

МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ,
СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФ. М.А. БОНЧ-БРУЕВИЧА»
(СПбГУТ)

Санкт-Петербургский колледж телекоммуникаций им. Э.Т. Кренкеля

Отделение: *Фиксированной связи*

Специальность: *11.02.09 Многоканальные телекоммуникационные системы*

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА (проект)

«Разработка проекта внедрения SIEM-системы отечественного вендора»

Дипломник: **Андреев Михаил Юрьевич**

Руководитель: **Крючихина Людмила Валентиновна**

Санкт-Петербург
2023

СПбГУТ)))

Цель:

разработка проекта внедрения SIEM системы

Задачи:

- провести сравнительный анализ отечественных SIEM-систем;
- выбрать SIEM –систему для внедрения в «Магистраль-Телеком»;
- выбрать оборудование для реализации проекта;
- разработать проект внедрения SIEM-системы на предприятии «Магистраль-Телеком»;
- провести технико-экономическое обоснование проекта




Актуальность проекта



Понятие SIEM-систем



Анализ SIEM систем отечественного производства

Наименование SIEM	 Эшелон комплексная безопасность	MaxPatrol SIEM	 RUSIEM Всё под контролем	 SIEM SEARCHINFORM
Возможность приоритизации инцидента с учетом уровня критичности актива	+	+	-	+
Относительная простота интеграции	-	+	-	+
Оперативная техническая поддержка вендора	-	+	+	+
Удобство при установке «из коробки»	+	+	+	+
Высокая производительность	+	+	-	+
Соотношение параметров цены и качества	+	+	+	-
Возможность обучения SIEM, применение технологий искусственного интеллекта	-	+	-	+
Дополнительные возможности	Поддержка отечественных СЗИ, возможность получения журналов событий от любого типа источника благодаря универсальному адаптеру. КОМРАД поддерживает интеграцию с ГосСОПКА	Особенностью MaxPatrol SIEM является актив-ориентированный подход, который обеспечивает устойчивость работы системы к изменениям в ИТ-инфраструктуре компании.	Развертывание решения возможно как в виртуальной среде на гипервизорах, так и на физической платформе.	Низкие требования к аппаратно-программным средствам, для работы не требуется навыков программирования и приложение поставляется с набором готовых политик

Постановка задачи



«Магистраль-Телеком»

Адрес компании: ул. Ломоносова, 60, Санкт-Петербург, 194362

Необходимость внедрения SIEM-системы в компанию:

- низкая скорость реагирования;
- отсутствие реагирования;
- участвовавшие инциденты проникновения в систему.

