

Использование SIEM-технологий в расследовании инцидентов информационной безопасности

Александр Кузнецов
НТЦ «Вулкан»

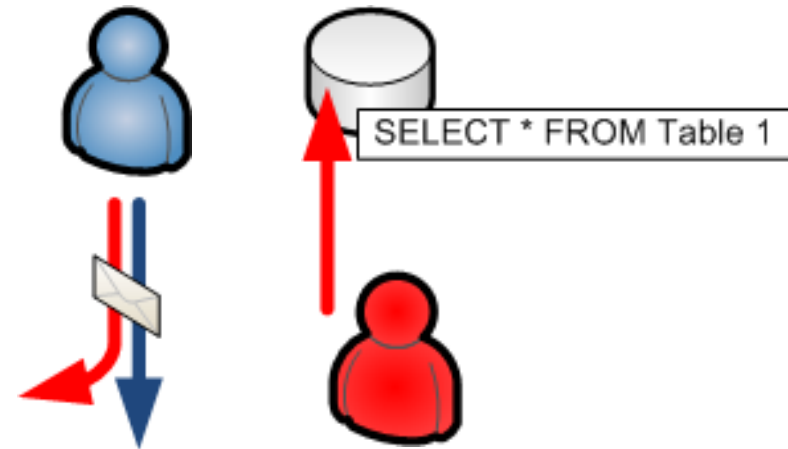
Инцидент ИБ

- **Причина инцидента ИБ:**

- преднамеренные действия
- непреднамеренные действия

- **Порядок расследования:**

- подготовка (preparation)
- **выявление и анализ (detection and analysis)**
- локализация, ликвидация и восстановление (containment, eradication and recovery)
- действия по результатам инцидента (post-incident activity)



Ищем следы инцидента ИБ

- **Log-файлы – важнейшие источники**
- **Анализ log-файлов:**
 - ОС
 - СУБД
 - сетевого оборудования
 - прикладного ПО

