ПОВЕДЕНЧЕСКИЙ АНАЛИЗ, ВЫЯВЛЕНИЕ АНОМАЛИЙ И ОЦЕНКА РИСКОВ

Роман Ванерке
Руководитель отдела технических решений
АО «ДиалогНаука»

ДиалогНаука

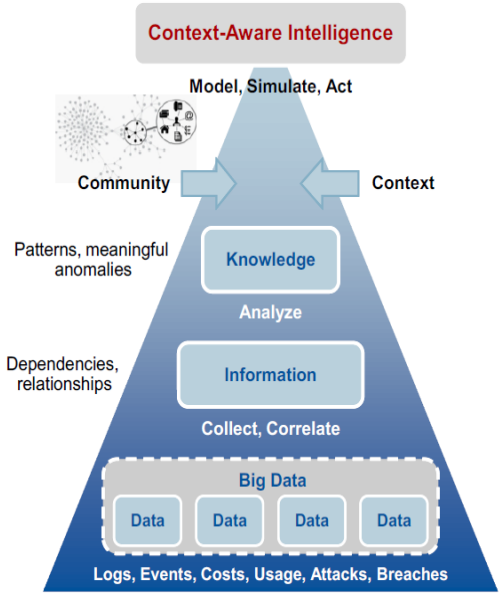
SOC-Forum

В чем проблема?

- **Внутренний пользователь** – самое слабое звено!
  - В последних атаках пользователь всегда был замешан или скомпрометирован
- Представьте, что злоумышленник в сети
  - Он будет обходить системы защиты, которые базируются на сигнатурах и контролируют периметр
- Объемы данных и границы расширяются
  - Отделы ИБ завалены оповещениями, которые если и приоритезированы, то не содержат контекста
- Эволюция угроз ИБ продолжается
  - Еще недавно долгое время угрозы переполнения буфера и SQL инъекций были в тренде, то сейчас уже Zero-day, целенаправленные атаки, инсайдеры …

Рекомендации аналитиков

- «Объемы анализируемых данных **будут увеличиваться вдвое** ежегодно после 2016»
- «К 2016, 40% организаций будут анализировать **не менее 10 терабайт** данных по сравнению с 3% в 2011»
- «Используйте UBA для **оперативного** выявления «плохих» учетных записей и поведения, **приоритезации** и **уменьшения** количества инцидентов, и **выстраивания** процесса расследования»
- «Интеграция технологий IAM и SIEM позволяют улучшить возможности по управлению пользователями и ролями, расширяют возможности мониторинга SIEM, что намного шире, чем каждое из решений по отдельности»



User Behavior Analytics станет частью SOC

- Традиционный подход SIEM:
  - Защита сети и периметра – эффективный, масштабируемый
  - Широкие возможности по сбору данных, нормализации и анализа контекста (сеть, приложения)
  - Выявление инцидентов (корреляция) на основе заранее подготовленных

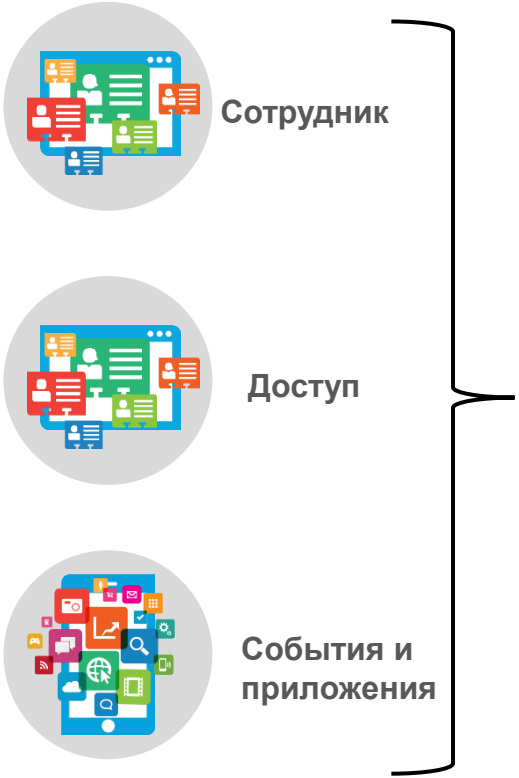
- **Являются** доверенными сущностями: сотрудники, партнеры
- **Имеют** (высокий риск) доступ к внутренним данным
- **Кто** злоупотребляет доступом и полномочиями, знает ценность данных, и знает о применяемых системах защиты
- **UBA** выявляет возникающие угрозы за счет аномального поведения в сравнении с его коллегами

