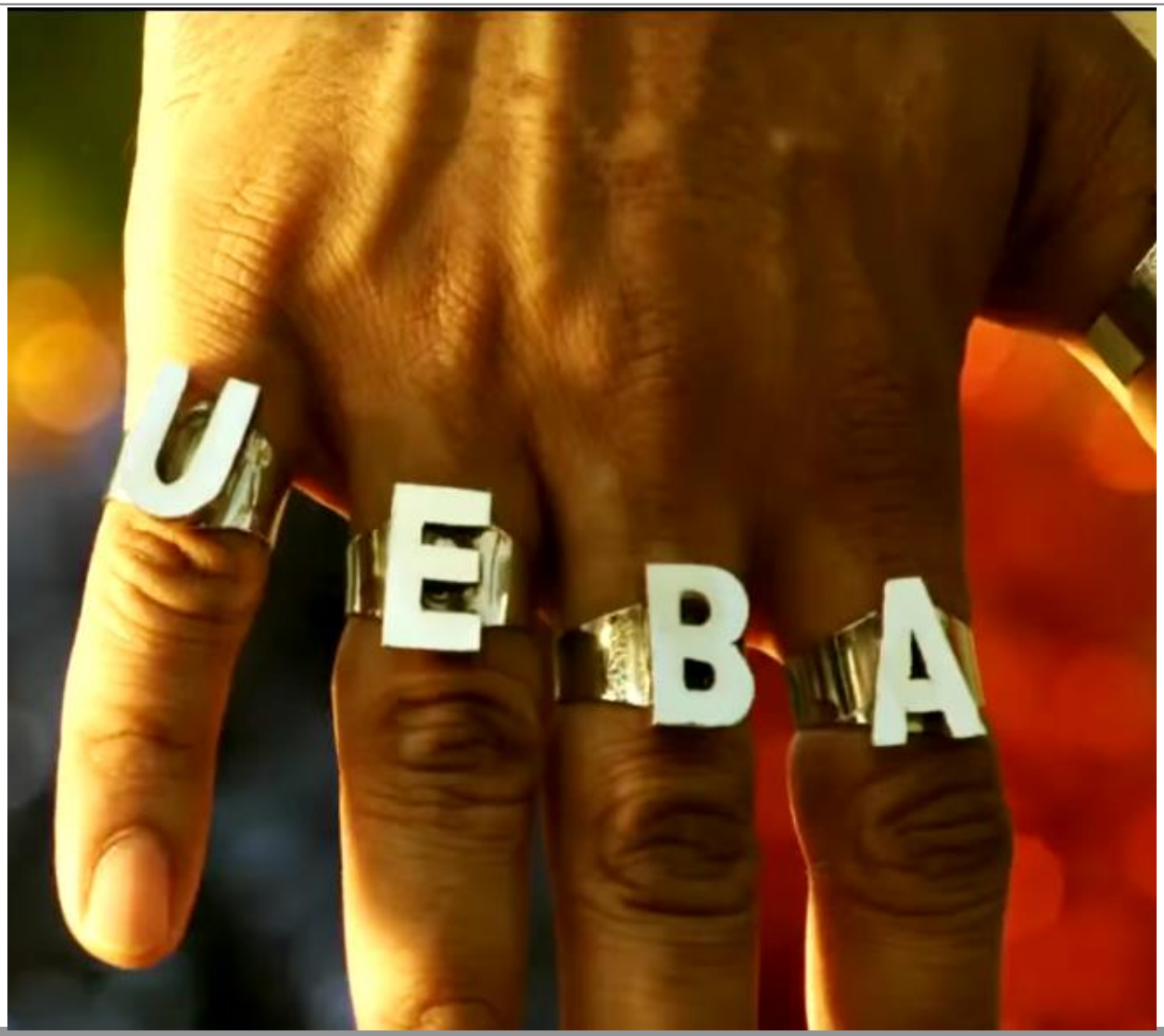
SOLAR SECURITY
software&services

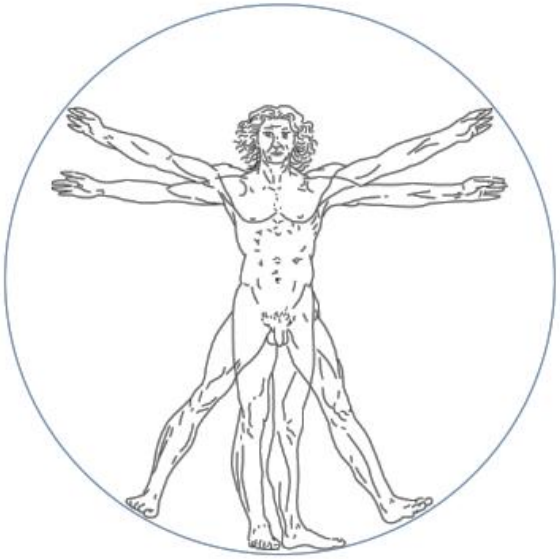
UEBA – поведенческий анализ, а не то, что Вы подумали

Андрей Данкевич
Люблю горячие ИТ тренды

Что русскому смешно, то Gartner-у — тренд



Смена парадигмы



Data-centric approach

People-centric approach

System-centric approach

Как UBA превратилась в UEBA

User Behavior Analytics ("**UBA**") по определению Gartner – это процесс кибербезопасности для детектирования внутренних угроз, целенаправленных атак и финансового мошенничества.

Решения класса UBA анализируют образцы поведения пользователей, применяя специализированные алгоритмы и статистический анализ для детектирования значительных аномалий в поведении, указывающих на потенциальные угрозы.

UEBA успешно детектирует подозрительную и злонамеренную активность, которая в противном случае остаётся незамеченной, кроме этого эффективно объединяет и приоритезирует уведомления с других средств ИБ.

Зачем нужны технологии UEBA

UEBA успешно детектирует подозрительную и злонамеренную активность, которая в противном случае остаётся незамеченной, кроме этого эффективно объединяет и приоритезирует уведомления с других средств ИБ.

Как жили до их появления?

Аналитик + SIEM

Подход к профилированию критичных хостов

- Сетевые коммуникации (включая локальные)
- Аутентификация в ОС и приложениях
- Работа с ключевыми файлами и объектами ОС
- Операции с приложениями/сервисами
- Факты изменения реестра

