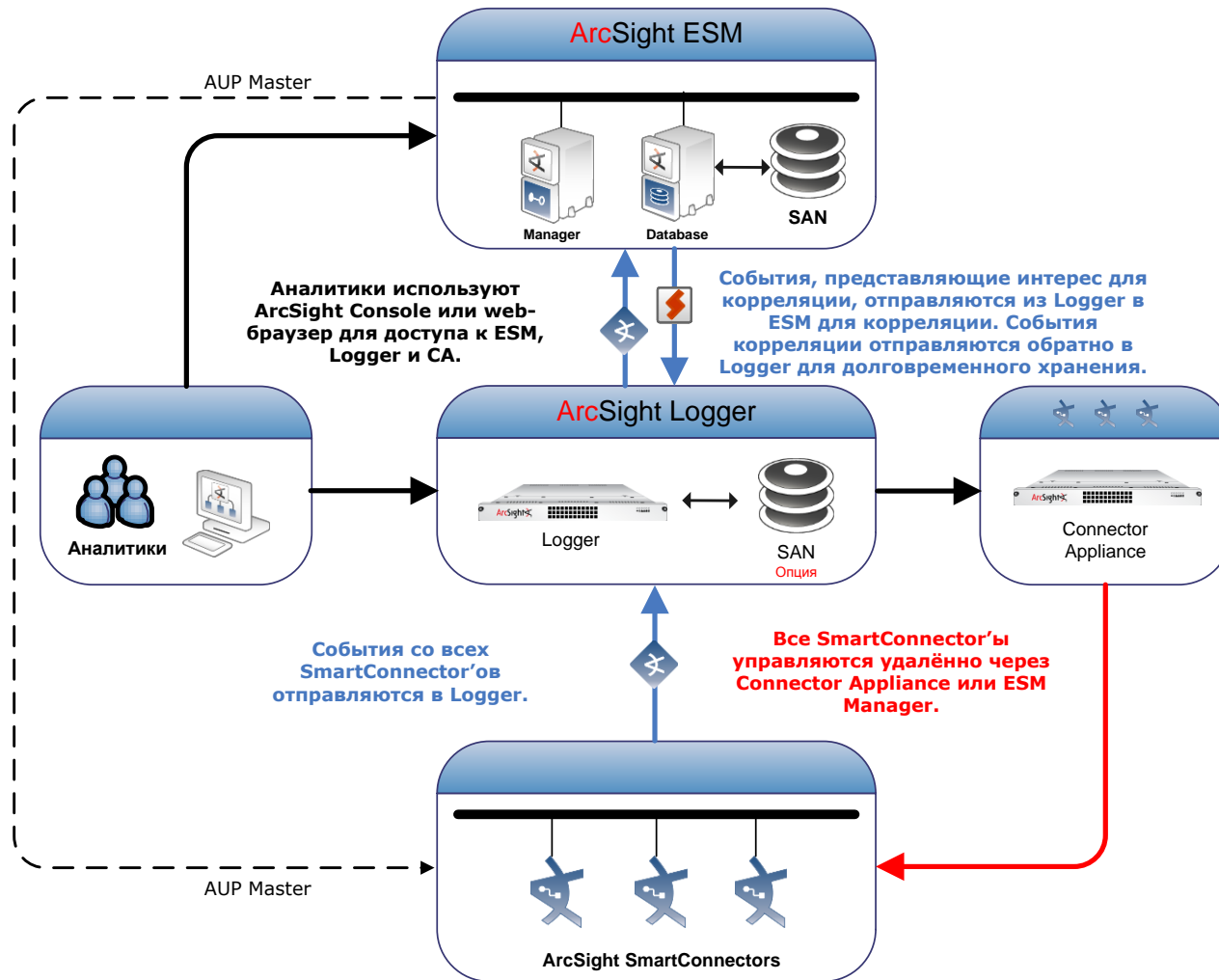
Attributes | Notes

Stage	
Name	Final
Subsequent Stages	Closed
User required	<input checked="" type="checkbox"/>
Comment required	<input type="checkbox"/>
Can be skipped	<input checked="" type="checkbox"/>
Mark Similar	
Mark similar required	<input type="checkbox"/>
Mark Similar Stage	Final
Configuration flags	
Hidden:	True
Closed:	False
Common	
Resource ID	Rq8HINfoAABCA5cxbPIxG0g==
External ID	
Alias	
Description	Investigation has concluded
Version ID	AAAAA11Jgu9tyJ3v
Deprecated	<input type="checkbox"/>
Assign	
Owner	
Notification Groups	
Parent Groups	
All Stages	/All Stages/
+ Creation Information	
+ Last Update Information	
Creation Information	

