

ПРОГРАММА ОБУЧАЮЩЕГО КУРСА SOLAR DOZOR 7.10 | 22, 23, 24 НОЯБРЯ

Дата и время	Тема	Ведущий	Тезисы
22.11.2023 (среда) 11:00 – 13:00	Общий обзор DLP-системы Solar Dozor. Новости последних релизов	Андрей Щербаков, руководитель группы анализа и методологии	<ul style="list-style-type: none"> • Концептуальная и модульная архитектура Solar Dozor. • Инцидентная модель в DLP-системе. • Ролевая модель пользователей системы. • Инвентаризация содержимого файловых хранилищ. • What's new в релизе 7.10 Solar Dozor.
22.11.2023 (среда) 14:00 – 16:00	Проведение расследований с помощью Solar Dozor: кейсы из жизни заказчиков	Сергей Волгин, аналитик	<ul style="list-style-type: none"> • Жизненный цикл сообщений в DLP-системе. • Цели и задачи работы с архивом коммуникаций в целях проведения расследований. • Обновленная зона поиска в Solar Dozor: поиск в системе, быстрый поиск, шаблоны поиска, расширенный поиск и умный поиск. • Примеры расследований с помощью работы с архивом.
23.11.2023 (четверг) 11:00 – 13:00	Политика фильтрации Solar Dozor на страже безопасности: интересные приемы использования	Эра Бубликова, старший аналитик	<ul style="list-style-type: none"> • Политика DLP как технология анализа трафика. • Системные наборы правил политики в Solar Dozor. • Структура политики фильтрации в DLP: информационные объекты, политика, досье и справочники. • Инструменты политики фильтрации: шаблоны документов, цифровые отпечатки, идентификаторы и графические шаблоны. • Методика применения сочетания условий политики для построения сложных правил.
23.11.2023 (четверг) 14:00 – 16:00	Контроль действий сотрудников на рабочих станциях	Маргарита Филатова, ведущий аналитик	<ul style="list-style-type: none"> • Концепция и архитектура перехватчика Dozor Endpoint Agent. • Настройка перехватов действий пользователей рабочих станций. • Особенности применения агентской политики на основе пользователей, OU AD, групп безопасности AD, групп особого контроля. • Возможности нового агента по контролю WiFi и записи видео.
24.11.2023 (пятница) 11:00 – 13:20	UBA - анализ поведения сотрудников и выявление аномалий Личный кабинет ИБ	Екатерина Иванова, старший аналитик	<ul style="list-style-type: none"> • Концепция поведенческого анализа на основе данных DLP. • Показатели поведения сотрудников в целях выявления аномалий. • 20 паттернов поведения персон в модуле UBA Solar Dozor. • Методика работы с системой поведенческого анализа. • Примеры расследований при работе с UBA Solar Dozor. • Личный кабинет ИБ.