# Поведенческий анализ. Рекомендации по проведению лекций.

Данные рекомендации прилагаются к презентации лекции «Поведенческий анализ».

Структура рекомендаций устроена следующим образом:

* Номер слайда
* Тезисы, рекомендуемые к обсуждению
* Дополнительная информация, ссылки на источники (опционально)

1. Тема лекции.
2. Что это? Определение Gartner (Если член Garnter: <https://www.gartner.com/en/documents/2831117>).
3. Смена парадигмы. Ориентир на людей и систему а целом, а не на защиту данных.
4. UBA или UEBA? Или же SIEM и SOAR?

* <https://blog.varonis.ru/user-entity-behavior-analytics-ueba/>
* <https://www.exabeam.com/siem/uba-ueba-siem-security-management-terms-defined-exabeam/>
* <https://www.cshub.com/executive-decisions/articles/unlock-hidden-threats-with-uba-and-ueba>
* <https://www.s3-uk.com/user-entity-behaviour-analytics-siem/>
* <https://www.securitylab.ru/blog/personal/80na20/342749.php>
* <https://xakep.ru/2020/09/10/trend-micro-xdr/#toc01>.
* <https://can-topay.medium.com/yet-another-soar-design-3278194a71f5>
* <https://www.paloaltonetworks.com/cyberpedia/what-is-ueba>

1. UBA или UEBA? Или же SIEM и SOAR?
2. Три столпа UEBA.

* <https://habr.com/ru/company/varonis/blog/468989/>
* <https://www.researchgate.net/publication/336259455_The_role_of_User_Entity_Behavior_Analytics_to_detect_network_attacks_in_real_time>

1. Что нужно знать при интеграции UEBA?

<https://www.logpoint.com/en/blog/ueba-user-and-entity-behavior-analytics/>

1. Источники данных UEBA

<https://www.splunk.com/en_us/data-insider/user-behavior-analytics-ueba.html>

1. Playbooks. Разработка сценариев атак на систему. Слабые места систем. Причинно-следственные связи. Определение целей обнаружения.
2. Поиск метрик и очистка данных. Влияние избыточности данных на ложное принятие решений.
3. Создание профилей пользователей и других сущностей.
4. Моделирование шаблонов поведения. Принцип формирования, группировки по необходимым направлениям.
5. Моделирование шаблонов поведения. Кластеризация пользователей на группы по поведению.
6. Определение нормального состояния. Обучение модели.
7. Корреляция событий и поведенческого шаблона.
8. Корреляция событий и поведенческого шаблона. Примеры отклонения от нормального поведения.
9. Регистрация отклонений. Привести примеры возможных отклонений. Регистрация может идти в SIEM, на базе которой располагается UEBA.
10. Обнаружение отклонений. Способы
11. Классификация вектора атаки. Таблица Mitre ATT&CK.

<https://xakep.ru/2021/03/17/mitre-att-ck/>

1. Классификация вектора атаки. Таблица Mitre ATT&CK русский вариант от Positive Technologies.
2. Оценка риска. Управление рисками компании на основе определения метрики у каждого субъекта. Аномальное поведение повышает уровень риска.
3. Оценка риска. Отслеживание изменения показателей. Превышение допустимого порога влечет оповещение сотрудников, которые специализируются на конкретной группе отклонений (администратор информационной безопасности, DLP-систем или же отдел кадров). Приоритезация событий дает быструю реакцию на инциденты, что позволяет предотвратить причинение ущерба.
4. Сценарии. Манипуляции с данными.
5. Как можно избежать? События, которые бы отслеживались UEBA.
6. Сценарии. Фишинговая атака.
7. Как можно избежать? События, которые бы отслеживались UEBA.
8. Community open-source UBA. Решении под лицензией GNU, не зависит от SIEM.

<https://openuba.org/>

<https://github.com/GACWR/ouba-paper/blob/master/openuba.pdf>

1. Вопросы.

Рекомендуется к ознакомлению:

Анализ поведенческих данных на R и Python / пер. с англ. А. В. Логунова. – М.: ДМК Пресс, 2022. – 368 с.