RSA

RSA NETWITNESS® UEBA 활용 사례

사용자 기반 위협에 대한 강력한 탐지 역량

RSA NetWitness UEBA는 빅데이터 중심으로 특별히 설계되고, RSA NetWitness Platform의 핵심 구성 요소로 통합된 사용자 및 개체 동작 분석 솔루션입니다. RSA NetWitness UEBA는 통계적 이상 징후 자율 탐지 기능 및 머신 러닝으로 알려지지 않은 위협을 동작에 기반하여 종합적으로 탐지함으로써 다양한 활용 사례를 해결합니다. RSA NetWitness UEBA는 공격 수명주기의 모든 단계에서 신속하게 탐지하고 유용한 분석 정보를 제공할 수 있도록 기존 보안 팀의 역량을 높입니다.

UEBA(User and Entity Behavior Analytics) 솔루션을 평가하는 경우 다음과 같은 중요한 특징 및 기능을 살펴보시기 바랍니다.

- 완벽한 자동화 및 지속적인 위협 탐지 및 모니터링
- 데이터 수집, 탐지, 조사 및 대응을 활용하여 전체 공격 수명주기 파악 가능
- MITRE ATT&CK™ 프레임워크에 부합하는 자연어 지표
- 제로 터치로 튜닝이 필요하지 않은 턴키 데이터 과학 모델을 지원하는 자율 머신 러닝
- 플랫폼의 핵심이며 로그 수집과 함께 엔드포인트 탐지 및 대응을 지원하는 엔드포인트 에이전트

엔터프라이즈급 UEBA의 핵심 기능

기본 데이터 수집

대부분의 SOC 팀에게 가장 큰 당면 과제는 온프레미스 시스템 및 클라우드 기반 시스템으로 구성된 기업의 방대한 포트폴리오에 의해 다양한 형식으로 생성된 모든 로그의 수집, 저장 및 분석을 관리하는 것입니다. RSA NetWitness UEBA는 이러한 시스템에서 원시 로그 데이터를 수집하고, 사용자 및 프로세스에 의해 다양한 소스에서 생성되는 활동을 동적으로 구문 분석하며, 이러한 데이터 소스의 관련 보안 정보를 해석함으로써 이 당면 과제를 해결합니다.

통합 메타데이터 분류 체계

UEBA 솔루션이 최적의 성능을 발휘하려면 로그, 네트워크 트래픽 및 엔드포인트 데이터를 캡처 시점에 구문 분석, 표준화 및 변환하여 일관된 통합 메타데이터 분류 체계로 전환해야 합니다. RSA NetWitness UEBA는 RSA NetWitness Platform Evolved SIEM의 핵심 구성 요소이므로 이러한 과정이 자동으로 이루어집니다.

머신 러닝 속도로 탐지

포인트 보안 솔루션의 위협 지표를 신뢰할 수 없거나 공격 식별에 일관되게 사용할 수 없는 경우가 너무 많습니다. 대부분의 경우 이러한 활동은 단독으로 이루어져 공격의 일부가 아니며, 이에 대해 알리는 것은 분석가에게 전혀 도움이 되지 않는 알림으로 업무 부담만 가중될 뿐입니다. RSA NetWitness UEBA는 시간 경과에 따른 활동 및 동작 패턴을 살펴보고, 머신 러닝을 사용하여 기준 동작의 편차를 식별하고, 거짓 양성으로 판명된 과거의 알림을 학습하므로 포인트 보안 솔루션보다 훨씬 구체적이고 실제 활용 가능한 알림을 생성합니다.

UEBA가 핵심 보안 요구 사항이 된 이유는 무엇입니까?

- 보고된 보안 침해 중 28%가 내부 행위자로부터 발생하며, UEBA를 통해 이러한 종류의 위협을 더 쉽게 탐지할 수 있습니다.
- 보고된 보안 침해를 유발한 상위 내부 행위자는 시스템 관리자 및 최종 사용자입니다.
- 보안 침해 중 68%가 발견에 2개월 이상 소요되었습니다. UEBA를 사용하면 보안 팀에서 위협을 더 빠르게 탐지할 수 있습니다.
- 보고된 보안 침해에서 상위를 차지한 활동은 도난당한 자격 증명과 권한의 남용 및 오용입니다. UEBA는 이러한 활동에 대해 알림을 제공하도록 설계되었습니다.

Verizon Data Breach Investigations Report 2018, Verizon.