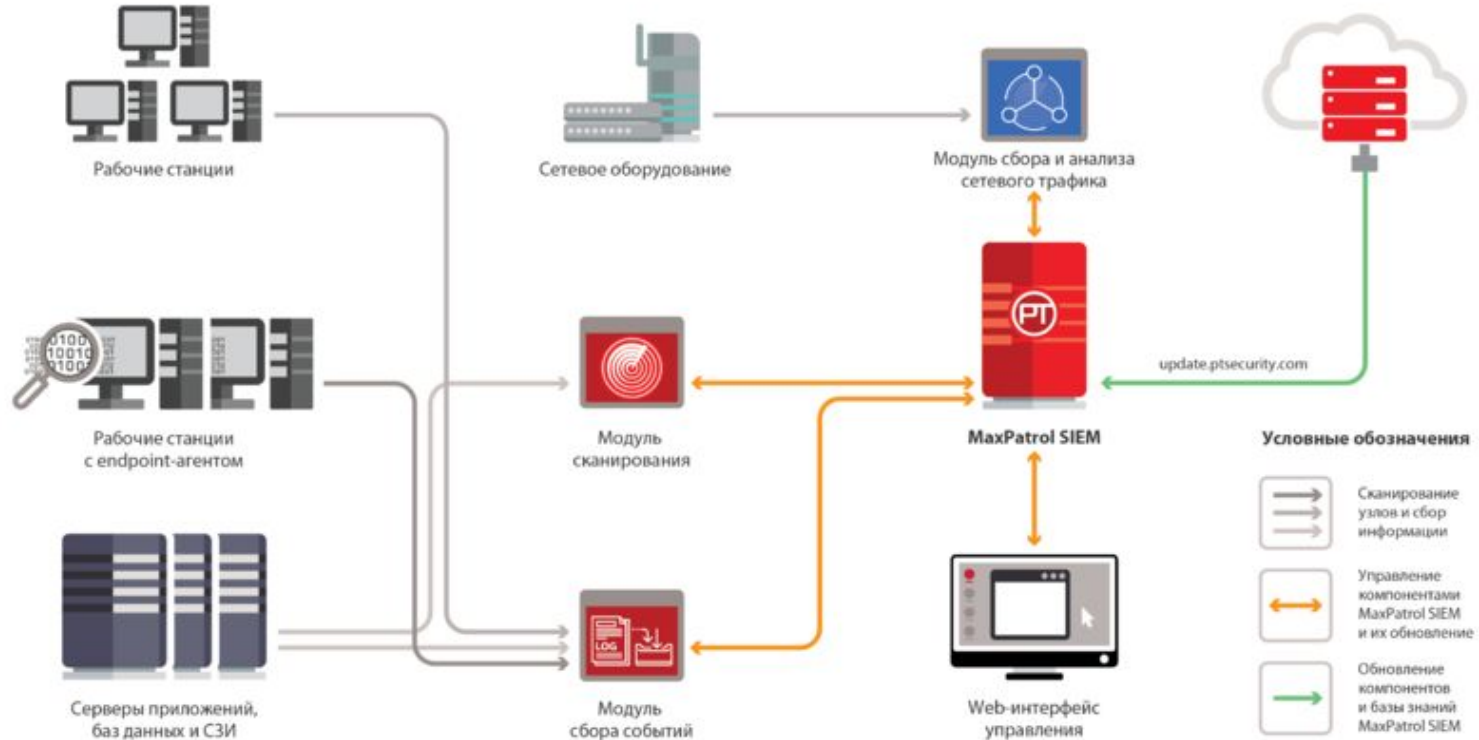
Оборудование для реализации проекта



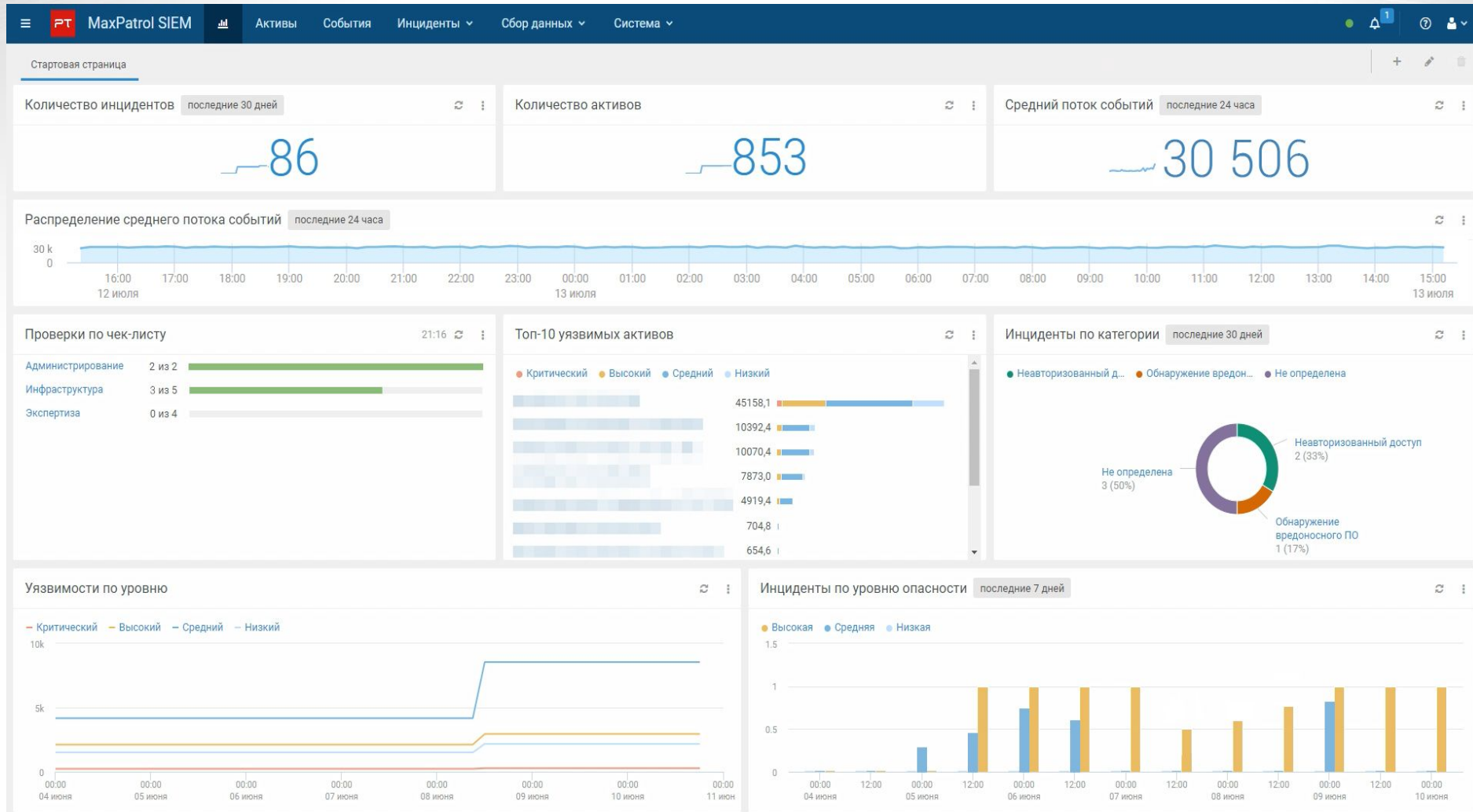
Комплектующие:	Модель:	Кол-во:
Базовая модель	Dell R550 (up to 16 x 2.5" HDD/SSD) rack 2U	1
Процессоры	Intel Xeon Gold 5318Y (2.1 Ghz, 24 cores, Cache 36MB, 165W, 2933 Mhz)	2
Оперативная память	64Gb PC4-25600(3200MHz) DDR4 ECC Registered DIMM	6
Жёсткие диски	3.84TB SSD SAS Read Intensive 12Gbps HS 2.5"	1
Дополнительные жёсткие диски	2.4TB 10k SAS 12Gbps HS HDD 2.5"	10
Raid контроллер	PERC H755 8Gb RAID(0, 1, 5, 6, 10, 50, 60) 12Gb/s	1
Оптический привод	DVD-RW USB 2.0	1
Модуль управления	iDRAC 9 Datacenter	1
Основной адаптер	Embedded NIC 2x1Gb + Broadcom 57414 2x10Gb/25Gb SFP28 OCP Card	1
Блоки питания	Power Supply, 800W, Hot-plug	2

Программное обеспечение для реализации проекта

MaxPatrol SIEM



Ключевые возможности MaxPatrol SIEM



Отслеживание общего состояния ИБ в организации

Ключевые возможности MaxPatrol SIEM

The screenshot displays the MaxPatrol SIEM interface. The top navigation bar includes 'МакPatrol SIEM', 'Активы', 'События', 'Инциденты', 'Сбор данных', and 'Система'. The user is logged in as 'Administrator'. The main view is titled 'Конфигурация' and shows a list of hosts on the left and a detailed configuration page for a selected host on the right.

