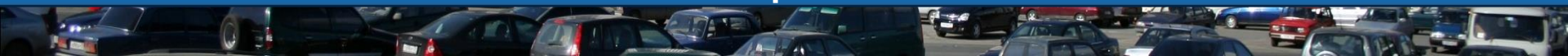
ПЕРМСКИЙ НАЦИОНАЛЬНЫЙ
ИССЛЕДОВАТЕЛЬСКИЙ
ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ

ПНИПУ

PERM NATIONAL
RESEARCH
POLYTECHNIC UNIVERSITY

г. Пермь, Комсомольский пр., 29
www.pstu.ru



ПЕРМСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ

ПНИПУ

PERM NATIONAL RESEARCH POLYTECHNIC UNIVERSITY

Опыт внедрения и использования SIEM

Роман Рашевский

Инженер систем безопасности ПНИПУ

Пермь 08.12.2016

ОБЩАЯ ИНФОРМАЦИЯ О ПНИПУ

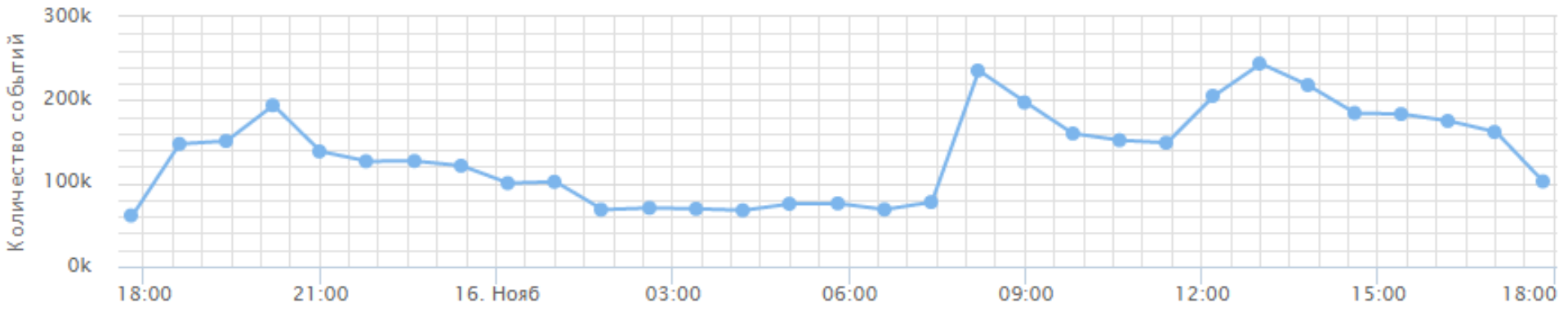
- Основан в 1953 году
- С 2009 года первый в Пермском крае «Национальный исследовательский университет»
- 3 500 сотрудников, 1 200 преподавателей
- Более 20 000 студентов, 4 500 выпускников ежегодно

ИТ-ИНФРАСТРУКТУРА ПНИПУ

- 2 независимых ЦОДа
- Подключение к 10Gb магистральной линии связи RUNNet (Амстердам – Стокгольм – СПб – Москва – Пермь), 10Gb кольцо между кампусами
- >200 коммутаторов уровня доступа, ~30 – уровня агрегации, 6 – в ядре сети
- Система виртуализации на базе решений IBM и VMWare (HS22 + XIV + ESXi + vSphere)
- 2 000 рабочих станций, 200 VDI-клиентов на базе VMware Horizon View

НЕОБХОДИМОСТЬ ВНЕДРЕНИЯ SIEM СИСТЕМЫ

- Большое разнообразие источников событий, с различными форматами данных
- Огромное количество событий



SIEM vs LOG MANAGEMENT

- Возможность обработки (нормализации) и корреляции событий
- Реализация рабочего процесса реагирования на инциденты и управления ими
- Готовый инструмент для служб ИБ

ЭФФЕКТ ОТ «ПРАВИЛЬНОГО» ВНЕДРЕНИЯ SIEM

SIEM – «СЕРЕБРЯНАЯ ПУЛЯ»?