Пример Инцидента

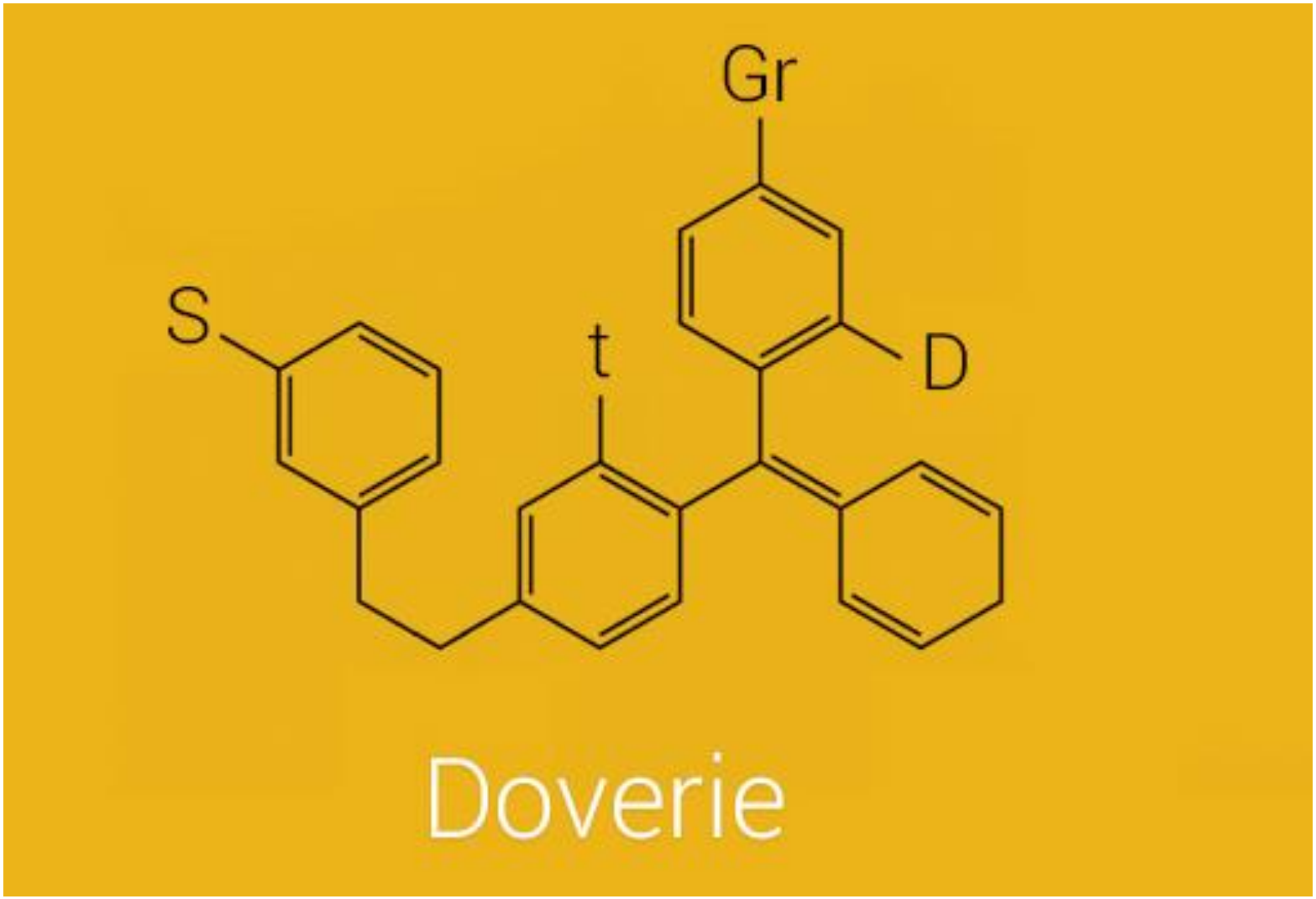
Фиксация инцидента

- Зафиксировано подключение к Windows серверу СУБД АБС под учетной записью ИТ-специалиста поддержки
- Учетная запись с доступом на все хосты, но специалист поддержки отвечает за UNIX
- Пользователь не подтвердил попытку доступа
- Вывод – учетная запись скомпрометирована

Итоги разбора

- Локализация атаки показала:
  - Найдена машина не в домене
  - На машине нет антивируса
  - Располагается на месте одного из сотрудников поддержки
- Внутренний злоумышленник
- Личный ноутбук с хакерскими утилитами, подключение к сети через подмену MAC
- Скомпрометированы:
  - Учетная запись системы мониторинга
  - 4 учетные записи администраторов
  - Около 20 хостов в инфраструктуре

Behavior Analytics
в DLP / Insider Threat Detection



Behavior Analytics в DLP / Insider Threat Detection

Уровне доверия - показатель, который присваивается каждому человеку в компании и отражает вероятность того, что данный сотрудник окажется нарушителем

- С точки зрения бизнес-поведения здесь применяются методы современной психологии, физиологии, социологии (2, 3).
- В качестве вычислительного аппарата рассматриваются методы математической статистики, случайных процессов, статистической физики – (4, 5, 6, 7, 8, 9). Отдельная ветвь моделей опирается на теорию нейронных сетей

Измеряемые факторы

- объем переписки
- количество событий и инцидентов ИБ
- распределение событий по группам персон особого контроля
- распределение сообщений по каналам коммуникации
- распределение событий по уровням критичности
- персоны, попавшие в отчет проведения пилотов или внедрений — реальные участники инцидентов безопасности
- и другие.

Формула неДОВЕРИЯ

Статистика + Социология + Специфика бизнеса

- традиционную модель авторегрессии с ошибкой в виде белого шума
- «слепое» разделение персон по группам

- халатные пользователи
- осторожные пользователи
- продвинутые пользователи

- лица, согласующие документы;
- лица, имеющие привилегированные права доступа;
- сотрудники, несущие материальную ответственность,
- и некоторые другие.

