**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**

СПб ГУТ)))

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 приоритезации инцидента с учетом уровня критичности актива	+	+	-	+
Относительная простота интеграции	-	+	-	+
Оперативная техническая поддержка вендора	-	+	+	+
Удобство при установке «из коробки»	+	+	+	+
Высокая производи-тельность	+	+	-	+
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

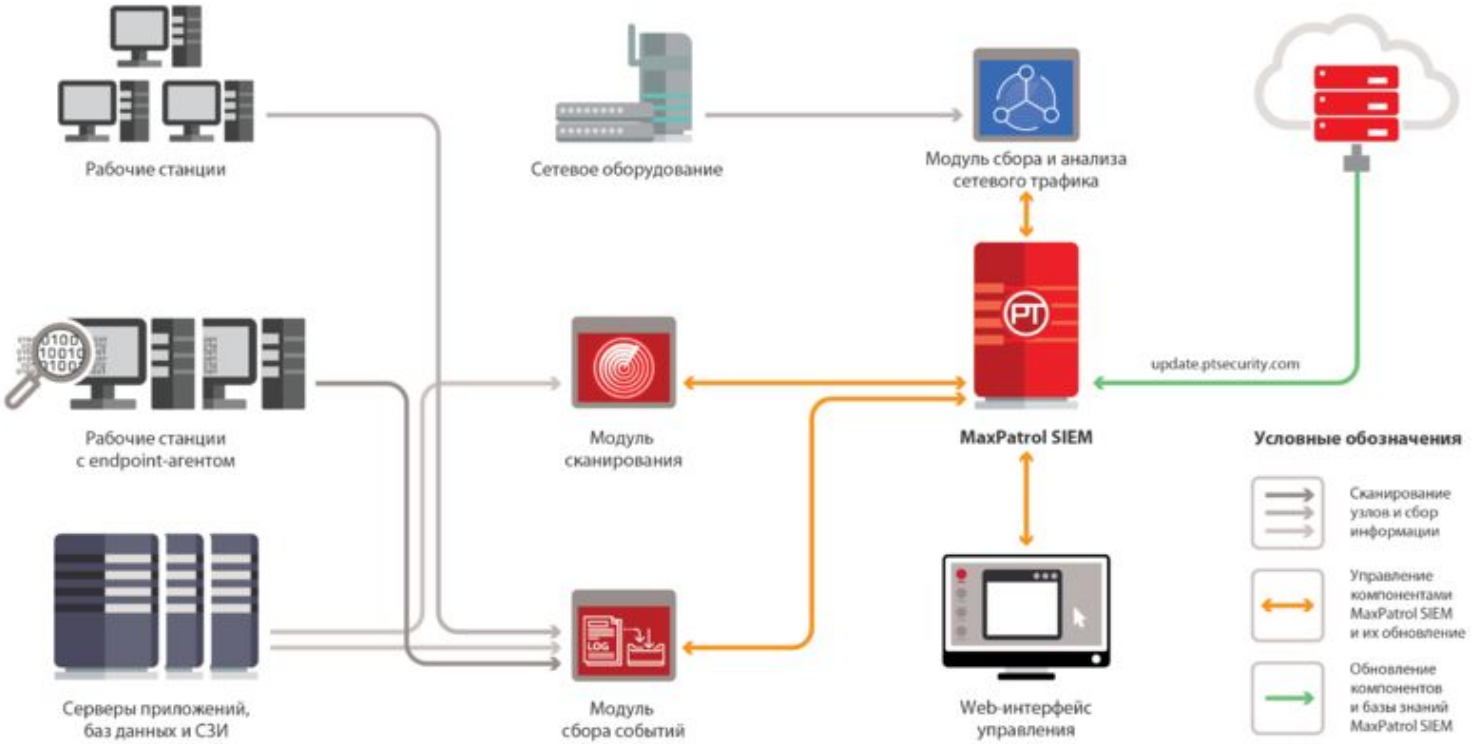
Необходимость внедрения SIEM-системы в компанию:
- низкая скорость реагирования;
- отсутсвие реагирования;
- участившиеся инциденты проникновения в систему.