자세한 정보

RSA.com/ko-kr/DoMore 방문 또는 데모 예약

RSA

RSA NETWITNESS UEBA가 탐지하도록 설계된 6가지 활용 사례

비정상적인 행위/변경

공격자가 AD(Active Directory) 도메인 또는 도메인 컨트롤러에 대한 액세스 권한을 획득하는 경우 공격자는 해당 액세스 권한을 활용하여 전체 AD 포리스트를 제어하거나 제거할 수 있습니다. 공격자가 단일 도메인 컨트롤러만 손상했더라도, 해당 컨트롤러에 대한 수정 사항이 다른 모든 시스템으로 복제될 수 있습니다. RSA NetWitness UEBA를 통해 분석가는 계정이 손상되었거나 중요한 디렉토리 데이터를 손상 또는 파괴하는 데 사용될 수 있는 AD 도메인에 대한 사용자 활동량의 급증을 식별하여 이러한 유형의 시나리오를 탐지할 수 있습니다.

비정상적인 권한이 있는 사용자 액세스

RSA NetWitness UEBA를 통해 권한이 있는 사용자가 내부자 위협을 가할 수 있는 시기를 파악할 수 있습니다. 예를 들어 헬프 데스크 기술 지원 담당자가 "정상적인" 루틴과 확립된 보안 정책을 벗어나 새 사용자의 암호가 만료되지 않도록 구성하기 시작하면 RSA NetWitness UEBA가 이를 포착합니다.

스누핑

스누핑이란 다른 사용자 또는 기업 데이터에 대한 무단 액세스를 말합니다. 중요한 기업 정보를 찾아 획득하기 위해 일반적으로 내부 사용자 또는 외부 공격자가 액세스 권한이 없는 서버 및 폴더 위치를 탐색하려고 시도하는 과정이 수반됩니다. 정교한 스누핑은 컴퓨터의 작업을 원격으로 모니터링하거나 자동 파일 검색을 수행하는 맞춤형 프로그램을 활용합니다.

RSA NetWitness UEBA는 다음과 같은 다양한 방법으로 스누핑을 탐지할 수 있습니다. 합법적인 액세스 권한이 없는 사용자가 데이터 액세스에 성공한 시도와 실패한 시도를 포착합니다. 솔루션이 새 위치에서 짧은 기간 내에 비정상적으로 많이 이루어진 성공 및 실패한 파일 액세스 시도를 식별하면 알림을 트리거합니다.

무차별 대입 인증

정교한 UEBA 솔루션은 다른 비정상적인 사용자 활동을 고려하여 실패한 인증을 검토함으로써 실제 무차별 대입 공격과 거짓 양성에 해당하는 인증 실패를 구별할 수 있습니다. RSA NetWitness UEBA는 반복적인 인증 실패와 함께 다른 의심스러운 동작 패턴을 탐지하는 경우에만 알림을 트리거합니다. 이로 인해 네트워크 구성의 결함이나 사용자의 암호 입력 실수와 관련된 거짓 양성을 제거할 수 있습니다.

머신 러닝에 의한 조치

RSA NetWitness UEBA는 악성 프로그램이 손상된 자격 증명을 사용하여 제한된 기업 리소스에 액세스하려고 할 때 이를 탐지할 수 있습니다. 사용자 프로파일링은 무차별 대입 공격의 징후를 포착하지만, 개체 프로파일링은 단일 디바이스 또는 IP 주소를 통해 수백 개의 계정에서 이루어진 과도한 활동 또는 모두 악성 프로그램이 설치된 단일 디바이스를 통해 여러 컴퓨터에 걸쳐 자행된 파일 이름 변경 등 의심스러운 개체 동작의 급증을 포착할 수 있습니다.

권한 상승

공격자는 조직의 일반 사용자, 네트워크를 더욱더 악용하기 위해 자신에게 높은 권한을 부여하기보다는 더 쉬운 타겟을 활용하려고 시도할 것입니다. 권한이 있는 사용자의 활동, 액세스 권한 부여, 중요 그룹 등을 면밀히 모니터링하는 일은 자격 증명이 손상되지 않도록 방지하는 데 매우 중요합니다. 그러나 권한이 있는 사용자는 항상 "정상적인" 동작의 정해진 패턴을 따르지 않으므로 거짓 양성이 불가피합니다. 따라서 지표의 축적을 식별, 수집 및 구문 분석하는 것은 악의적인 동작을 정확히 파악하는 데 매우 중요합니다.

따라서 행위자가 여러 번 인증에 실패한 후 비정상적인 위치로부터 로그인한 상태에서 권한이 상승된 경우, 높은 권한을 보유한 새 사용자 계정을 생성하면 주요 알림 목록 내에서 고위험으로 표시됩니다.

보안 스택에 다른 포인트 솔루션(이 경우 UEBA)을 추가하기 전에 진정으로 가치를 높일 것인지, 아니면 단순히 무의미한 정보만 생성할 것인지를 자문해 보시기 바랍니다. RSA NetWitness UEBA의 이점은 단일 플랫폼 내에서 기존 위협과 함께 중요한 사용자 기반 이상 징후를 탐지한다는 것입니다.