VB-Trend 2019

plan>b

VolgaBlob

Путь от SIEM к решению Big Data, полезному бизнесу

Опыт компании СУЭК

Smart Monitor > Splunk > Plan-B

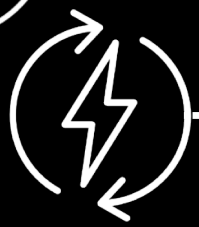
Начало пути: формирование потребности в SIEM

VB-Trend 2019 plan>b VolgaBlob

Большая инфраструктура > Разрозненные средства ИБ

Более 20 вендоров ИБ

Квалификация специалистов недостаточна для ручной аналитики **ВСЕХ** источников Компании



Необходимость в процессе обработки инцидентов с SLA

Smart Monitor

СУЭК

Критерии выбора SIEM

VB-Trend 2019 plan>b VolgaBlob

	«Коробочные» SIEM		Платформенный подход
Ready To Go	8 «все в одном»	7	Модули надо настраивать под себя, это проект
Выявление инцидентов	6 Правила «из коробки» не работают	10	Гибкость в создании правил и поиске аномалий
Визуализация	6 «Автор так видит»	8	Настраиваем под себя, вообще ушли от стандартных форм
Источники	8 Тут »коробка» пригождается на типовых СЗИ	10	Достаточно просто подключить **ЛЮБОЙ** источник