10 000 log-ов

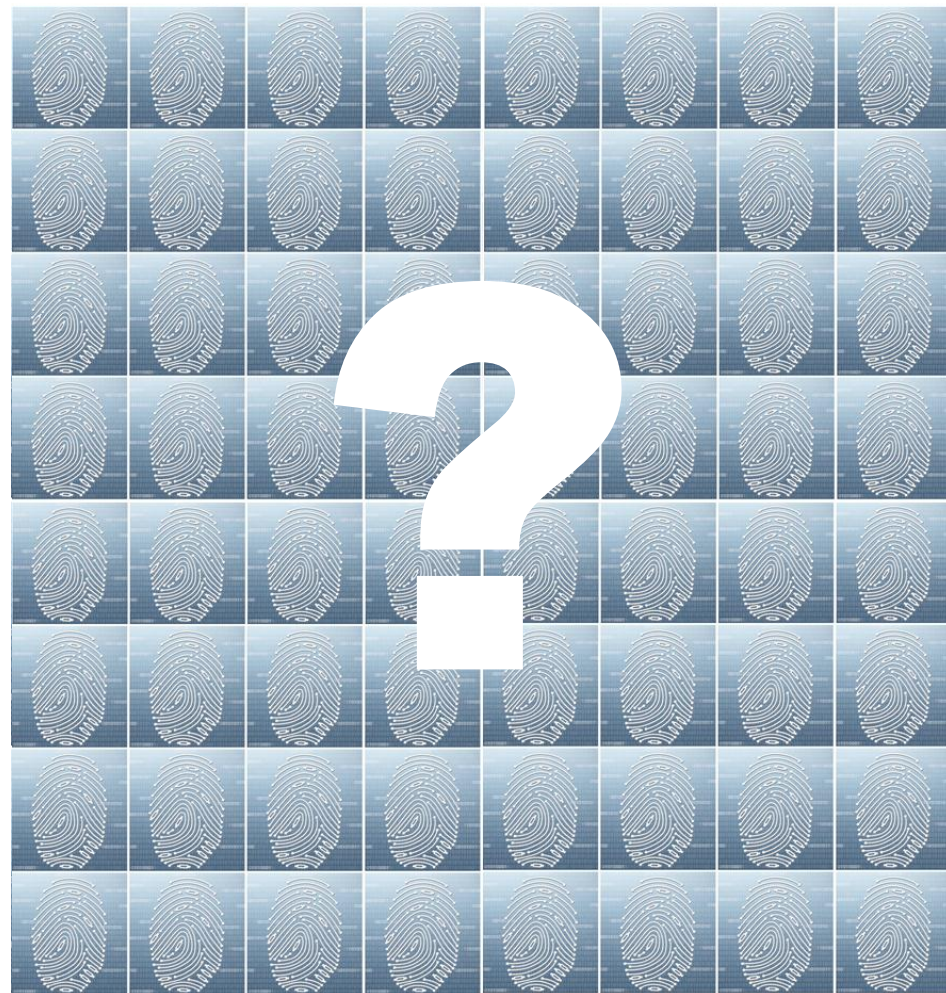


Рисунок с <http://pixelbrush.ru>

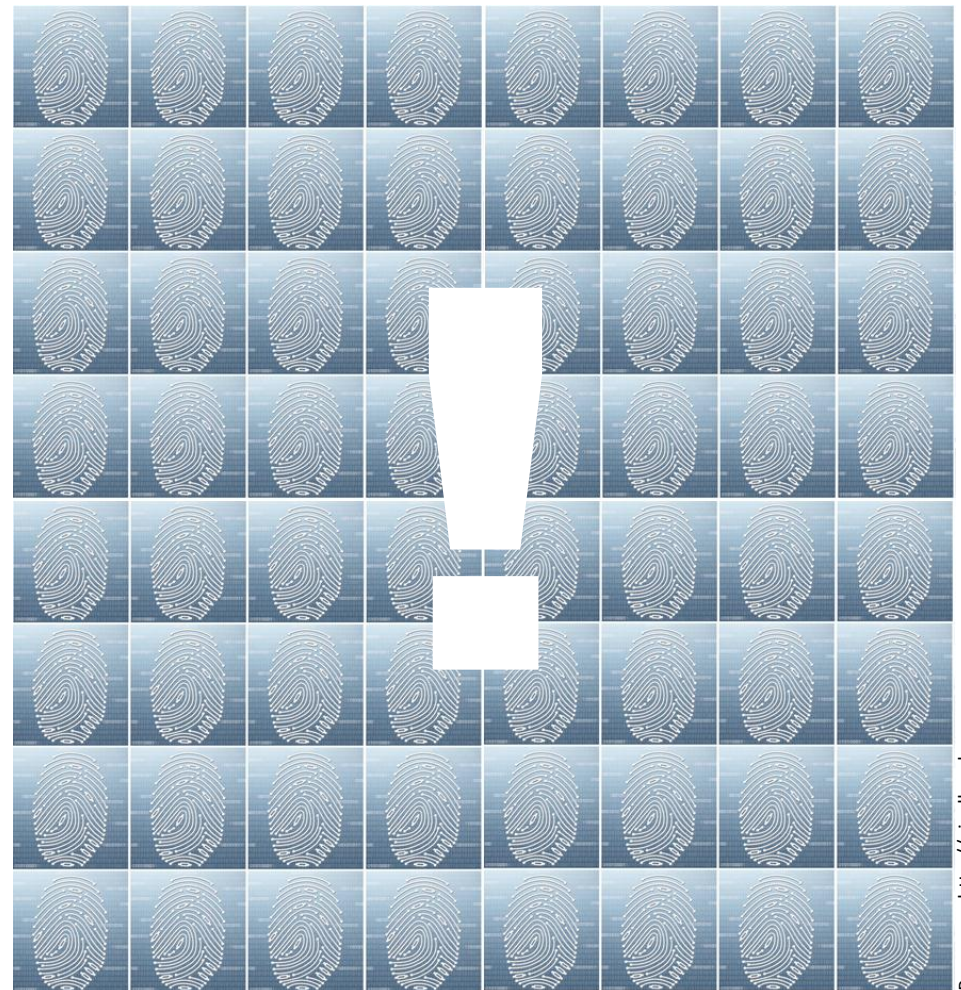
А где ваши log-файлы?