Оборудование для реализации проекта

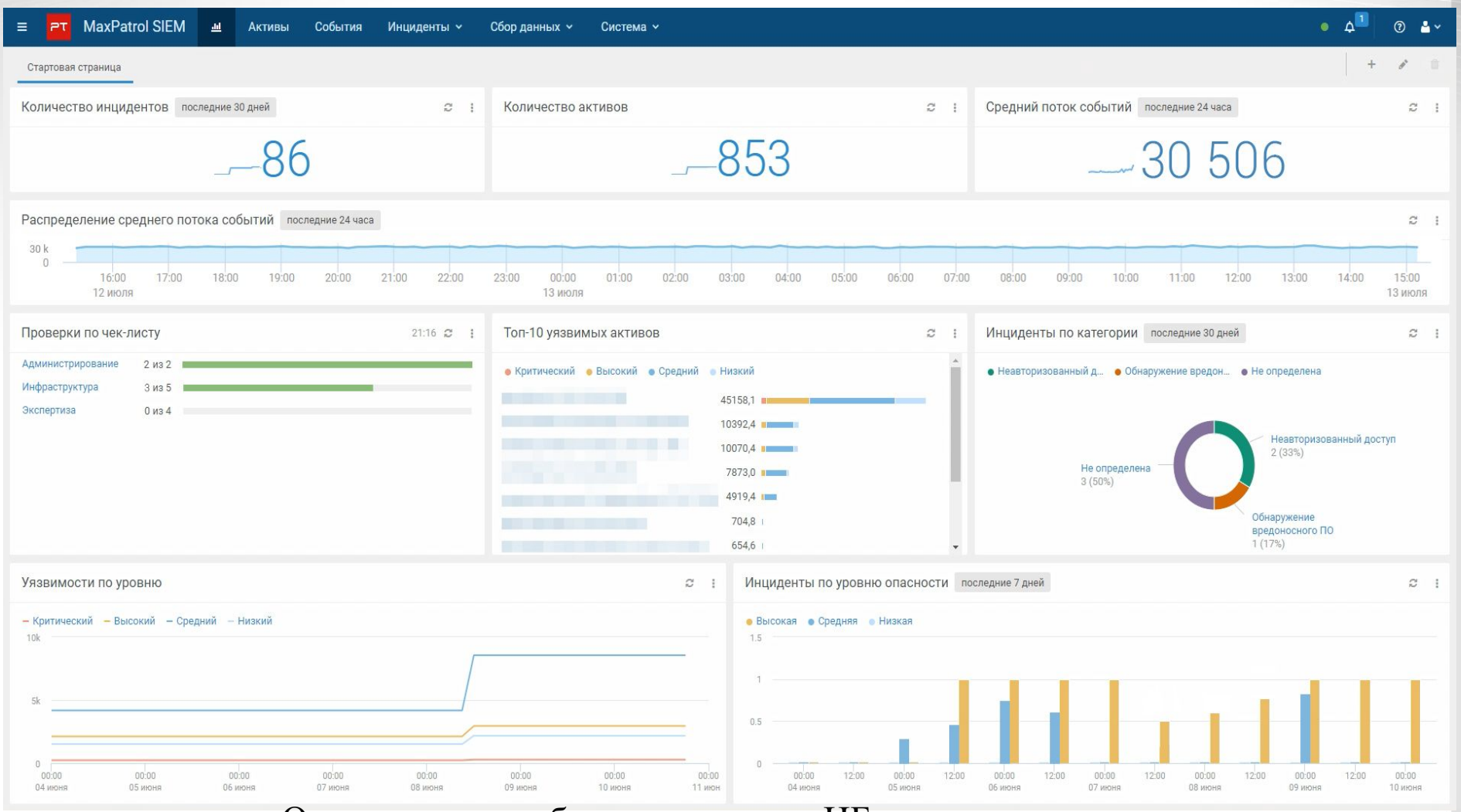
Комплектующие:	Модель:	Кол-во:
Базовая модель	Dell R550 (up to 16 x 2.5″ HDD/SSD) rack 2U	1
Процессоры	Intel Xeon Gold 5318Y (2.1 Ghz, 24 cores, Cache 36MB, 165W, 2933 Mhz)	2
Оперативная память	64Gb PC4-25600(3200MHz) DDR4 ECC Registered DIMM	6
Жёсткие диски	3.84TB SSD SAS Read Intensive 12Gbps HS 2.5″	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

