SOC Prime
Predictive Maintenance

IT Guard

ПОСТАВКА ПЕРЕДОВЫХ ТЕХНОЛОГИЙ
ЗАЩИТЫ ИНФОРМАЦИИ

SOC PRIME
POWER ON SECURITY

Predictive Maintenance

Статистика по 65+ SIEM проектам

- 30% всех SIEM проектов не имеют отдельно закрепленных сотрудников или максимум 1 сотрудник
- среднее количество SIEM команды – до 3 человек
- отсутствие выделенных администраторов
- большой спрос на опытный персонал по работе с SIEM
- низкий бюджет или его полное отсутствие на обучение
- текучесть кадров

IT Guard

SOC PRIME
POWER ON SECURITY

Predictive Maintenance

Решение - Автоматизация SIEM и SOC

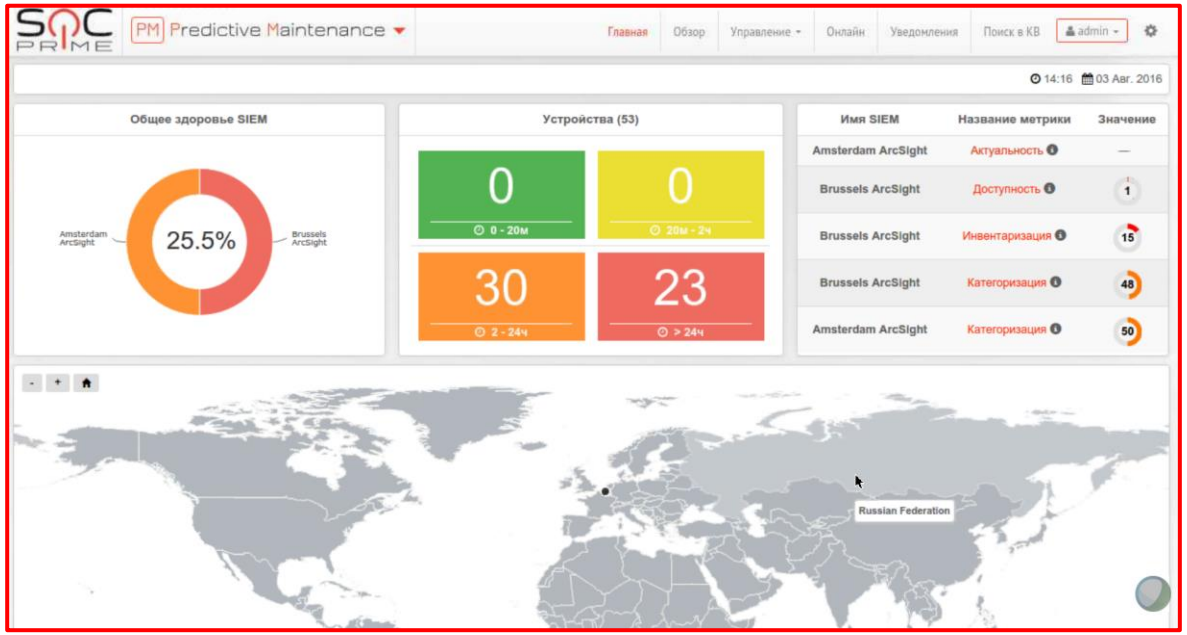
Predictive Maintenance - автоматизирует работу с ошибками, предоставляя оповещения об их возникновении, анализ их влияния, приоритеты по исправлению и подробные инструкции по устранению, пока они не переросли в проблемы.

- Эффективный мониторинг инцидентов
- Автоматизация рутинных процедур
- Повышение эффективности SOC
- Уменьшение загрузки персонала

SOC PRIME
POWER ON SECURITY

IT Guard

Predictive Maintenance



Predictive Maintenance – обеспечивает бесперебойную работу критически важных функций систем безопасности; устранить ложные сигналы и поддерживать точность работы SIEM на максимальном уровне, чтобы гарантировать непрерывность процесса предотвращение мошенничества и снизить риски финансовых потерь.

