Рекламный проспект

Аналитика и большие данные
Безопасность

Поведенческая аналитика пользователей и объектов

Система поведенческой аналитики пользователей и объектов (UEBA) Micro Focus® Interset открывает новые возможности обнаружения, исследования и устранения скрытых угроз в вашей компании до наступления инцидента.

Используя машинное обучение, решение Interest UEBA трансформирует миллиарды событий в приоритизированный список высококачественных признаков безопасности, чтобы направить и ускорить работу центра управления безопасностью (SOC). Используемые в Interset модели машинного обучения в сочетании с удобным пользовательским интерфейсом сокращают время обнаружения и исследования угроз с нескольких недель до нескольких минут.

Преимущества решения Interset

Для многих организаций актуален вопрос защиты важных информационных активов — сведений о клиентах, интеллектуальной собственности, критически важных элементов управления инфраструктурой (или всего перечисленного). К сожалению, существующие подходы к защите этих активов регулярно демонстрируют свои ограничения, вынуждая службы ИТ-безопасности довольствоваться жесткой аналитикой на базе правил, фрагментированными экосистемами безопасности и бесконечным потоком оповещений, большинство из которых оказываются ложными тревогами. А между тем от этих служб требуют безупречной защиты от критических угроз, таких как эксфильтрация данных и несанкционированный доступ к сети.

Уникальность решения Interset заключается в том, что оно позволяет выявлять значимые угрозы на предприятиях, у которых есть ценные защищаемые ИТ-активы и большая поверхность мониторинга, но при этом ограниченные возможности службы ИТ-безопасности или финансовые ресурсы. В отличие от других решений, Interset UEBA не использует правила и пороговые значения, а вместо этого оценивает потенциальный риск пользователя или объекта в вашей организации, основываясь на математической вероятности и неконтролируемых моделях

Рис. 1. Interset UEBA по-новому анализирует существующие данные безопасности, чтобы выявить скрытые угрозы путем поиска аномального поведения. Это позволяет специалистам по ИТ-безопасности быстро и эффективно реагировать на угрозы и устранять их.

машинного обучения. Такой подход в сочетании с собственной архитектурой больших данных Interset позволит вашей службе ИТ-безопасности быстро и в больших масштабах выявлять угрозы.

Используя неконтролируемое машинное обучение (тип искусственного интеллекта, для которого не требуются метки), алгоритмы Interset извлекают доступные объекты (пользователи, компьютеры, IP-адреса, серверы, принтеры и т. д.) из файлов журналов и наблюдают за событиями, в которых участвуют эти объекты, чтобы определить ожидаемое поведение (показатель, который называется «уникальной нормой»). По мере поступления новой информации в процессе аналитики события сравниваются с ранее наблюдавшимся поведением для оценки риска.

Сценарии обнаружения угроз

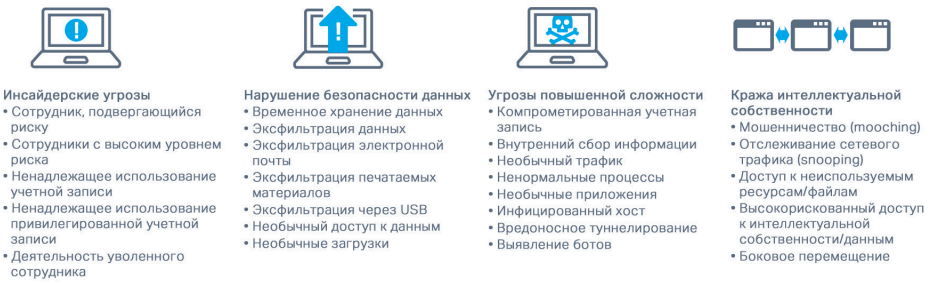


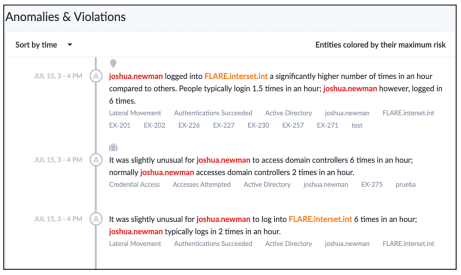
Рис. 2. Interset UEBA использует расширенные математические алгоритмы для постоянного отслеживания миллиардов точек данных и обнаружения индикаторов инсайдерских угроз, утечек данных, постоянных угроз повышенной сложности (APT), кражи интеллектуальной собственности и многого другого.