- SIEM – инструмент, но не решение всех проблем ИБ
- Управления инцидентами начинается с политики ИБ, а не с приобретения SIEM
- SIEM, реализующий политику ИБ, требует тонкой настройки под инфраструктуру организации

НАШ ОПЫТ РАБОТЫ С SIEM

- В начале 2014 года приобретен и внедрен ПАК IBM QRadar All-in-One 3105

- В ноябре 2016 года совместно с компанией «Авитек» запущен пилотный проект RuSIEM

ОПЫТ ИСПОЛЬЗОВАНИЯ IBM QRADAR

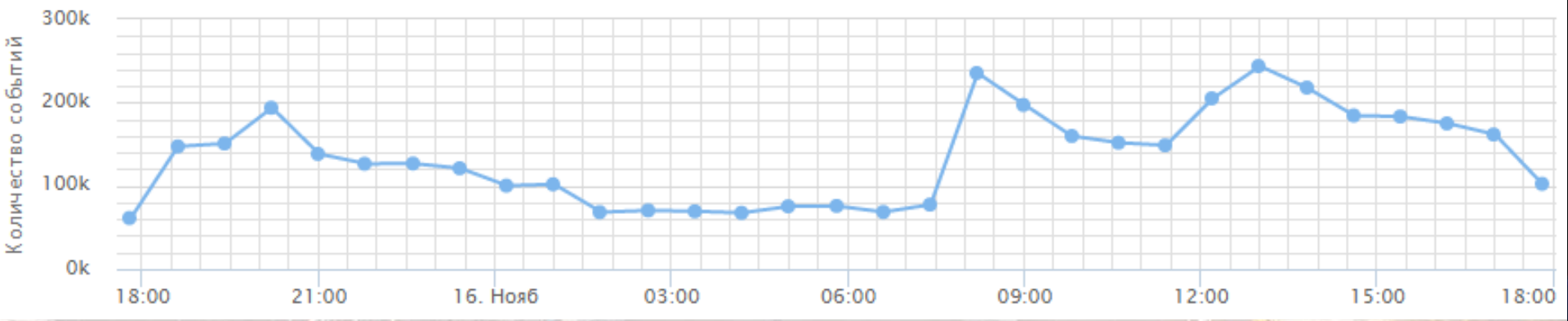
- За время эксплуатации выявлено >10 инцидентов
- Отсутствие качественной технической поддержки от интегратора и вендора
- Деградация производительности ноды при >5000EPS
- Высокая стоимость лицензий на продление