Результаты внедрения SIEM за год

Cisco ESA

Check Point

Smart Monitor

TREND MICRO

Docsvision

CITRIX

Microsoft Exchange

AVAYA

SAP Modules

Cloud

SAP ERP

cisco

Antivirus Systems

WEB Servers

VoIP

Microsoft Active Directory

Servers + PCs

Firewalls

СКУД

Microsoft Exchange

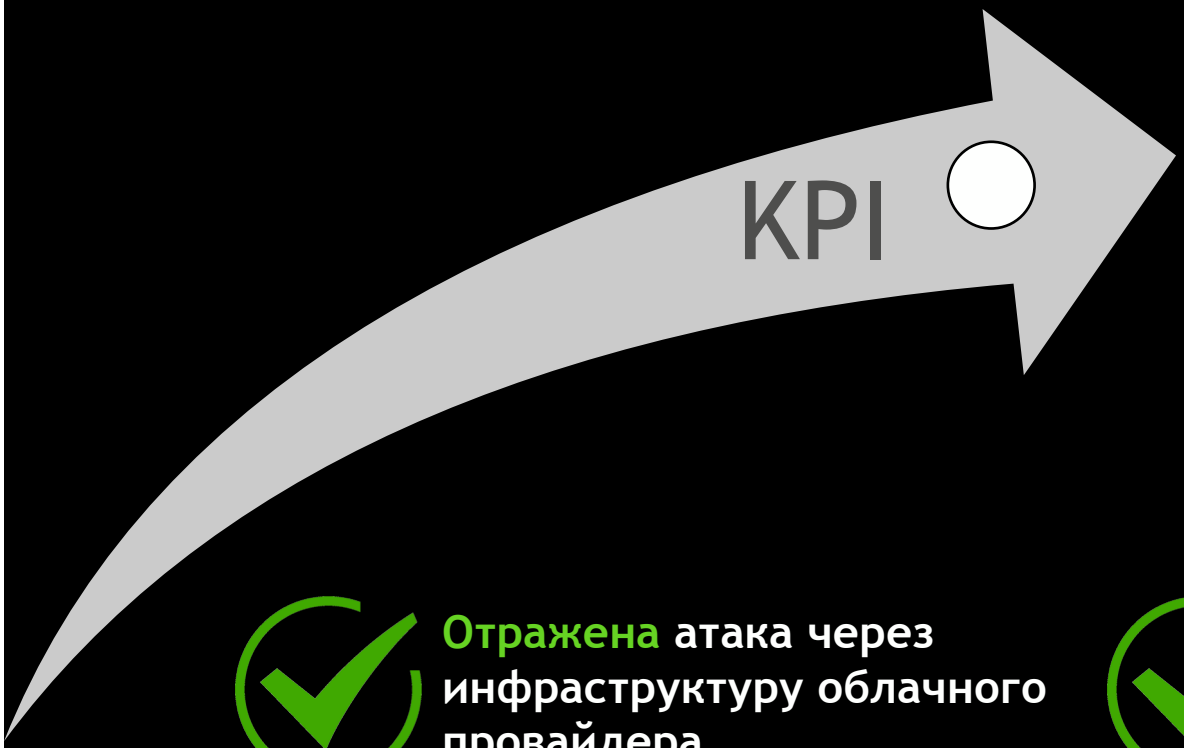
Microsoft AD

Ключевой результат

Формирование собственной команды аналитиков больших данных

VB-Trend 2019 plan>b VolgaBlob

Эффективность SIEM



SIEM показывает эффективность по мере **накопления** данных

Отражена атака через инфраструктуру облачного провайдера

Удалось внедрить **автоматический** контроль внешних атак

Big Data: текущее состояние

VB-Trend 2019 plan>b VolgaBlob

Цифровой феодализм

Каждое подразделение владеет своим набором данных и проблем

- **Кадры** – не готовы обмениваться данными с другими подразделениями
- **Производство** – зачастую не имеет компетенций в IT
- **Финансы** – не может получить доступ к данным
- **ИТ** – хранит, но не использует

Big Data: текущее состояние

VB-Trend 2019 plan>b VolgaBlob

Проблемы существующих систем бизнес-аналитики

SAP BW и/или собственные разработки:

- **Малый охват** (1-2 источника входных данных)
- **Малая область** видимости данных
- **Сложность разработки** и высокая стоимость аналитиков (среднее время доработки – месяц)
- **Нет единых требований** к нормализации – везде свои базы и типы данных
- **Малая глубина хранения** (не регламентировано, часто - полгода)

Big Data: текущее состояние

ИТ и бизнес говорят на разных языках

Бизнес не готов обмениваться данными для решения совместных задач

Пример: карьерная техника

VB-Trend 2019 plan>b VolgaBlob

Задача: Оценить эффективность работы

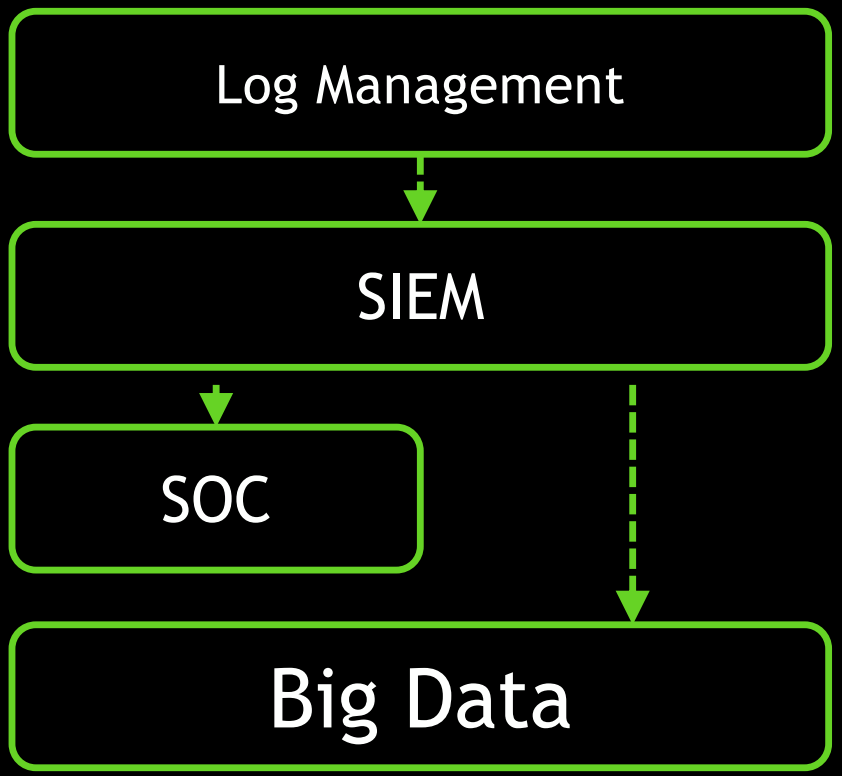
Источники данных > ключевая информация > владелец данных:

- **Система диспетчеризации** > данные о объемах перевозки > производственный блок, подразделение 1
- **Система АСУ** > данные о топливе > производственный блок, подразделение 2
- **Кадры** > данные о бригадах > блок по работе с персоналом
- **Система автоматизации ремонтов** > данные о ремонтах > Финансы/ИТ

Если **объединить данные** – можно оценить эффективность в привязке к выработке, финансам и сотрудникам.