Внутренний злоумышленник

- **Являются** продвинутыми злоумышленниками, действующими изнутри сети, тихо и незаметно
- **Имеют** скомпрометированные действующие учетные записи
- **Кто** нацелен на привилегированные учетные записи и конфиденциальную информацию
- **UBA** выявляет сложные угрозы за счет аномального поведения в сравнении с историческими данными с привязкой к данным сети, пользователя и периметра

Advanced Persistent Threat

Описание HP UBA



Процесс анализа HP UBA

Ключевые области решения HP UBA

Привилегированные пользователи

- Мониторинг угроз привилегированных пользователей
- Мониторинг угроз сервисных учетных записей

Защита приложений

- Выявление кражи данных
- Выявление фактов наблюдения за данными
- Выявление мошеннических действий

Сотрудник

- Мониторинг пользователя
- Контекстный анализ группы
- Статистический анализ
- Централизованный анализ по пользователями и расчет риска
- Внутренний злоумышленник и скомпрометированные учетные записи

Защита данных

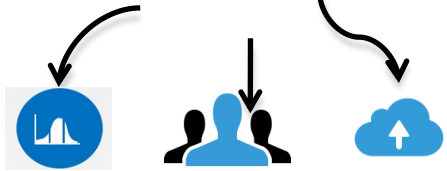
- Выявление утечки данных и защита
- Выявление наблюдения за VIP и защита

Анализ доступа

- Мошеннический доступ
- Анализ доступа с учетом уровня риска
- Анализ запросов на доступ с учетом уровня риска

Рассмотрим кейс

Иван, разработчик, который был атакован хакерами с целью получения доступа к исходным кода и кражи коммерческой тайны. Злоумышленники украли учетные данные Ивана, зашли в репозиторий и украли КТ.

	Компрометация учетки	Что было выявлено	Что было пропущено
Цель>>	 Иван Петров: Старший разработчик	✓ Фишингое письмо ✓ Отправка электронного сообщения на плохой внешний адрес	
Что>>	IAM HR AD LDAP  Имеет привилегированный доступ	✓ Доступ к репозиторию с исходным кодом	▪ Несоответствующий доступ приложения в сравнении с коллегами (группы) ▪ Аномальная активность событий VPN, неизвестные IP для пользователя
Как>>	ArcSight  Аномальное поведение; Аномалия группы; Подозрительная активность	✓ Авторизованный доступ к репозиторию с исходным кодом	▪ Привилегированный доступ из неизвестного источника ▪ Аномальные время доступа и частота ▪ Учетная запись выполняет действия, которые до этого не выполнялись ранее ▪ Аномальный файловый доступ в сравнение с коллегами (группой) ▪ Загрузка большого объема конфиденциальных данных

Что дает HP UBA?

Найти злоумышленника

Более быстрое решение событий

Приоритезация и расчет уровня риска

Эффективное расследование и визуализация

Влияние ROI 5-1

КАК HP UBA ДЕЛАЕТ ЭТО: КОНТРОЛЬ ПОВЕДЕНИЯ

Шаг 1. Выявление аномалий

Шаг 2. Определение нормального

Профилирование поведения пользователя для каждого приложения и источника событий

I. Поток транзакций и частота
II. Типы транзакций и процессов
III. Объемы транзакций (общее за час/день/неделю/месяц)
IV. Источники транзакций (обычные хосты)
V. Обучение и корреляция всех учетных записей к одному пользователю (личности)

Убедитесь, что «нормальное» поведение уже нескомпрометированно

I. Сравнение с коллегами: должность, руководитель, департамент, код позиции, тип системы, ОС, местоположение…
II. Если никто больше не делает X или имеет привилегии Y, то это отклонение и потенциальная проблема

Шаг 3а. Аномалии по пользователю

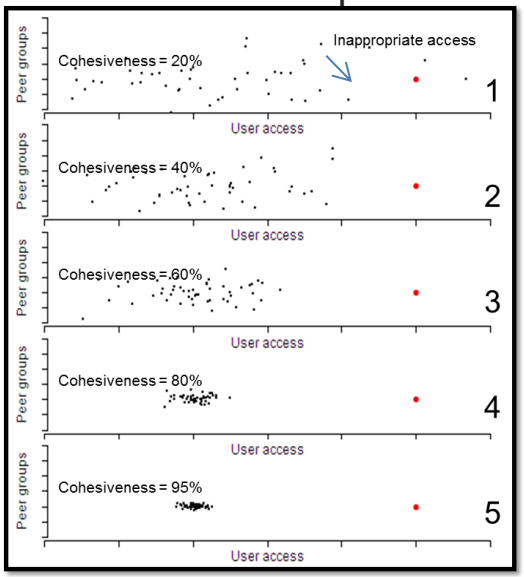
Шаг 3б. Аномалии по группе

Классификация всплесков

- Статистический расчет групповой связанности
- Риск, связанный с всплесками, увеличивается с учетом групповой связанности