ПИЛОТНЫЙ ПРОЕКТ RUSIEM

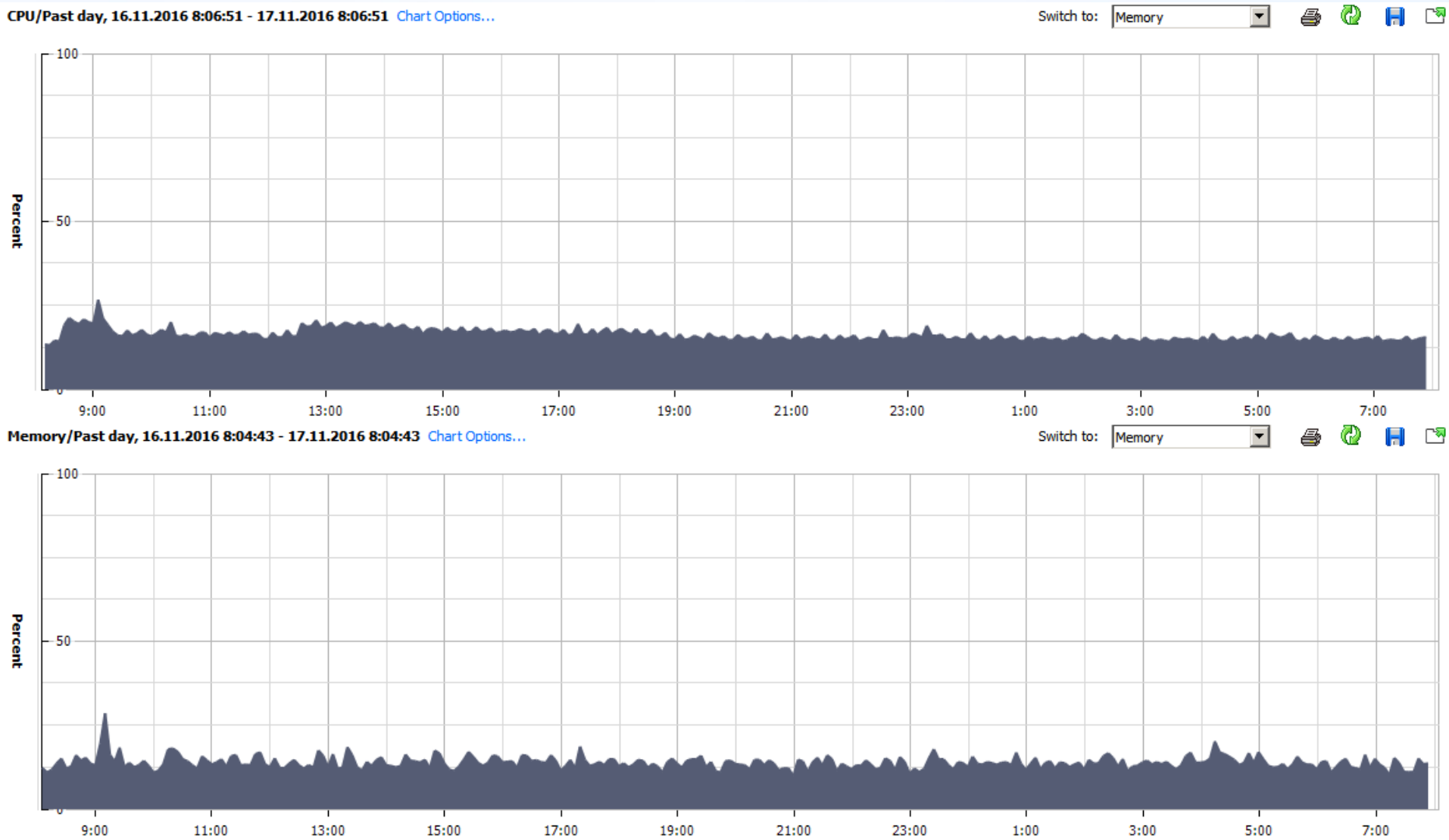
- Время развертывания и подключения базового набора источников – 5 дней
- Грамотные консультации технических специалистов вендора в режиме реального времени

ИСТОЧНИКИ СОБЫТИЙ RUSIEM

- Контроллеры домена Active Directory (5 штук)
- Сервера Microsoft Exchange Server (HT+CAS, 2 штуки)
- Сервер управления Dr.Web



ПРОИЗВОДИТЕЛЬНОСТЬ RUSIEM



ПЛАНИРУЕМЫЕ ИСТОЧНИКИ RUSIEM

- Сервера Microsoft Exchange Server (EDGE+MB+UAG, 5 штук)
- Серверная инфраструктура (Windows/Linux/FreeBSD)
- Критичные рабочие станции
- NetFlow
- PIM-система SafeInspect
- Сетевое оборудование
- Оборудование среды виртуализации

ОСНОВНЫЕ ПРЕИМУЩЕСТВА RUSIEM

- **Отечественный разработчик**
- **Высокая производительность**
- **Гибкая модель лицензирования**
- *Входит в стандарт Ростеха*

АРХИТЕКТУРА RUSIEM

АРХИТЕКТУРА RUSIEM

- **Локальный сборщик событий:**
  - **Syslog**
  - **Netflow (etc.)**
  - *SNMP*
- **Сетевой сенсор (выделенный сервер):**
  - **Анализ сетевого трафика на SPAN-порте**
- **RuAgent (выделенный сервер/локальная установка):**
  - **Windows Event Log (локально и удаленно)**
  - **DB-коннектор (Oracle, MS SQL, MySQL)**
  - **Файловые логи (локально и удаленно)**
  - **1C v8**

Спасибо за внимание!

т: +7 (342) 219-88-22
м: +7 (919) 496-59-89
e: roman@pstu.ru

ПЕРМСКИЙ НАЦИОНАЛЬНЫЙ
ИССЛЕДОВАТЕЛЬСКИЙ
ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ

ПНИПУ

PERM NATIONAL
RESEARCH
POLYTECHNIC UNIVERSITY

г. Пермь, Комсомольский пр., 29
www.pstu.ru