

ФУНКЦИОНАЛЬНЫЕ ВОЗМОЖНОСТИ СОВРЕМЕННЫХ SIEM-СИСТЕМ

Чехарин Родион
Руководитель проектов
АО «ДиалогНаука»

О КОМПАНИИ «ДИАЛОГНАУКА»

Создана в 1992 году СП «Диалог» и ВЦ РАН

Первыми и самыми известными отечественными продуктами, поставляемыми компанией, были ревизор ADinf, Doctor Web и Aidstest

В настоящее время ДиалогНаука является системным интегратором в области информационной безопасности

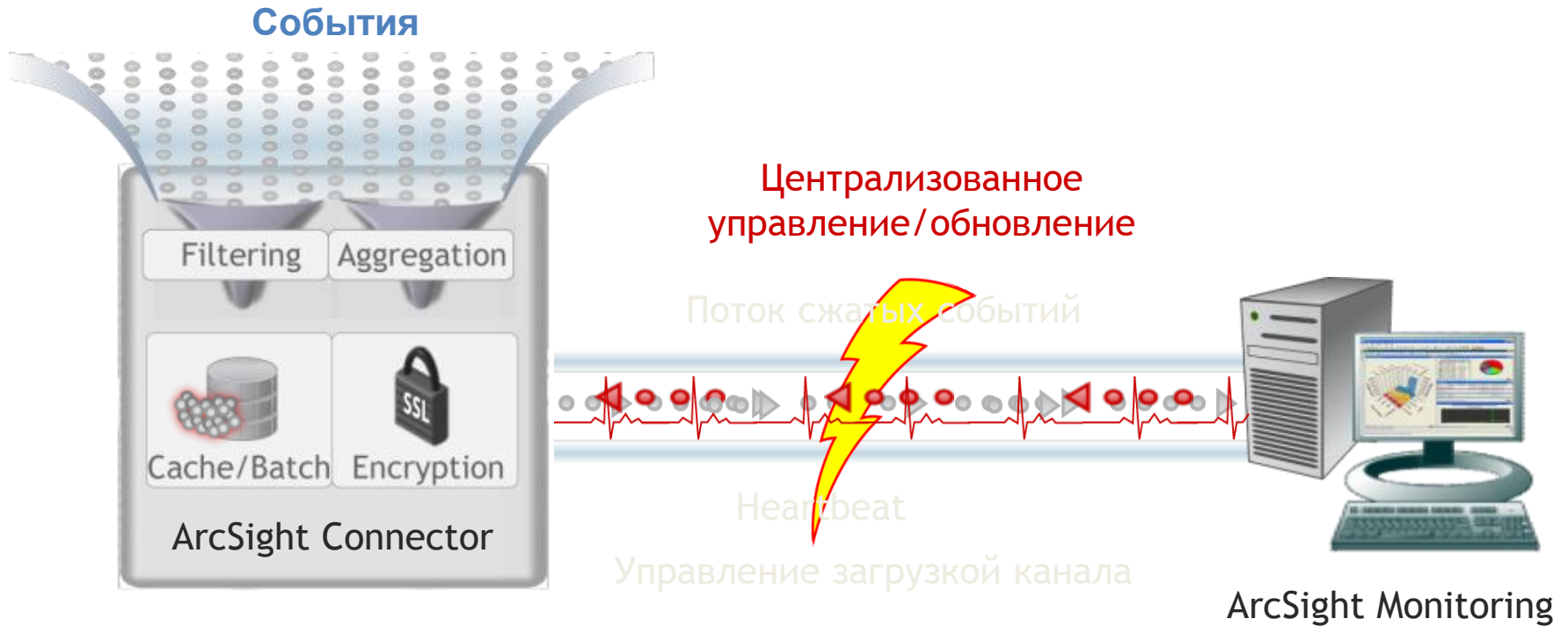
- Общие сведения о SIEM системах
- Основные требования к данным системам
- Функциональность HP ArcSight Logger \ ESM
- Модель пользователя \ модель ресурса \ сетевая модель
- Дополнительные модули
- Базовые примеры использования

- 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

ФУНКЦИОНАЛЬНОСТЬ HP ARCSIGHT



OS/390
Ошибка входа

UNIX
Ошибка входа

Oracle
Ошибка входа

Windows
Ошибка входа

HID-карты
Вход запрещён

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...	

