OTUS

Экспресс-курс «ELK»

Экспресс-курс по Elasticsearch, Logstash, Kibana

Длительность курса: 8 академических часов

1 Теоретический модуль

1	**Введение в ELK. Elastic Stack**	**Цели занятия:** 1.Как приложение пишет логи, когда и куда? 2.Типовые примеры работы с логами. 3.Проблематика хранения и анализа логов 4.Примеры использования (эксплуатация, тестирование, аналитика в реальном времени, аналитика по истории, аудит) 5.Устройство Elastic Stack 6.Как начать использовать Elastic Stack? 7.Механизмы сбора логов (из файлов, напрямую из приложения) 8.Практика структурирования логов 9.Сокрытие приватных данных при сборе логов 10.Работа с данными, язык запросов ElasticSearch 11.Визуализация в Kibana + XPack 12.Алертинг в Elastic Stack

2 Практический модуль

1	**Сбор и отправка лог данных и визуализация данных в Kibana. Подключение приложения к системе логирования и работа с преобразованием логов.**	**Цели занятия:** 1.Из приложения 2.Из файлов (конфигурация, beats) 3.Интеграция с коробочным ПО 4.Работа с поиском, поиск ошибок за период времени 5.Создание визуализаций по поисковым выборкам 6.Алертинг в ELK 7.Grok patterns 8.Преобразование типов данных