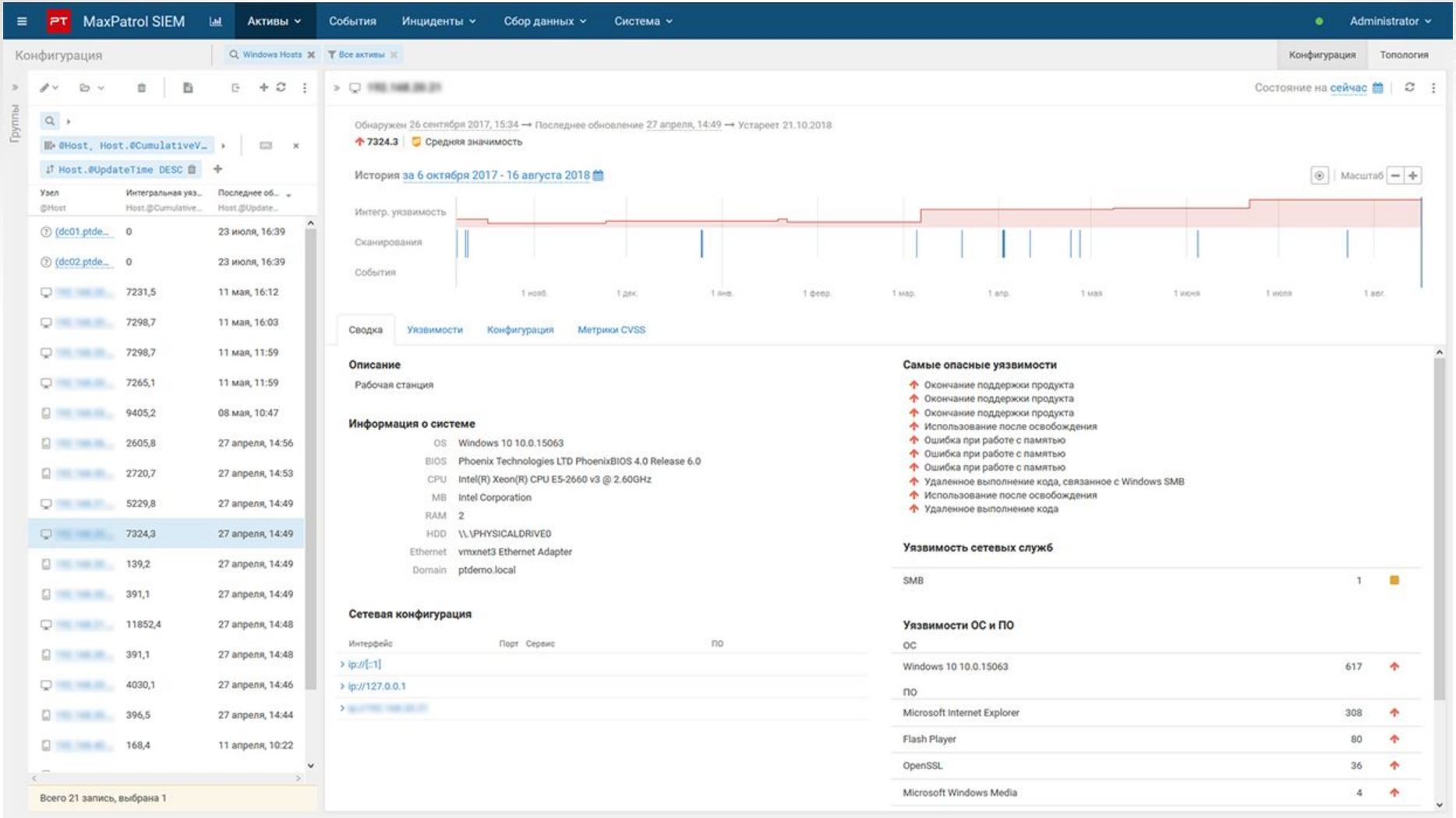


Ключевые возможности MaxPatrol SIEM