В реальности **объединения не происходит**, хотя все необходимые данные к компании **уже есть**

Необходима единая методология работы с данными



Целевая схема

- SIEM как инструмент гарантированной сохранности и нормализации данных
- Единый протокол/шина доступа к данным
- Регламентированный срок хранения данных
- Регламентированный перечень источников

ИБ и SIEM как центр консолидации

VB-Trend 2019 plan>b VolgaBlob

Компетенции, полученные при внедрении SIEM ИБ позволяют обрабатывать и бизнес-данные

ИБ как подразделение имеет возможность собирать бизнес-данные

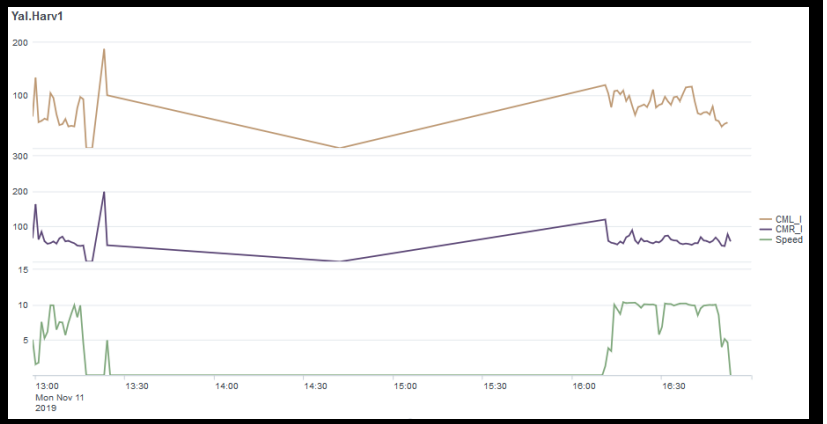
Что сделано для обработки Big Data?

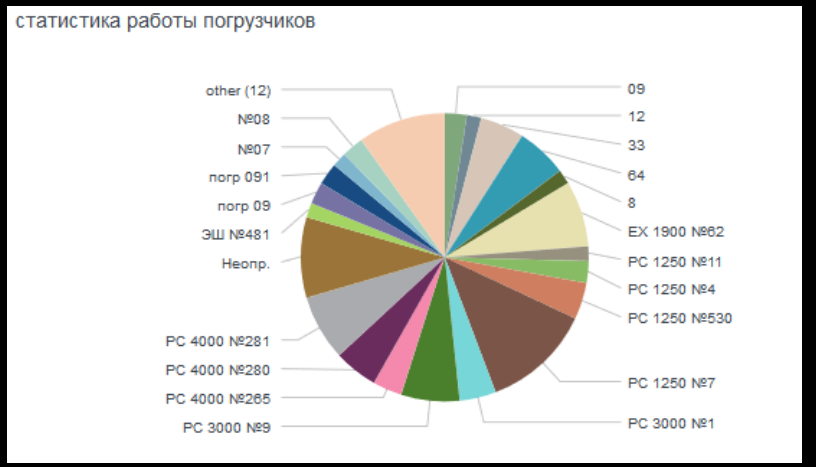
VB-Trend 2019 plan>b VolgaBlob

Разработаны коннекторы к:

Производственным системам:

- системам диспетчеризации (карьерная техника, комбайны, конвейеры)
- системам АСУ (учет топлива)