- **Действия с log-файлами:**
 - не ведутся / уничтожаются (перезаписываются) / накапливаются
 - не обрабатываются / обрабатываются вручную



Требования к средствам обработки событий

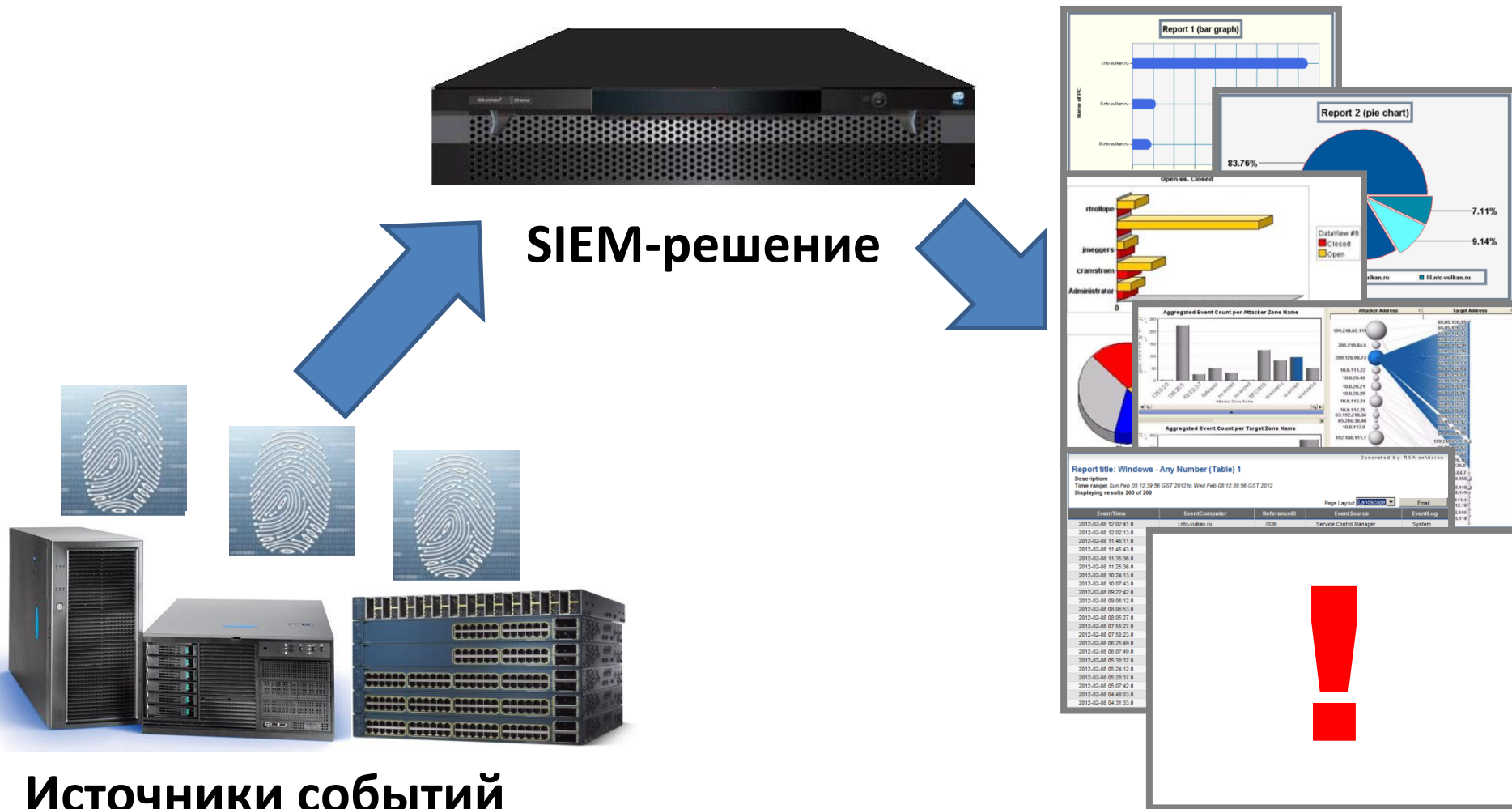
- Автоматизация процесса обработки множества событий от различных источников
- Фильтрация (расширенный поиск)
- Корреляция событий
- Защищенное хранение зарегистрированных событий