Host List (Left Panel):

Узел	Интегральная уяз...	Последнее об...
@Host	Host.#CumulativeV...	Host.#Update...
(dc01.ptde...)	0	23 июля, 16:39
(dc02.ptde...)	0	23 июля, 16:39
7231,5		11 мая, 16:12
7298,7		11 мая, 16:03
7298,7		11 мая, 11:59
7265,1		11 мая, 11:59
9405,2		08 мая, 10:47
2605,8		27 апреля, 14:56
2720,7		27 апреля, 14:53
5229,8		27 апреля, 14:49
7324,3		27 апреля, 14:49
139,2		27 апреля, 14:49
391,1		27 апреля, 14:49
11852,4		27 апреля, 14:48
391,1		27 апреля, 14:48
4030,1		27 апреля, 14:46
396,5		27 апреля, 14:44
168,4		11 апреля, 10:22

Host Configuration Page (Right Panel):

Обнаружен 26 сентября 2017, 15:34 → Последнее обновление 27 апреля, 14:49 → Устаревает 21.10.2018
 ↑ 7324.3 Средняя значимость

История за 6 октября 2017 - 16 августа 2018

Интегр. уязвимости
 Сканирования
 События

Сводка: Уязвимости | Конфигурация | Метрики CVSS

Описание: Рабочая станция

Информация о системе:

- OS: Windows 10 10.0.15063
- BIOS: Phoenix Technologies LTD PhoenixBIOS 4.0 Release 6.0
- CPU: Intel(R) Xeon(R) CPU E5-2660 v3 @ 2.60GHz
- MB: Intel Corporation
- RAM: 2
- HDD: \\.\PHYSICALDRIVE0
- Ethernet: vmxnet3 Ethernet Adapter
- Domain: ptdemo.local

Сетевая конфигурация:

Интерфейс	Порт	Сервис	ПО
> ip://[::1]			
> ip://127.0.0.1			

Самые опасные уязвимости:

- Окончание поддержки продукта
- Окончание поддержки продукта
- Окончание поддержки продукта
- Использование после освобождения
- Ошибка при работе с памятью
- Ошибка при работе с памятью
- Ошибка при работе с памятью
- Удаленное выполнение кода, связанное с Windows SMB
- Использование после освобождения
- Удаленное выполнение кода

Уязвимость сетевых служб:

Служба	Уязвимостей
SMB	1

Уязвимости ОС и ПО:

Компонент	Уязвимостей
ОС	
Windows 10 10.0.15063	617
ПО	
Microsoft Internet Explorer	308
Flash Player	80
OpenSSL	36
Microsoft Windows Media	4

Полная видимость Инфраструктуры

Ключевые возможности MaxPatrol SIEM

Скриншот интерфейса MaxPatrol SIEM, демонстрирующий удобные возможности наблюдения за топологией сети. Интерфейс разделен на несколько панелей:

- Верхняя панель:** Содержит меню (Максимум, PT, MaxPatrol SIEM) и кнопки для переключения между вьюшками: Активы, События, Инциденты, Сбор данных, Система. В правом верхнем углу отображены права доступа (Administrator).
- Левая панель:** Содержит панель «Группы» с поиском и таблицу данных. В таблице перечислены узлы с их IP-адресами, значениями интегральной оценки и временем последнего обновления.
- Центральная панель:** Отображает топологию сети, состоящую из множества узлов (серверов, рабочих станций, маршрутизаторов) и связей между ними. В центре выделены два узла: 29 и 48.
- Панель справа:** Показывает подробные сведения о выбранном узле (TCP/22). Включает информацию о типе устройства (Рабочая станция, Маршрутизатор), маршрутах и конфигурации сетевых интерфейсов.

Узел	Интегральная оценка	Последнее обновление
Host	99,1	01 июня, 17:32
Host	89,1	01 июня, 17:30
Host	48,2	01 июня, 17:31
Host	48,2	01 июня, 17:30
Host	48,2	01 июня, 17:30
Host	48,2	01 июня, 17:30
Host	48,2	01 июня, 17:31
Host	48,2	01 июня, 17:31
Host	48,2	01 июня, 17:30
Host	48,2	01 июня, 17:30
Host	46,1	31 июля, 15:13
Host	46,1	01 июня, 17:32
Host	10	20 сентября, 16...
Host	10	20 сентября, 16...
Host	5	20 сентября, 16...
Host	5	20 сентября, 16...
Host	5	20 сентября, 16...
Host	5	20 сентября, 16...
Host	5	20 сентября, 16...