Благодаря таким базовым показателям и оценкам решение Interset UEBA повышает эффективность и скорость, с которой службы ИТ-безопасности обнаруживают, сортируют, исследуют и устраняют угрозы. Оценки рисков, выдаваемые решением Interset, можно использовать для инициирования действий в системах автоматизации, оркестрации и оповещения, что позволяет реагировать на возникновение рисков со скоростью, превышающей человеческие способности. Решение Interset также создает загружаемые отчеты, содержащие сводную информацию об актуальных организационных рисках.

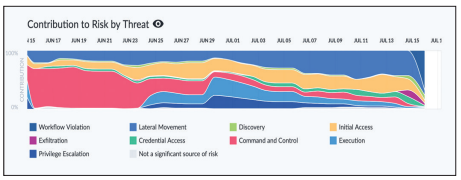
Визуализация рискованных объектов

Специалисты по ИТ-безопасности взаимодействуют с решением Interset через удобную и понятную веб-панель управления. На панели управления Interset пользователи могут быстро и легко определить, какие объекты представляют наибольший потенциальный риск. В случае выявления таких объектов на панели управления можно детализировать результаты, чтобы понять потенциальный риск в контексте созданных оповещений и, при необходимости, вызвавших их событий. На приведенных ниже снимках экрана показана детализация от списка самых рискованных пользователей до фактических событий.

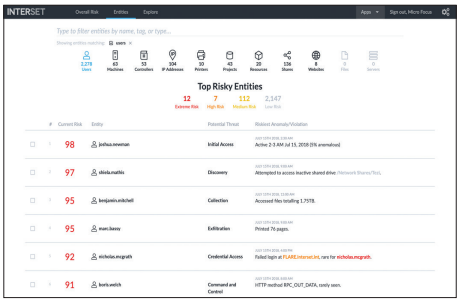
1. Просмотр всех объектов предприятия, сгруппированных по типу объекта, с отображением аналитической информации. На снимке экрана показан список пользователей, упорядоченный по убыванию оценки риска с самой высокой до самой низкой.



2. При просмотре каждого объекта на хронологической диаграмме отображается изменение его оценки риска. Такой способ представления показывает не только изменение оценки риска, но и в целом характеризует типы поведения, которые вызвали это изменение.



3. При просмотре объекта под хронологической диаграммой отображаются оповещения, связанные с этим объектом. Их можно фильтровать по связанным объектам и типам рисков. Кроме того, поскольку они отображаются в хронологическом порядке, связанном с хронологической диаграммой, можно легко составить описание меняющегося поведения в контексте других событий.



4. При нажатии на любое из этих оповещений можно провести исследование, чтобы показать событие в контексте базового поведения пользователя и других соответствующих объектов предприятия. Отображается риск, связанный с оповещением, и подробное описание модели, инициировавшей создание этого оповещения. Обратите внимание, что базовое поведение пользователя сравнивается с собой и с другими аналогичными объектами. Эти аналогичные объекты определяются при помощи статистически определенных одноранговых групп.

5. Фактические события, инициировавшие оповещение, можно просмотреть всего за один клик. Помимо просмотра фактического содержания файла журнала, ответственного за аналитику, пользователи могут с помощью этого интерфейса создавать дополнительные запросы.

Таблица 1. Снимки экрана панели управления Interset, на которых показана работа с аналитическими результатами