Анализ группы

- Логически группы объединяются по ролям и зонам ответственности
- Выявление аномального поведения пользователя в сравнении с группой



Низкий риск

Высокий риск

Шаг 4. Выявление пользователей с наивысшем уровнем риска

Статический риск (критичность)

- Основан на анализе риска
- Критичные активы и приложения
- Права доступа и группы пользователей

Динамический риск (производный)

- Основан на уровне всплесков:
  - Нарушение политики
  - Подозрительное поведение
  - Сравнение с группой

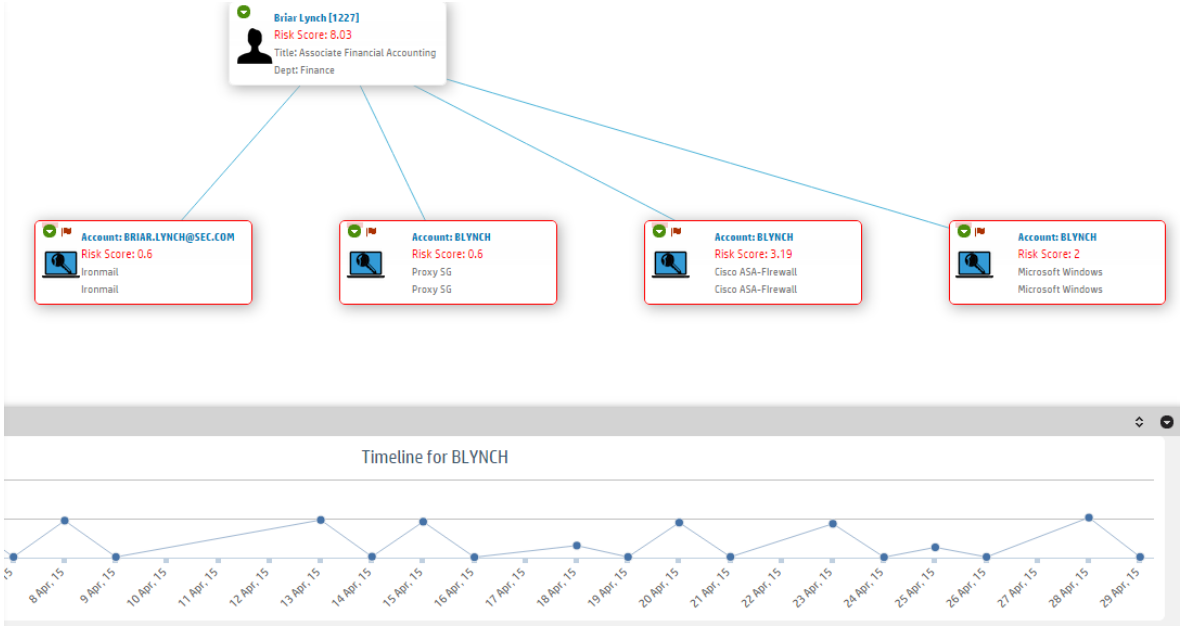
Дополнительные факторы (усилители)

- Тип сотрудника – по контракту или сторонняя организация
- Данные HR (плохие результаты работы, понижение)

Пользователи с высоким риском

Шаг 5. Анализ таких пользователей с помощью Анализа связей

- Графический интерфейс для анализа связей
- Возможность более детального изучения и расследования событий и пользователей



Выводы

- Выявление инцидентов ИБ за счет анализа поведения пользователя\группы пользователей и выявления отклонений в поведении в режиме реального времени
- Использование средств визуализации и детализации инцидента
- Снижение времени расследования и реагирования на инциденты
- Снижение рисков информационной безопасности за счет своевременного обнаружения и обработки инцидентов информационной безопасности

Вопросы?

Спасибо за внимание!

Роман Ванерке

rv@dialognauka.ru
+7 (495) 980-67-76, доб. 162

АО «ДиалогНаука»
http://www.DialogNauka.ru