Security Information and Event Management

- **Действия (функционал):**
 - сбор событий от компонент ИТ-инфраструктуры
 - нормализация событий
 - фильтрация событий
 - обработка и корреляция событий
 - формирование отчетности и информирование (alert)
 - хранение событий
- **Прием событий по протоколам: Syslog, ODBC, SNMP, FTP, SDEE и др.**
- **Работа в режиме реального времени и в режиме отложенного анализа**

Принцип работы SIEM-решений



Ключевые преимущества SIEM-решений

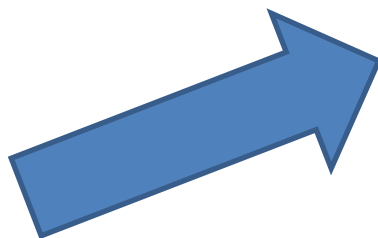
- Централизованное хранение журналов событий вне ИС («вынос доказательств в специальное хранилище»)
- Способность к глубокой ретроспективе – возврат назад до нескольких месяцев и более
- Формирование «слепок» информационной среды на основе информации о событиях от самых разных источников
- Корреляционный и статистический анализ большого числа данных

Ценные качества SIEM-решений

- Хранить независимо
- Хранить много
- Хранить долго



Источник событий



SIEM-решение

- Обеспечение полного жизненного цикла события

От теории к практике (начало)

•

•

Свойства: Событие

Событие

Дата: 15. Источник: Windows File Protection
 Время: 12:04:30 Категория: Отсутствует
 Тип: Предупреждение Код (ID): 64008
 Пользователь: Н/Д
 Компьютер:

Описание:
 Защищенный системный файл c:\windows\system32\termsrv.dll не удалось проверить, поскольку защита файлов Windows завершает работу. Проверьте целостность этого файла позже с помощью служебной программы SFC.

Свойства: Событие

Событие

Дата: 15. Источник: Tcpip
 Время: 12:10:49 Категория: Отсутствует
 Тип: Уведомление Код (ID): 4201
 Пользователь: Н/Д
 Компьютер:

Описание:
 Система обнаружила, что сетевой адаптер Hamachi Network Interface был подключен к сети, и инициировала нормальную работу через этот сетевой адаптер.

1

Свойства: Событие

Событие

Дата: 15. Источник: Service Control Manager
 Время: 12:11:30 Категория: Отсутствует
 Тип: Уведомление Код (ID): 7036
 Пользователь: Н/Д
 Компьютер:

Описание:
 Служба "Hamachi Service" перешла в состояние "Работает".
 Дополнительные сведения можно найти в центре справки и поддержки, в "<http://go.microsoft.com/fwlink/events.asp>".