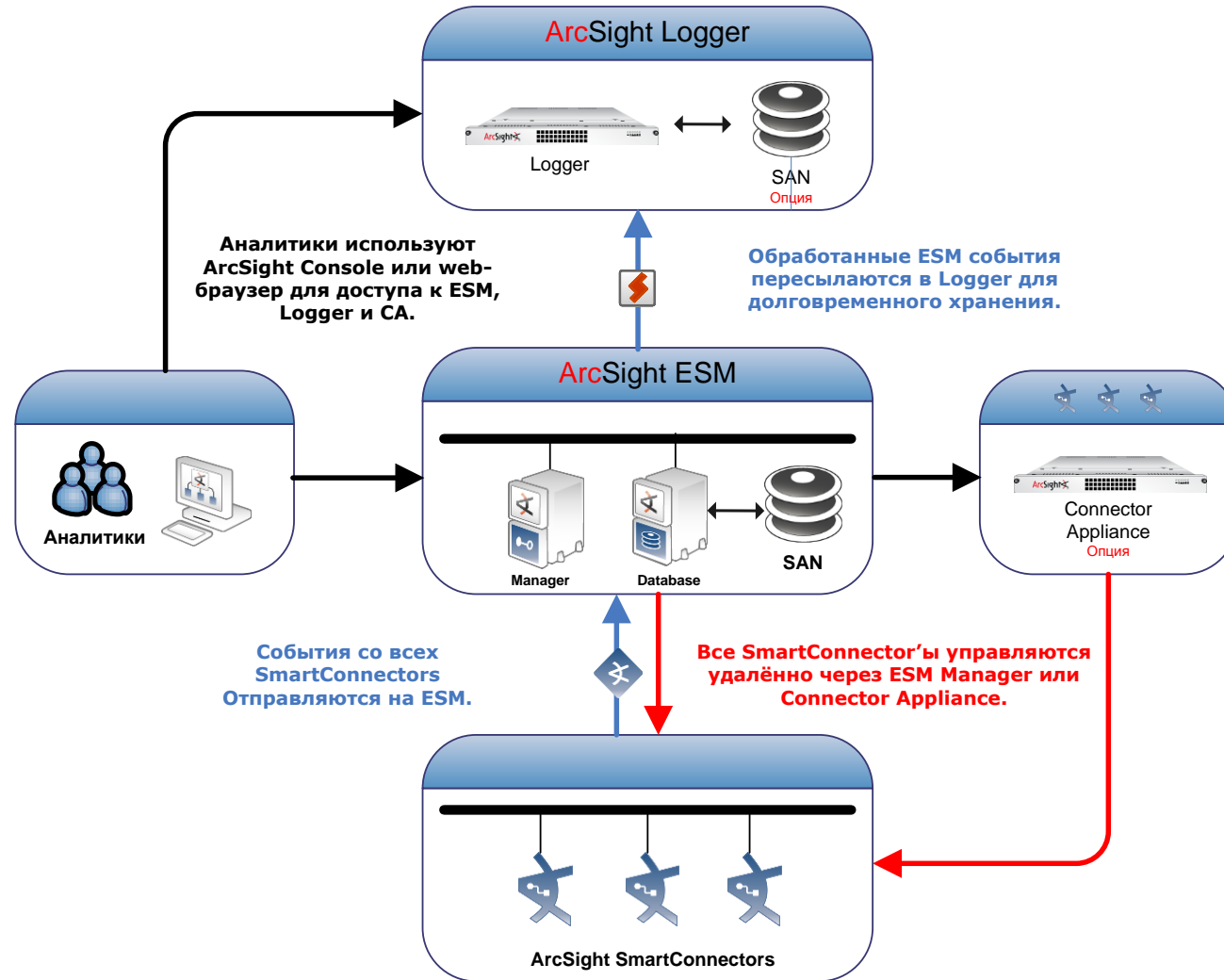
OK Cancel Apply Help

- Соответствие стандартам
 - PCI DSS
 - HIPAA...
- Автоматизация и интеграция
 - Threat Detector
 - User Behavior Analytics
 - System Monitoring
 - Reputation Security Monitor
 - Domain Name System Malware Analytics

ESM + Logger



Logger + ESM



- Пакеты правил\фильтров
- Нестандартные агенты
- Интеграция со сторонними системами
- Дополнительные утилиты

Browse by category



Activate Packages

→ View 29 items



Activate Product Packages

→ View 16 items



Classic Packages

→ View 8 items



SmartConnectors

→ View 1 item



Partner Integrations

→ View 61 items



Products

→ View 11 items



Resource Center

→ View 16 items



Utilities and Tools

→ View 10 items



FlexConnectors

→ View 27 items



NEW!



→ View 33 items







All Categories (185)
Partner Integrations (61)
NEW! (33)
Activate Packages (29)
FlexConnectors (27)
Activate Product Packages (16)
Resource Center (16)
Products (11)
Utilities and Tools (10)
Logger (8)
Classic Packages (8)
FalseCONNECT (1)
SmartConnectors (1)

Utilities and Tools

Utilities and Tools

All products ▾ All versions ▾ All companies ▾ [Clear filters](#)

Sort by: **Newest** Downloads A-Z  

<p>HPE FREE</p> <p>IPv4 Internet Dark Zones Update Hewlett Packard Enterprise</p>  <p>↓ 480 ★★★★★</p>	<p>HPE FREE</p> <p>Tool Commands Web App Hewlett Packard Enterprise</p>  <p>↓ 221 ★★★★★</p>	<p>HPE FREE</p> <p>ArcSight Activate Templates Hewlett Packard Enterprise</p>  <p>↓ 173 ★★★★★</p>
<p>HPE FREE</p> <p>Activate Customer Base Template Hewlett Packard Enterprise</p> <p>NEW! Customer Template</p>  <p>↓ 43 ★★★★★</p>	<p>HPE FREE</p> <p>G7 to G9 Migration Tool Hewlett Packard Enterprise</p>  <p>↓ 93 ★★★★★</p>	<p>HPE FREE</p> <p>Activate Package Installation Checker Hewlett Packard Enterprise</p>  <p>↓ 72 ★★★★★</p>

Tel: +7 (495) 980-67-76 доб. 151

Web: www.DialogNauka.ru

E-mail: Rodion.Chekharin@DialogNauka.ru

117105, г. Москва, ул. Нагатинская, д.1