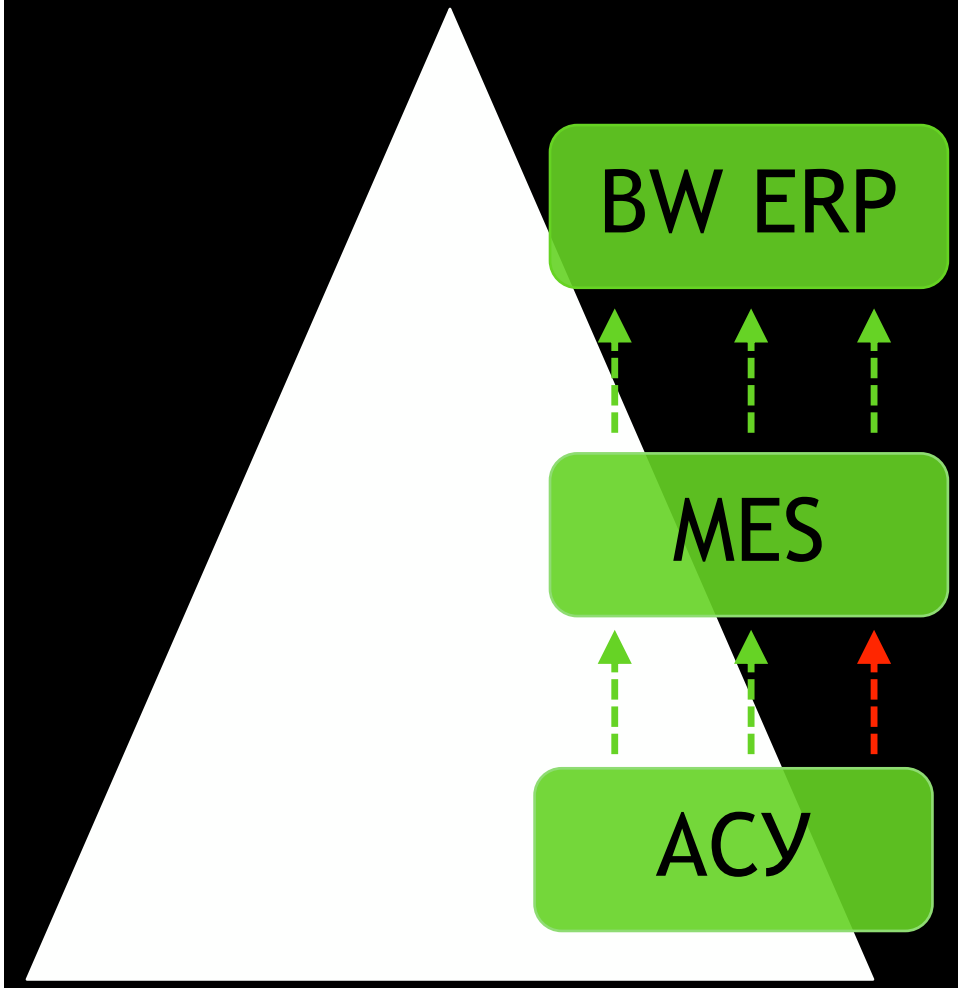




Бизнес-системам:

- ERP
- кадрового учета
- контрактации

Диспетчеризация производства



Корректность и целостность данных в пирамиде автоматизации

Часть данных передается автоматически и корректно

Часть данных – перегружаются из АСУ вручную

Кейс – найден обход процедуры/конфликт интересов

в АСУ есть необходимые данные для автоматического формирования табеля, но:

данные в ERP перегружаются вручную

KPI табельщика зависит от «качества» данных

данные «подгоняются» под нужные значения

На уровнях ERP и выше это было незаметно – слишком низкий уровень квантования

Топливо

VB-Trend 2019 plan>b VolgaBlob

Источники: системы диспетчеризации техники

Проблема:

В системе диспетчеризации есть подсистема безопасности, но нет контроля.

Причина/пример:

При отключенном датчике самосвал используется, а не простаивает.

Далее отчетность «подгоняется» под нужные значения.

Пример – топливо списывается вручную на сломанную технику.

Нерабочий тепловоз потратил 700л топлива.

SIEM обеспечит целостность данных - поможет обнаружить «подгонку значений»

Анализ закупочной деятельности

VB-Trend 2019 plan>b VolgaBlob

Источники: информация о договорах, конкурсах, заявках

Проблема: низкая прозрачность процесса

- Информация о заключенных договорах по видам деятельности
- Аналитика конкурсов
- Проверка контрагентов

Создание **«единого окна»** для принятия решений о работе с поставщиками

SIEM обеспечивает прозрачность и целостность процесса

Планы развития

VB-Trend 2019
plan>b
VolgaBlob

Создание **единой платформы** для аналитиков различных подразделений

Регламентированное хранение всех ключевых данных о бизнесе

Спасибо за внимание!

Вопросы?

VB-Trend 2019

plan>b

VolgaBlob

СУЭК