Описание продукта

userinsight

UserInsight — обнаружение скрытых атак

Rapid7® UserInsight™ — самое эффективное решение для обнаружения и анализа атак, связанных с раскрытием учетных данных, действий от имени другого пользователя и постепенных атак.

Это единственное решение, позволяющее находить нарушения безопасности в локальных, облачных и мобильных средах, со встроенными аналитическими инструментами, способными выявлять изменения поведения, которые могут указывать на атаку.

Обнаруживайте атаки самых распространенных типов в своей сети и анализируйте их.

76 % атак связаны с раскрытием учетных данных пользователей, и 86 % специалистов по безопасности утверждают, что обнаружение инцидентов занимает слишком много времени.

Обнаружение и анализ нарушений безопасности и раскрытия учетных данных

Вашим пользователям грозит опасность. Кража учетных данных стала распространенным способом взлома сети, однако современные средства мониторинга практически не способны определять такие атаки. И проницательные руководители отделов безопасности понимают, что просто предотвращать их уже недостаточно.

Rapid7 UserInsightT — самое эффективное решение для обнаружения и анализа атак, связанных с раскрытием учетных данных, действий от имени другого пользователя и постепенных атак. Это единственное решение, позволяющее находить нарушения безопасности в локальных, облачных и мобильных средах, со встроенными аналитическими инструментами, способными выявлять изменения поведения, которые могут указывать на атаку.

Обнаружение — автоматическое определение нарушений безопасности и постепенных атак благодаря пониманию принципов действия злоумышленников. Проверка конечных систем без использования агента позволяет UserInsight находить то, что другие решения пропускают.

Анализ — сокращение времени анализа и предоставление полной информации о деятельности пользователей до и после каждого инцидента. Выявление всех вовлеченных лиц позволяет быстро отразить атаку.

Наблюдение — получайте полную картину деятельности пользователей в локальных, облачных и мобильных сетях без установки тяжеловесных прокси-серверов и систем управления устройствами.

201014

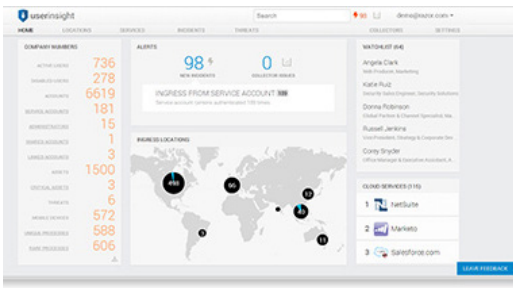
Штаб-квартира Rapid7 для Европы, Ближнего Востока и Африки
1st Floor, Building 1025, Arlington House, Reading, UK (Великобритания)

userinsight

UserInsight позволяет обнаруживать атаки, обычно остающиеся незамеченными:

«Меньше действий с момента обнаружения подозрительных действий до определения возможной атаки».

—руководитель отдела безопасности и рисков крупной некоммерческой организации



Обнаружение взлома — UserInsight не только обнаруживает распространенные атаки, но и запоминает поведение пользователей, что позволяет отмечать доступ пользователей к сети из необычных мест, обращение к критически важным ресурсам и попытки одновременного доступа пользователя к сети из двух разных точек. Сочетание правил и аналитики помогает легко обнаруживать попытки взлома без множества ложных срабатываний защиты.

Просмотр всех постепенных действий без установки агентов на конечные системы — оказавшись в сети, злоумышленники ищут привилегированные учетные записи и стараются действовать постепенно. Для выявления шаблонов таких атак необходимо наблюдать за конечными системами, а для этого в системах требуется установить агенты. Однако UserInsight позволяет проверять конечные системы без применения агентов, при этом обнаруживая постепенные атаки и неожиданное расширение полномочий. Обнаруживайте и устраняйте ранее незаметные атаки, такие как передача хеша.

Использование ловушек Honeypot для более тщательной проверки при каждом сканировании сети — после того, как злоумышленник получает доступ, ему требуется составить карту сети и определить дополнительные цели. Встроенные в UserInsight ловушки Honeypot могут повысить эффективность проверки сети и помочь остановить злоумышленников.

Локализация инцидентов путем выявления связи между действиями и конкретными пользователями — одной из главных задач при локализации инцидента является выявление всех вовлеченных в него пользователей и проверка того, изменилось ли их поведение после взлома. UserInsight позволяет связать пользователей с ресурсами и действиями, чтобы быстро получить ответ на вопрос: «Кто выполнил это действие?»

Выявление уязвимых ресурсов и пользователей — UserInsight использует данные об уязвимости, полученные от сканера Nexpose, показывая, ресурсы каких пользователей уязвимы и являются наиболее вероятными целями атаки. Обладая данной информацией, можно правильно расставлять приоритеты при реагировании на инциденты.

Наблюдение за привилегированными и ненадежными учетными записями — для перемещения по сети злоумышленники используют привилегированные, отключенные и машинные учетные записи. Для обеспечения безопасности важно внимательно наблюдать за такими учетными записями. UserInsight предоставляет аналитические данные об этих учетных записях и позволяет выявлять такие риски, как наличие учетных записей с чрезмерными правами или паролями с неограниченным сроком действия.