Хранение и поиск: ArcSight Logger

The screenshot displays the ArcSight Logger web interface. At the top, navigation tabs include Summary, Analyze (selected), Dashboards, Reports, Configuration, and System Admin. The top right shows system metrics: EPS In: 0, EPS Out: 0, CPU: 52%, and the user 'admin'.

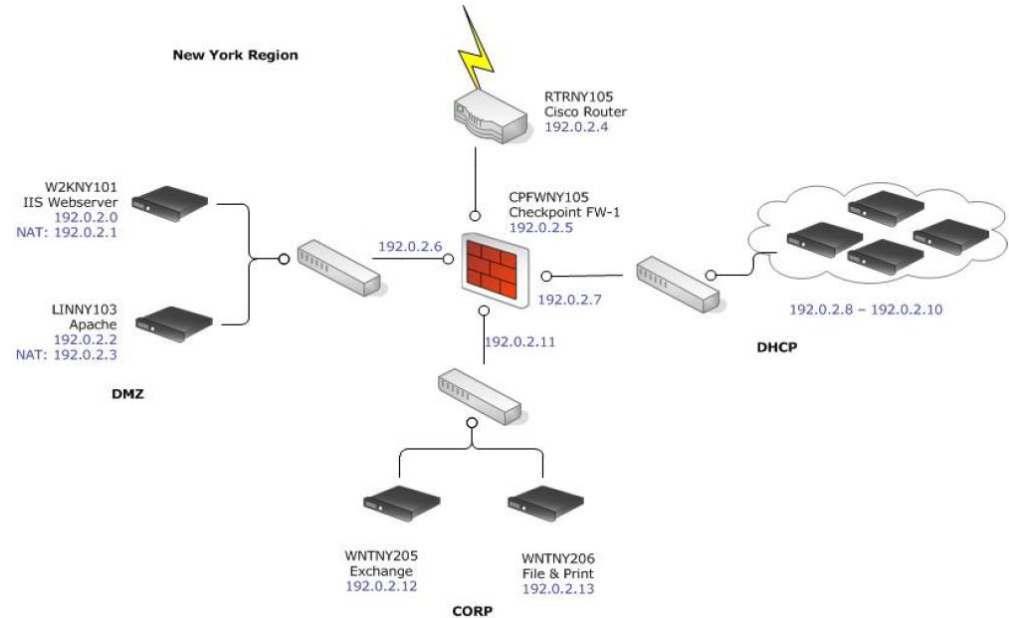
The main interface is divided into two sections. The top section shows a search for "Logger and deviceEventClassId = memory:100" with 7,455 events. A bar chart shows event counts over time from Monday 00:00:00 to Tuesday 00:00:00. Below the chart is a table of selected fields: deviceEventClassId 1, deviceProduct 1, deviceVendor 1, deviceVersion 2, and name 1. A table lists 9 events with their timestamps.

The bottom section shows a search for "Logger | chart count by name" with 27 events. A bar chart displays the count for three categories: CPU Usage (approx. 15), Disk Space Remaining (approx. 5), and Disk bytes read (approx. 25). Below the chart is a table with the following data:

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

On the right side, there is a "Chart Settings" panel with a tree view of categories like Anti-Virus, CrossDevice, Database, Firewall, Identity Management, IDS-IPS, Network, Operating System, VPN, Foundation, and SANS Top 5. A list of actions is provided, including "Failed Anti-Virus Updates", "Top Infected Systems", and "Virus Activity by Hour". A "Properties" section shows details for "Top Infected Systems": Name: Top Infected Systems, Type: Adhoc, Format: HTML.

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 a software interface for inspecting and editing user data. The window title is 'Inspect/Edit'. The main content area is divided into several sections:

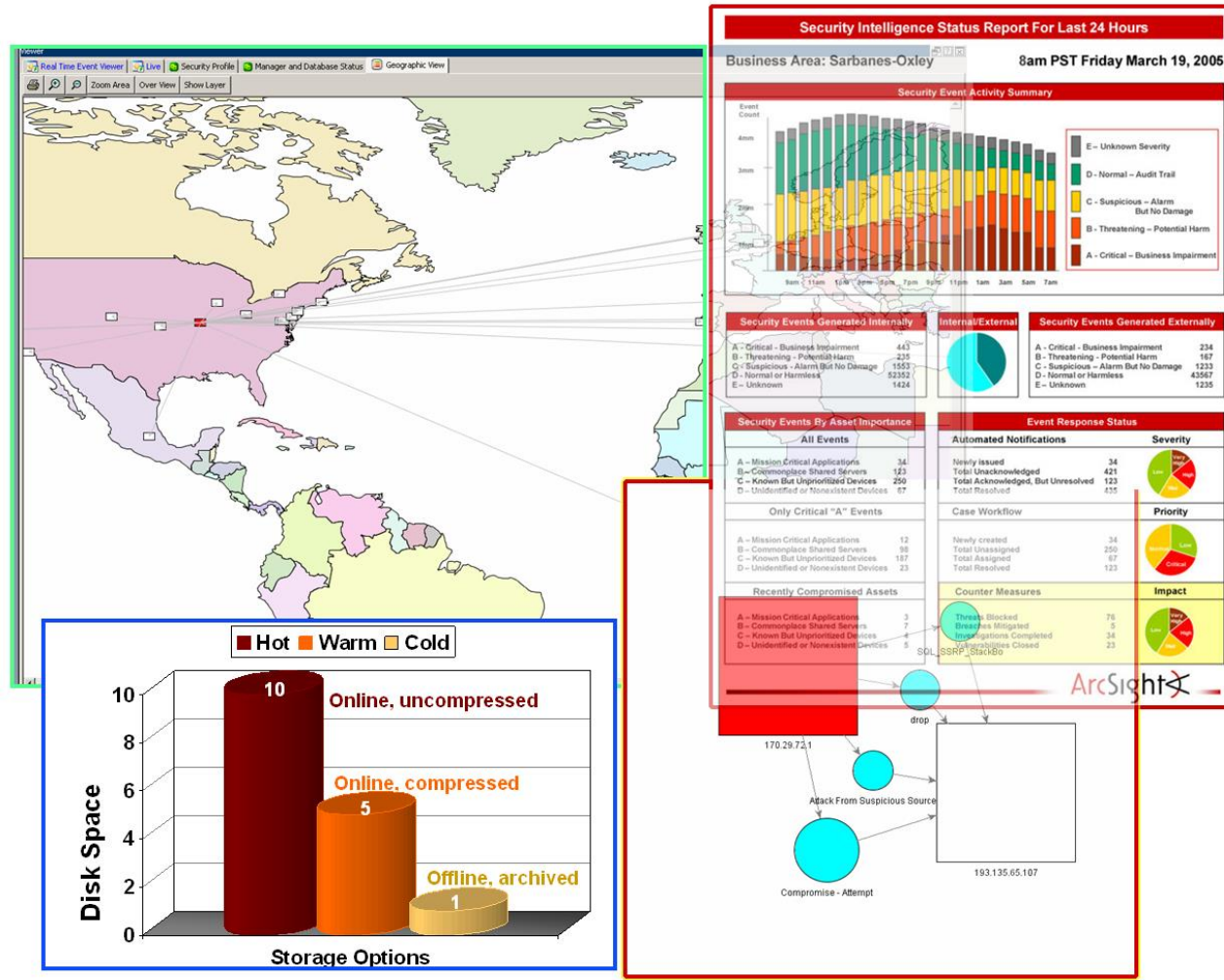
- Attributes**: A table listing user details for 'Actor:User1'.

* 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**: A table listing account details.

Authenticator	Account ID
Oracle	user1
ABS	I.Ivanov
Docs	Ivanov.fin
Windows	IvanovIF
- Role Attributes**: A table listing role details.

Role Name	Resource Name	Role Type
Analist	ABS	User

- 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 key components:

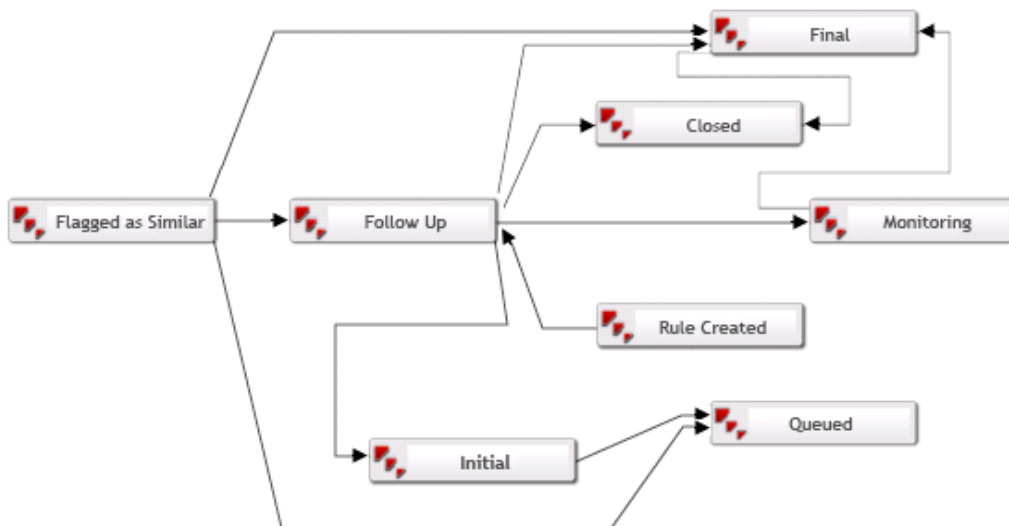
- Section 11 Overview:** Shows a 'Violation' status with a red arrow icon.
- Rules Attacker and Targets:** A network diagram showing nodes and connections. A large blue square highlights a central node.
- Last 20 Rules Fired:** A list of rules with their names and counts.
- Top 20 Rules Fired:** A table showing the most frequent rule violations.
- Top 20 Targets in Rule Firings:** A bar chart showing the number of times specific IP addresses were targeted.
- 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
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 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 Logged in from Two Locations

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
10.0.112.210	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	Rq8HINfoAABCAScxbPIxGDg==
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

БАЗОВЫЕ ПРИМЕРЫ ИСПОЛЬЗОВАНИЯ

Пример 1:

- Будем считать, что некоторая СМ имеет возможность определять географическое расположение объекта по его IP-адресу
- Рассмотрим далее такую ситуацию:
СМ регистрирует факт удаленного доступа по VPN-каналу с IP-адреса, который находится за пределами России, а в настройках указано, что данный сотрудник не находится в зарубежной командировке и может удаленно работать только внутри страны, тогда система СМ автоматически сигнализирует о возможной компрометации логина и пароля, при помощи которого был выполнен удаленный доступ

Пример 2:

- Для операторов связи, предоставляющих доступ в Интернет по логину и паролю, СМ при помощи корреляции может выявлять факты одновременного доступа с одним и тем же логином и паролем из географически разных точек, что может являться признаком компрометации

Пример 3:

- СМ при помощи корреляции может сопоставлять зарегистрированные действия пользователей с их должностными ролями. Например, таким образом СМ может зарегистрировать факт получения доступа рядового сотрудника к бухгалтерской информации, к которой он не должен иметь доступ

Пример 4:

- СМ при помощи корреляции может выявлять факты доступа к конфиденциальной информации в ночное (или в нерабочее) время

Пример 5:

- СМ при помощи корреляции может выявлять факт добавления и удаления у обычного пользователя административных прав в течение заданного промежутка времени. Это может свидетельствовать о том, что пользователю не санкционированно были добавлены права, и после того как он выполнил определённые действия, эти права были удалены

Пример 6:

- СМ при помощи корреляции событий ИБ может выявить факт доступа к конфиденциальной информации с одним и тем же логином и паролем с разных компьютеров в течение небольшого промежутка времени (например, одного часа)
- Это может свидетельствовать о компрометации логина и пароля пользователя
- Точно также СМ может регистрировать факт доступа к информации с одного компьютера, но с разными логинами и паролями

Пример 7:

- Предположим, что система обнаружения вторжений, установленная в какой-то автоматизированной системе, регистрирует атаку типа «SQL injection» на сервис СУБД Oracle сервера X
- Поскольку данная атака может нарушить работоспособность базы данных, система обнаружения вторжений устанавливает ей высокий уровень приоритета
- Однако СМ может проверить собственно сам факт наличия на сервере X базы данных Oracle, и только если она действительно установлена, и подтверждена указанной атаке, то тогда система SIEM оставляет уровень приоритета без изменений
- В противном случае СМ позволяет понизить уровень приоритета выявленного события

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