Вопросы к экзамену по модулю «Поведенческий анализ»

|  |  |
| --- | --- |
| № | Вопрос |
| 1 | Аналитика поведения пользователей ("UBA"), по определению Gartner, — это процесс кибербезопасности, направленный на:   1. обнаружение внешних угроз, целевых атак и финансового мошенничества 2. **обнаружение внутренних угроз, целевых атак и финансового мошенничества** 3. обнаружение внутренних угроз, массовых атак и финансового мошенничества 4. обнаружение внутренних угроз, целевых атак и имущественного мошенничества |
| 2 | Решения UBA изучают модели поведения:   1. **людей** 2. машин 3. IoT-устройств 4. узлов в сети |
| 3 | Какой подход применяется в системах U(E)BA?   1. Датацентричный 2. **Человекоцентричный** 3. **Системоцентричный** 4. Событийноцентричный |
| 4 | Что означает E в аббревиатуре UEBA?   1. Essence (существо) 2. Existence (наличие) 3. **Entity (сущность)** 4. Effect (влияние) |
| 5 | UEBA может входить в систему:   1. **SIEM** 2. **SOAR** 3. Treat Intelligence 4. Все перечисленное |
| 6 | Преимущества UEBA от классических SIEM:   1. **Большая вероятность найти внутреннюю угрозу** 2. Простота интеграции 3. **Самообучаема** 4. Все перечисленное |
| 7 | Три столпа UEBA:   1. Конфиденциальность, целостность, доступность 2. **Решаемые задачи, данные, аналитика** 3. Очистка данных, моделирование, представление 4. Наследование, инкапсуляция, полиморфизм |
| 8 | Источники данных UEBA:   1. **Письма электронной почты** 2. **Журналирование систем** 3. **Публикации в социальных сетях** 4. **Телефонные разговоры с рабочего телефона** |
| 9 | С помощью UEBA возможно:   1. **Оценить угрозу действий каждого сотрудника** 2. Обеспечивать мониторинг производительности сущностей 3. Отправлять оповещения подозрительным сотрудникам 4. Ограничить доступ злоумышленнику |
| 10 | Решения UBA изучают модели поведения людей, а затем применяют алгоритмы и \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ для обнаружения значимых аномалий в этих моделях – аномалий, указывающих на потенциальные угрозы   1. иммунные системы 2. кластерный анализ 3. **статистический анализ** 4. методы машинного обучения |