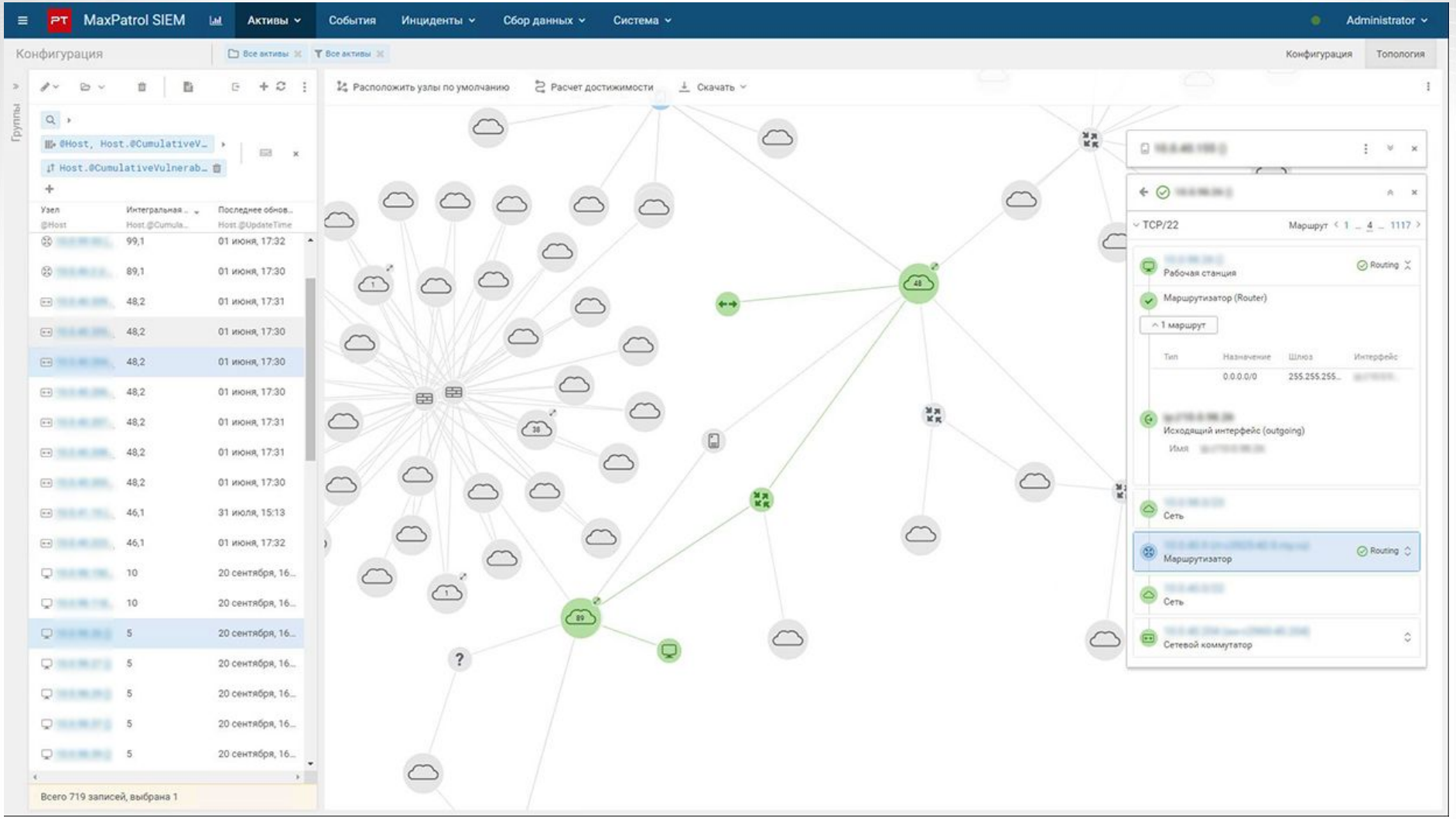
Отслеживание общего состояния ИБ в организации