С точки зрения трудовых особенностей можно выделять персон в группы:

- сотрудники на аутсорсинге, подрядчики;
- бизнес-активные пользователи;
- сотрудники, находящиеся на испытательном сроке или, напротив, увольняющиеся.

Автоматическое определение >60%
от общего числа нарушителей,
независимо выявленных офицерами
безопасности в ходе расследований
и разборов инцидентов

Какие вендоры развивают UEBA

Некоторые UEBA вендоры больше ориентированы на работы с SIEM или DLP, в то время, как другие на IDM и IAM, или различные облачные приложения, в зависимости от их фокуса.

- **SIEM-щики.** Быстрое детектирование и аналитика опасных активностей, которые могли остаться незамеченными, приоритезация алертов и эффективная реакция на инциденты.
- **DLP-шники**. Усиливают DLP через выявление аномалий и продвинутую аналитику. Снижают число ложно-положительных и -отрицательных срабатываний, приоритезируют полученные инциденты. Для получения большего контекста интегрируются с веб прокси
- **IDM-щики**. Мониторят и анализируют поведение пользователей относительно выданных прав. Клиенты также используют UEBA для зачистки спящих аккаунтов и привилегированных пользователей, которые таковыми быть не должны.

UEBA для DLP

Bay Dynamics осуществляет профилирование и анализирует поведение пользователей, рабочих станций и приложений и коррелирует алерты.

- Bay Dynamics успешно агрегирует различные потоки (изначально начали с DLP с помощью интеграции с Symantec DLP), и поддерживает множество юз кейсов по выходу данных за периметр.
- Например, решение уведомляет об аномалиях в поведении привилегированных пользователей. В решении также есть модуль для понимания оперативной обстановки в организации - "attack surface."

Raytheon Forcepoint SureView Insider Threat (ex Websense) фокусируется на внутренних угрозах, решение осуществляет мониторинг активности сотрудников на рабочих станциях с помощью агентов.

- Решение использует рисковый скоринг для определения кратких списков сотрудников, чья активность является потенциально опасной.
- SureView Insider Threat помогает аналитикам удобный интерфейс анализа рискованного поведения пользователей с учётом контекста и инструменты снижения урона от подобного поведения.
- В дополнение к собственному аналитическому движку SureView интегрируется со сторонними платформами аналитики, например RedOwl Analytics.

UEBA для «всего» Securonix

- Securonix – первая в отрасли платформа Security Intelligence (2011), теперь позиционируют себя как UEBA
- В 2012 году названы Cool Vendor by Gartner
- 2011: McAfee and Securonix Partner on Data Loss Prevention for Enterprise Resource Planning (DLP for SAP)

Securonix – платформа класса Security Intelligence Platform для идентификации ИТ угроз с помощью продвинутой аналитики **прав доступа** и **поведения пользователей и систем** и интерпретации данных в понятные для бизнеса риски**.**
Службы информационной и экономической безопаности используют Securonix, чтобы усилить свои программы **борьбы с мошенничеством, оценки рисков**, **SIEM, IAM, DLP** благодаря быстрой и автоматической идентификации опасных **пользователей, ресурсов и активностей**

- Треть финансовых компаний в Fortune 100 и треть Fortune 500 – клиенты Securonix

К чему всё это приведёт

UEBA и Security Intelligence

- В июле 2015 **Splunk** купил UEBA стартап **Caspida** с небольшим числом клиентов за **$190M**
- В сентябре 2015 **Microsoft** купил **Adallom**, брокера облачных услуги с функциями UEBA и порядка 100 клиентами за **$250M**
- **HPE** предлагает **HPE ArcSight User Behavior Analytics** на базе технологий **Securonix**

Прогноз Gartner

К 2017 году минимум **4 UEBA** вендора с выручкой **<$50M** будут куплены крупными вендорами из **SIEM, DLP** или других сфера ИБ

Спасибо за внимание

Андрей Данкевич
a.Dankevich@solarsecurity.ru