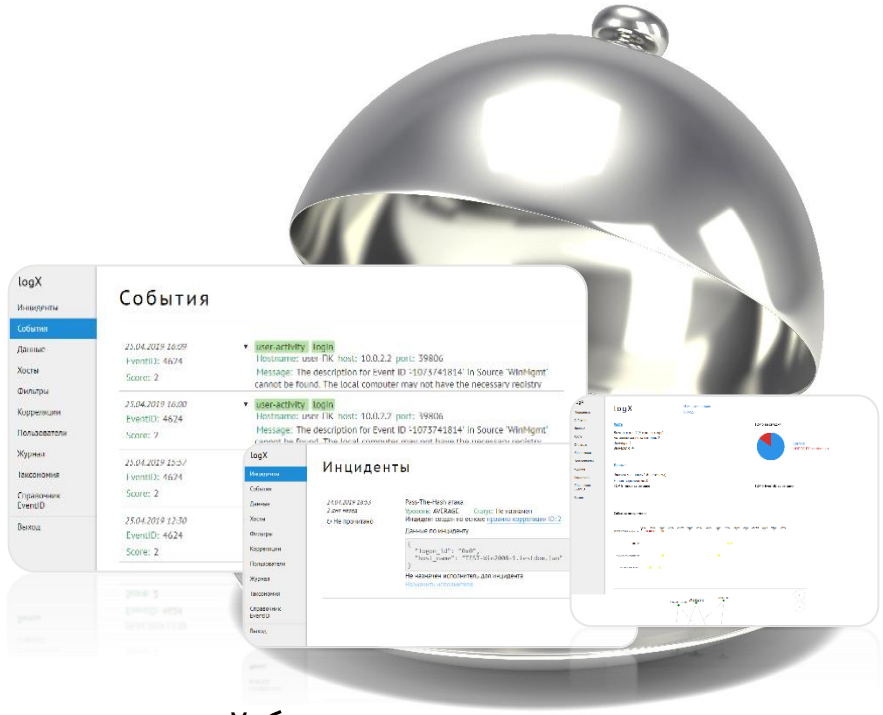
СИГНАЛТЕК

SIEM LogX



Решение для централизованного управления информационной безопасностью и событиями безопасности

Проблематика:

Подавляющее большинство действий, производимых в рамках целевой атаки, оставляют за собой следы в журналах сообщений. Однако, администраторы сети физически не могут отслеживать все события со всех рабочих станций в реальном времени.

LogX – решение для централизованного сбора, обработки и анализа событий из журналов сообщений.

Представляет из себя полностью готовый к использованию комплекс, оснащенный специальными фильтрами, и выявляющий аномалии в сети.

- Детектирование атак: отслеживает в реальном времени только самые важные события, касающиеся возможных угроз ИБ.
- Анализирует события в режиме реального времени и позволяет проводить ретроспективные проверки на наличие событий.