SOC PRIME
POWER ON SECURITY

IT Guard

Predictive Maintenance

Метрики, подтвержденные временем и практикой

7 метрик здоровья SIEM:

1). Доступность

2). Целостность

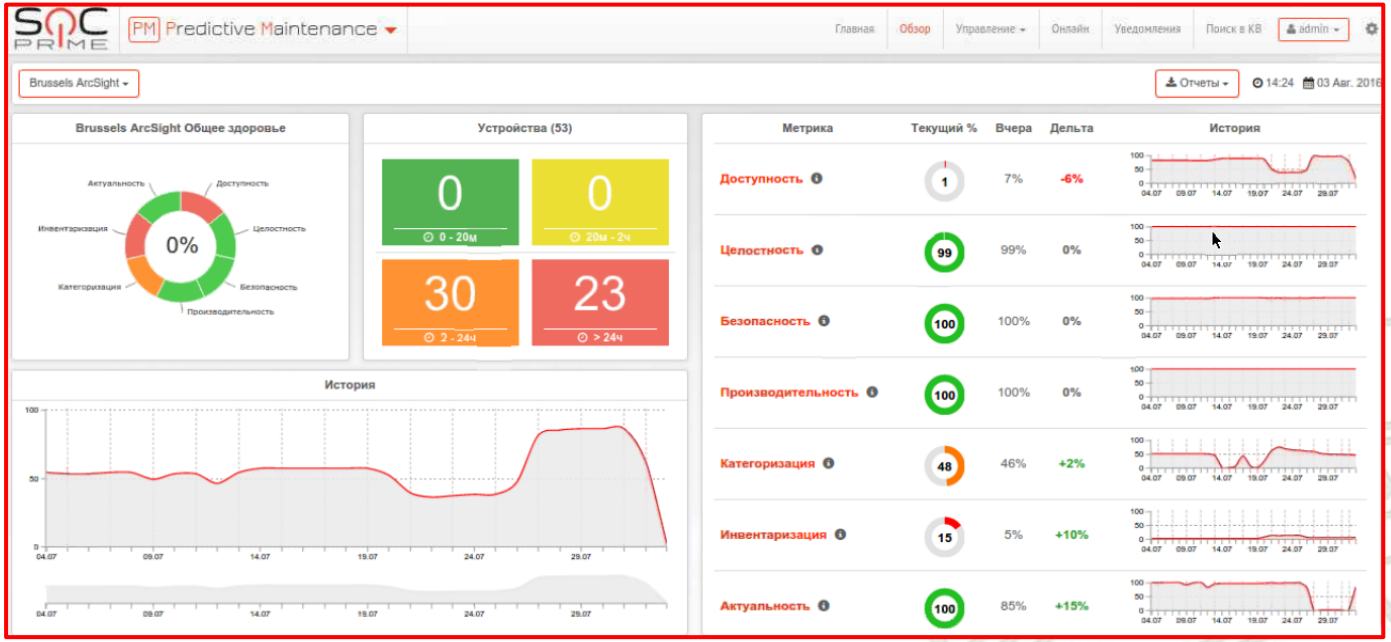
3). Безопасность

4). Производительность

5). Категоризация

6). Инвентаризация

7). Актуальность

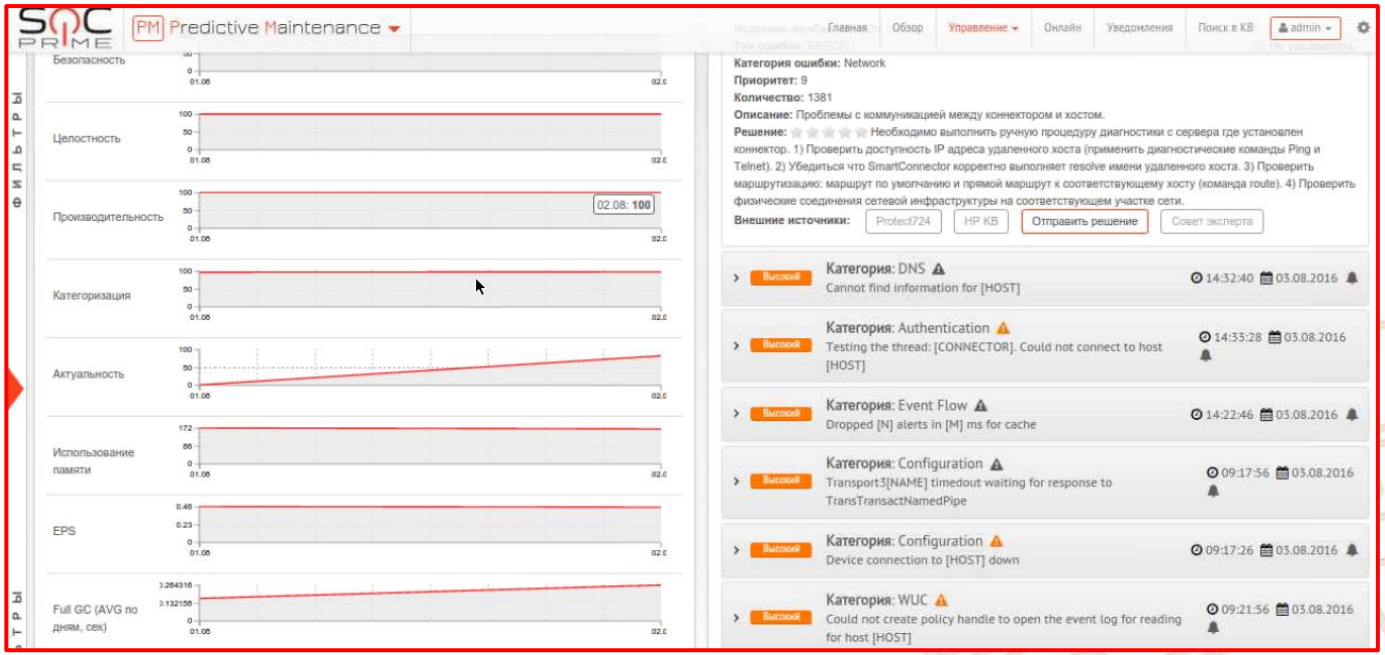


Predictive Maintenance

Детальная информация о работе SIEM

Информация об ошибках:

-название
-тип
-категория
-приоритет
-количество
-описание
-решение
-ссылка на внешние источники
(Protect 724, база HPE)



SOC PRIME
POWER ON SECURITY

IT Guard

Predictive Maintenance

Клиенты

motiv

EUROBANK

otpbank

SBERBANK
PUBLIC JOINT STOCK COMPANY

ISSP
Information Systems Security Partners

STAR LIGHT MEDIA

ВОЛЯ

UKRSIBBANK
BNP PARIBAS GROUP

Британская международная компания

Международная Австрийская банковская група

5 клиентов - ожидаем разрешение использования логотипа

SOC PRIME
POWER ON SECURITY

IT Guard

Predictive Maintenance

SOC Prime Predictive Maintenance

• Оптимизирует рабочее время персонала, автоматизируя рутинные процедуры;

• Обнаружение на ранних стадиях инцидентов безопасности и предоставление решений;

• Устранение ошибок с помощью оповещений и отчетов по нарушению информационной безопасности;

• Сокращение затрат на дополнительное оборудование для SIEM;

• Отличное решение на все требования соблюдения политик безопасности на целостность логов, их анализ и доступность.

SOC PRIME
POWER ON SECURITY

IT Guard

Predictive Maintenance

Лицензирование

Predictive Maintenance является отдельно стоящей виртуальной машиной, которая агентами собирает метрики с компонентов SIEM (менеджеры и коннекторы). Два вида лицензии – в облаке и локально у клиента. Лицензируется по количеству EPS или GB/day, обрабатываемых на SIEM. Минимум 250 EPS или 20 Gb/day, существуют Add-on по 50 EPS или 5 Gb/day. Лицензия на 1 год.

SOC PRIME
POWER ON SECURITY

IT Guard

Спасибо за внимание!