Свойства: Событие

Событие

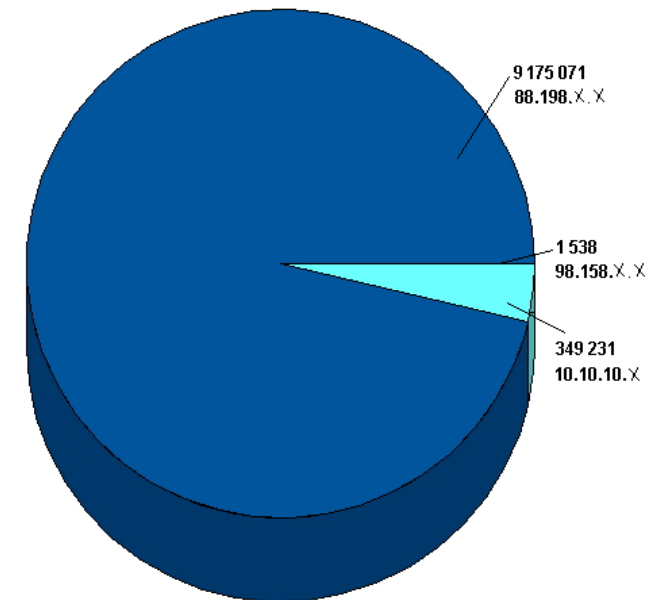
Дата: 15. Источник: Service Control Manager
 Время: 13:07:08 Категория: Отсутствует
 Тип: Ошибка Код (ID): 7031
 Пользователь: Н/Д
 Компьютер:

Описание:
 Служба Удаленный вызов процедур (RPC) была неожиданно завершена. Это произошло 1 раз(а). Следующее корректирующее действие будет предпринято через 60000 мсек: Перезагрузите компьютер.

От теории к практике (продолжение)

Date/Time	DeviceHostName	Description
2012-05-12 15:18:37.0	SERV-AD	The Windows Filtering Platform has allowed a connection.
2012-05-12 15:18:37.0	SERV-AD	A process has exited.
2012-05-12 15:13:37.0	SERV-AD	The Windows Filtering Platform has allowed a connection.
2012-05-12 15:13:37.0	SERV-AD	The Windows Filtering Platform has allowed a connection.
2012-05-12 15:13:37.0	SERV-AD	A process has exited.
2012-05-12 15:13:37.0	SERV-AD	A process has exited.
2012-05-12 15:13:37.0	SERV-AD	A new process has been created.
2012-05-12 15:13:37.0	SERV-AD	A new process has been created.

Process	UserName	SourceAddress	DestinationAddress
\\device\\harddiskvolume2\\users\\администратор.serv-ad\\desktop\\aa_v3.exe		10.10.0.5	88.198. ...
C:\\Users\\Администратор.SERV-AD\\Desktop\\AA_v3.exe	SERV-AD\$		
\\device\\harddiskvolume2\\users\\администратор.serv-ad\\desktop\\aa_v3.exe		10.10.0.5	98.158.1 ...
\\device\\harddiskvolume2\\users\\администратор.serv-ad\\desktop\\aa_v3.exe		10.10.0.5	88.198. ...
C:\\Users\\Администратор.SERV-AD\\Desktop\\AA_v3.exe	SERV-AD\$		
C:\\Users\\Администратор.SERV-AD\\Desktop\\AA_v3.exe	Администратор		
C:\\Users\\Администратор.SERV-AD\\Desktop\\AA_v3.exe	SERV-AD\$		
C:\\Users\\Администратор.SERV-AD\\Desktop\\AA_v3.exe	Администратор		



- Сокращение времени выявления и анализа инцидента ИБ
- Формирование наглядной отчетности

От теории к практике (окончание)

• Превентивная защита



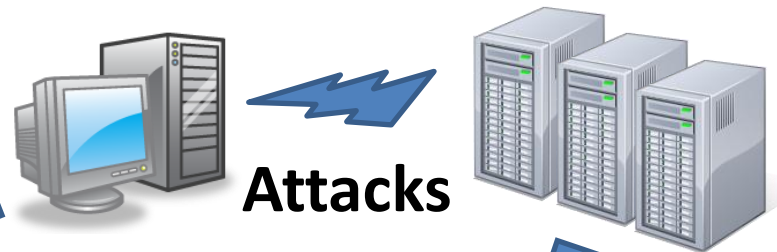
Scan on 10/05/2012 2012 at 14:57

IP : 195.191.88.11

Summary: 6 vulnerabilities found

HIGH 1 **MED** 1 **LOW** 4 **HOST INFO** 23

Name	Vulnerability
OpenSSL ASN.1 Parsing Vulnerabilities	■■■■■
SSL Server Has SSLv2 Enabled Vulnerability	■■■■■
Remote Access or Management Service Detected	■■■■■
Pre-shared Key Off-line Bruteforcing Using IKE Aggressive Mode	■■■■■
SSL Insecure Protocol Negotiation Weakness	■■■■■
Web Server Internal IP Address/Internal Network Name Disclosure Vulnerability	■■■■■



