Практика

Предлагаю теперь взглянуть на нашу схему с точки зрения технической стороны менеджмента информационной безопасности.

Необходимо решить задачу рационального использования рассмотренных на уроке инструментов.

Исходя из вашей методички и тех знаний, которые вы получили на сегодняшнем уроке, я предлагаю вам сделать 10 минутный тест и направить его мне почтовым сообщением.

Формат теста:

	ФИО студента: Лешков И.А.	
№	**Наименование средства защиты**	**Цели, прикладное размещение и необходимость использования**
1	SIEM	Сбор информации о событиях и инцидентах в ИБ для прогнозирования потенциальных угроз и подготовки сценариев пентеста. Необходимо использовать на входах извне (например, в DMZ) и в инсайде it-ландшафта для более эффективной защиты и контролем за инцидентами, а также, для более эффективного планирования, управления ресурсами и минимизации финансовых потерь.
2	SOAR	Функции и технологии, дополняющие siem-системы через автоматизацию и агрегирование информации об угрозах безопасности. Необходимо использовать на входах извне (например, в DMZ) и в инсайде it-ландшафта для более эффективной защиты и контролем за инцидентами, а также, для более эффективного планирования, управления ресурсами и минимизации финансовых потерь.
3	IPS	Дополнение к IDS. Предотвращение вторжений посредством инструментов ИБ, а именно, обнаружение + автоматическая защита. Необходимо использовать на входах извне (например, в DMZ) с целью обнаружения вторжений и незамедлительного реагирования на них.
4	IDS	Система обнаружения, регистрации и оповещения о вторжениях. Необходимо использовать на входах извне (например, в DMZ) с целью обнаружения, категорирования и регистрации вторжений.
5	Инструменты защиты от НСД	Предотвращение утечек и компрометации чувствительной информации. Необходимо использовать внутри периметра it-ландшафта, как для пользовательских, так и для серверных сервисов для защиты и сохранности конфиденциальной информации.