Ключевые возможности MaxPatrol SIEM



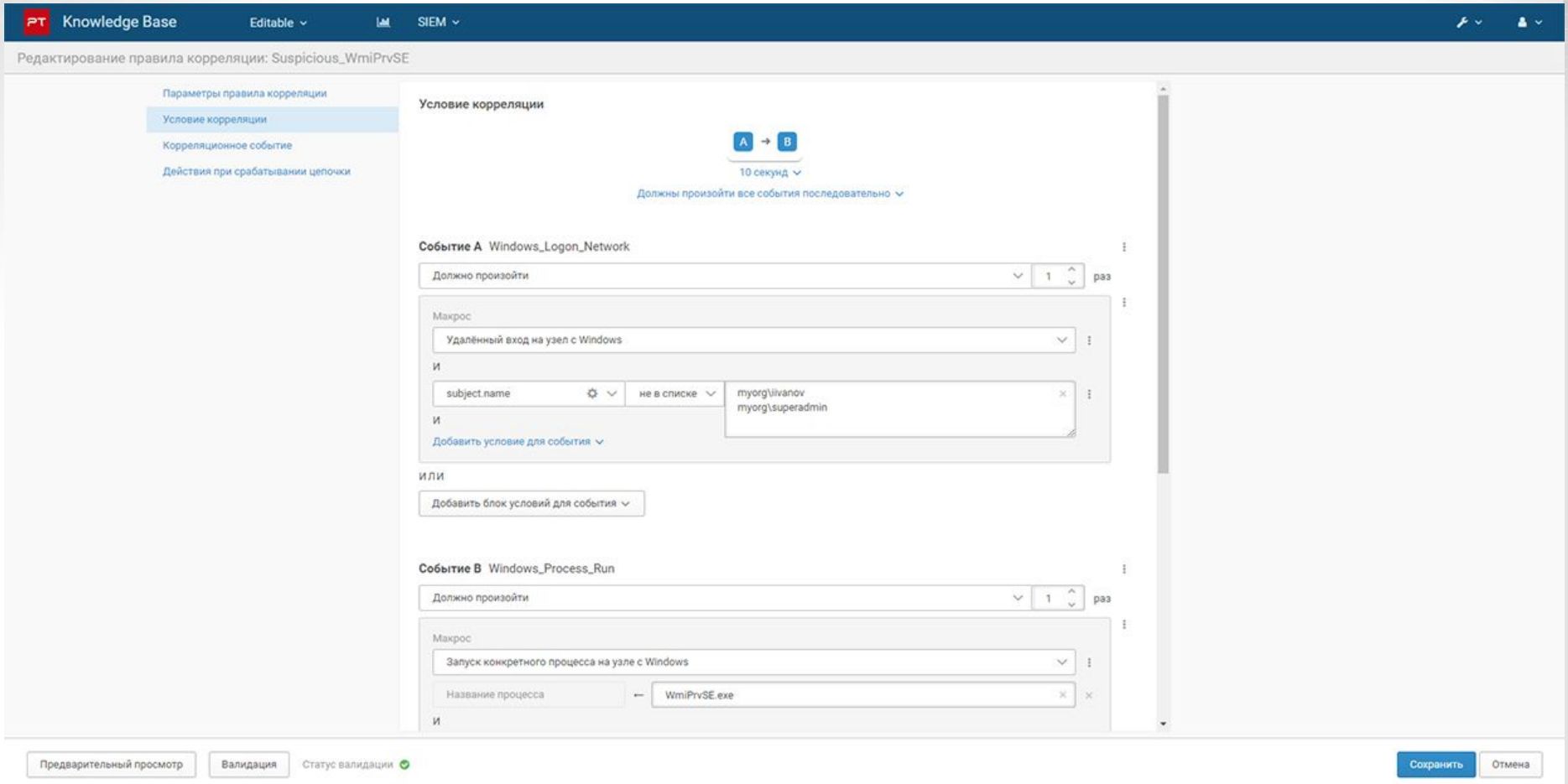
Полная видимость Инфраструктуры

Ключевые возможности MaxPatrol SIEM



Удобное наблюдение за топологией сети

Ключевые возможности MaxPatrol SIEM



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**

СПб ГУТ)))