Date/Time	EventCategory/Name	Message
10/05/2012 14:50	Attacks.Access.Modification.TCP/IP	Duplicate TCP SYN from outside:64.39.111.../3789 to dmz:195.191.88.../25 with different initial sequence number
10/05/2012 14:50	Attacks.Access.Modification.TCP/IP	Duplicate TCP SYN from outside:64.39.111.../3787 to dmz:195.191.88.../25 with different initial sequence number
10/05/2012 14:50	Attacks.Access.Modification.TCP/IP	Duplicate TCP SYN from outside:64.39.111.../3787 to dmz:195.191.88.../25 with different initial sequence number
10/05/2012 14:50	Attacks.Access.Modification.TCP/IP	Duplicate TCP SYN from outside:64.39.111.../3786 to dmz:195.191.88.../25 with different initial sequence number
10/05/2012 14:50	Attacks.Access.Modification.TCP/IP	Duplicate TCP SYN from outside:64.39.111.../3786 to dmz:195.191.88.../25 with different initial sequence number
10/05/2012 14:50	Attacks.Access.Modification.TCP/IP	Duplicate TCP SYN from outside:64.39.111.../3785 to dmz:195.191.88.../25 with different initial sequence number
10/05/2012 14:50	Attacks.Access.Modification.TCP/IP	Duplicate TCP SYN from outside:64.39.111.../3785 to dmz:195.191.88.../25 with different initial sequence number
10/05/2012 14:50	Attacks.Access.Modification.TCP/IP	Duplicate TCP SYN from outside:64.39.111.../3784 to dmz:195.191.88.../25 with different initial sequence number
10/05/2012 14:50	Attacks.Access.Modification.TCP/IP	Duplicate TCP SYN from outside:64.39.111.../3784 to dmz:195.191.88.../25 with different initial sequence number
10/05/2012 14:50	Attacks.Access.Modification.TCP/IP	Duplicate TCP SYN from outside:64.39.111.../4816 to dmz:195.191.88.../25 with different initial sequence number
10/05/2012 14:50	Attacks.Access.Modification.TCP/IP	Duplicate TCP SYN from outside:64.39.111.../4816 to dmz:195.191.88.../25 with different initial sequence number
10/05/2012 14:50	Attacks.Access.Modification.TCP/IP	Duplicate TCP SYN from outside:64.39.111.../4815 to dmz:195.191.88.../25 with different initial sequence number
10/05/2012 14:50	Attacks.Access.Modification.TCP/IP	Duplicate TCP SYN from outside:64.39.111.../4815 to dmz:195.191.88.../25 with different initial sequence number
10/05/2012 14:50	Attacks.Access.Modification.TCP/IP	Duplicate TCP SYN from outside:64.39.111.../4814 to dmz:195.191.88.../25 with different initial sequence number

- Использование ФЕМ-решения не



OpenNET

), СВЯЗКА

«SIEM-решения OpenNET «Трафика»»

А еще ...

- Взаимодействие с системами контроля и анализа защищенности (Nmap, Nessus, XSpider, MaxPatrol, QualysGuard, ISS и т.д.)
- Многоуровневая отчетность
- Оценка соответствий (Compliance)
- Формирование «единого окна» для администратора безопасности
- Подготовка данных для BI и GRC-решений

Экспресс-обзор SIEM-решений



Более 80 SIEM-продуктов

Спасибо за внимание!

e-mail: a.kuznetsov@ntc-vulkan.ru

тел. +7 (495) 663-9516