Обнаружение действий «Red Team» с помощью Interset UEBA

Система поведенческого анализа действий пользователей и активов (UEBA) Interset от Micro Focus позволяет использовать существующие события аудита Endpoint-систем для обнаружения неизвестных угроз. В крупном заказчике совместное использование технологий UEBA и EDR позволило выявить сложную атаку Red Team.

Система поведенческого анализа действий пользователей и активов (UEBA) Micro Focus Interset позволяет по новому взглянуть на существующие системы защиты endpoint для выявления трудно детектируемых угроз. В сочетании с EDR-решением, Interset, анализируя миллиарды событий, выявляет подозрительное поведение и предоставляет подразделениям информацилнной безопасности вызможность выявлять реальные угрозы.

Решение Interset выявило атаку «Read Team» на крупное предприятие

Read Teaming критически важен для эффективной стратегии кибербезопасности, он позволяет проверить навыки специалистов по выявлению и реагированию. Выявление подобных атак свидетельствует о вашей готовности обнаружить реальную атаку.

В одном из крупных заказчиков используя информацию с EDR-системы р процессах, активности пользователей и компьютеров, Interset позволил выявить хорошо подготовленную атаку Red Team. За короткое время были раскрыты поведенческие индикаторы атаки, и решение Interset раскрыло весь ее жизненный цикл и предоставило подразделению информационной безопасности необходимый контекст для реагирования.

Аномалии, выявленные Interset, позволили аналитикам следующие фазы атаки.

OWA Profiling	Злоумышленник использовал атаку по времени на Outlook Web Access (OWA) для обнаружения действительных учетных записей пользователей. Далее атака привела к внезапному повышению количества clear-text паролей, которое было выявлено по аномальной активности сервера OWA и типу входа.
Remote Exploit	Средства удаленной атаки, Mimikatz и CrackMapExec, были использованы на известном административном сервере и были Remote Exploit как аномальный процесс, выполняемый на сервере.
Reconnaissance	На один из ноутбуков администраторов был зафиксирован вход под скомпрометированной учётной записью, после чего хост инициировал поиск по всем доступным сетевым ресурсам файлов с паролями. Обнаруженные файлы складывались на скрытую общую папку ноутбука. На скомпрометированном ноутбуке был выполнен дамп части ветвей реестра. Эти признаки были выявлены на основании аномальной активности общего сетевого ресурса и большому количеству новых процессов.
Leteral movement	Взломанная учетная запись была использована для получения удаленного доступа к информационным активам соседних серверов и инициации дополнительных разведывательных атак, на что указали аномальный вход в систему с помощью учетной записи администратора и аномальные процессы на других компьютерах.
Password Guessing	Была выполнена вторичная атака для проверки использования пароля по умолчанию. Она заключалась в использовании сценария на Python для попытки маппинга сетевой папки каждой обнаруженной учётной записи с использованием пароля по умолчанию. Результатом этого стало множество выполняемых процессов и неудачных попыток аутентификации.
IP Address and Attack Tool	На последнем этапе была использована непрерывная серия атак на инструментарий управления Windows (WMI) на нескольких серверах. Она была обнаружена по аномальной активности процессов на атакуемых серверах и аномальному количеству процессов на компьютере, с которого была запущена атака. Interset сохраняет исходные события и позваляет использовать эту информацию в процессе расследования для определения инструментария атакующиего и хост инициатораю.