Всего 719 записей, выбрана 1

Удобное наблюдение за топологией сети

Ключевые возможности MaxPatrol SIEM

The screenshot displays the 'Knowledge Base' interface for editing a correlation rule. The rule is titled 'Условие корреляции' (Correlation Condition) and is set to '10 секунд' (10 seconds). The condition is defined as 'Должны произойти все события последовательно' (All events must occur sequentially).

The rule consists of two events:

- Событие А** (Event A): `Windows_Logon_Network`. It is configured to occur '1 раз' (1 time). The macro is 'Удалённый вход на узел с Windows' (Remote login on Windows node). The condition is 'subject.name' is 'не в списке' (not in list), with the list containing 'myorg\iivanov' and 'myorg\superadmin'.
- Событие В** (Event B): `Windows_Process_Run`. It is configured to occur '1 раз' (1 time). The macro is 'Запуск конкретного процесса на узле с Windows' (Execution of a specific process on Windows node). The condition is 'Название процесса' (Process name) is 'WmiPrivSE.exe'.

The interface includes a left sidebar with navigation options: 'Параметры правила корреляции', 'Условие корреляции', 'Корреляционное событие', and 'Действия при срабатывании цепочки'. At the bottom, there are buttons for 'Предварительный просмотр', 'Валидация', 'Статус валидации', 'Сохранить', and 'Отмена'.

Возможность настроить инциденты

Этапы реализации проекта



Оценка эффективности SIEM системы



PTSECURITY.COM

ОС, СКАНИРОВАННАЯ НА НЕОБХОДИМЫЙ ПОЛЬЗОВАТЕЛЮ СТАНДАРТ	ВРЕМЯ БЫЛО/СТАЛО	ПРОЦЕНТ УСКОРЕНИЯ
Windows Srv2012R2 на CIS-Windows 2012	11,6 мин 8,8 мин	+24%
Windows Srv2012R2 на CIS-Exchange 2016	17,2 мин 9,8 мин	+43%
Windows Srv2008R2 SP1 с СУБД Oracle12 на CIS-Oracle DB	14,2 мин 9,2 мин	+35%
Windows Srv2012 с MS SQL 2012 на CIS-SQL 2012	18,5 мин 13,5 мин	+27%
40 различных Unix-машин под RHEL/CentOS/SLES, Debian на CIS-Distribution Independent Linux и PT-Essential(UNIX)	82 мин 50 мин	+37%

Экономические расчёты

Статьи	Сумма/руб.
Стоимость оборудования	1 990 025
Общая стоимость на программно-аппаратные решения	19 422 433
Стоимость монтажных и настроечных работ	99 501
Транспортные расходы, связанные с доставкой оборудования	199 002
Капитальные вложения	21 710 961

Срок окупаемости проекта составит 2 года и 5 месяцев

Выводы:

- проведён сравнительный анализ отечественных SIEM-систем;
- выбрана SIEM –система для внедрения в компанию „Магистраль-Телеком“;
- выбрано оборудование для реализации проекта;
- разработан проект внедрения SIEM-системы в компанию „Магистраль-Телеком“;
- проведено технико-экономическое обоснование проекта

МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ,
СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФ. М.А. БОНЧ-БРУЕВИЧА»
(СПбГУТ)

Санкт-Петербургский колледж телекоммуникаций им. Э.Т. Кренкеля

Отделение: *Фиксированной связи*

Специальность: *11.02.09 Многоканальные телекоммуникационные системы*

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА **(проект)**

«Разработка проекта внедрения SIEM-системы отечественного вендора»

Дипломник: **Андреев Михаил Юрьевич**

Руководитель: **Крючихина Людмила Валентиновна**

Санкт-Петербург
2023

СПбГУТ)))