Tanium Software Bill of Materials (SBOM)

몇 초 안에 소프트웨어 공급망 취약점 파악

Tanium Software Bill of Materials (SBOM) 기능은 단일 Tanium 에이전트를 통해 복잡한 소프트웨어 환경에 대한 실시간 가시성을 제공하고 기업은 보다 정확한 정보를 통해 엔드포인트 위험 관리에 대한 의사 결정을 할 수 있습니다.

Tanium SBOM을 구성하면 환경 내 모든 소프트웨어 응용 프로그램에 대한 세부 정보와 취약한 패키지의 있는 위치를 알 수 있습니다. 또한 기업 전체 환경에 대한 궁금한 사항을 Tanium SBOM에 질문 할 경우, 원하는 답변을 신속하게 얻을 수 있습니다.

긴박한 질문에는 신속한 답변이 필요합니다.

제로데이 취약점이 식별되면 기존 툴을 사용하여 엔드포인트의 모든 인스턴스를 검색하는데 2주가 소요됩니다. 다음과 같은 작업은 매우 복잡합니다.

- 정확한 소프트웨어 패키지의 위치 파악
- 응용 프로그램이 사용하는 오픈 소스 연관성(있는 경우) 파악
- 실행 중인 소프트웨어 패키지 버전 확인
- 다른 응용 프로그램이 소프트웨어 패키지를 사용하는지 확인
- 위의 모든 것을 런타임에 신속히 파악

OpenSSL과 같은 중요한 제로데이 취약점이 발표되면, 경영진은 이와 같은 질문을 할 것입니다. "우리 조직에게 영향이 있습니까?" "OpenSSL을 사용하는 애플리케이션이 있습니까?" 만약 사용중이라면, "어떠한 애플리케이션에 사용중입니까?" "문제를 해결하는데 얼마나 걸립니까?"

여러분은 이와 같은 질문에 정확하고 신속하게 답변해야 합니다, 그런데 가능하신가요?

Linux Foundation에 따르면평균 1개의 응용 프로그램 개발 프로젝트를 수행하는 데에는 약 80개 이상의 직접 연관성이 있는 오픈소스가 사용되고, 여기에는 일반적으로 50개의 취약점이 포함되어 있습니다. 문제는 이 중 취약점의 40%가 패키지 속에 숨어 있어 찾기가 어렵다는 것 입니다.

복잡한 소프트웨어 패키지에 대한 실시간 가시성을 확보하여 위험을 더 잘 관리 할 수 있습니다.

가시성 (Visibility)
모든 소프트웨어 패키지 파악
클릭만으로도, 런타임에 있는 모든 라이브러리, 오픈 소스 프리웨어, 소프트웨어 패키지를 식별할 수 있습니다.

제어 (Control)
고도화된 수준의 결정을 할 수 있게 지원
조직에서 원하는 수준의 결정을 할 수 있도록 세부적이고 정확한 정보를 제공합니다.

조치 (Remediation)
어플리케이션 리스트 중심으로 수행
조직에 가장 적합한 방법으로 조치를 취할 수 있습니다.

가시성 확보및 제어로 소프트웨어 공급망 위험으로부터 벗어 날 수 있습니다.

런타임에 있는 모든 소프트웨어 구성요소를 파악합니다.

Tanium SBOM은 Java, JavaScript, Python, PHP, Ruby, GoLang-Binaries, OpenSSL 공유 라이브러리에 어떤 패키지가 있는지 확인 할 수 있도록 지원합니다.

예를 들어, Log4J, Open SSL과 같은 인스턴스를 조직 환경에서 식별 했을 경우, 다양한 헌팅 방법을 사용하여 전체 자산에 어디에 위치하는지 확인 할 수 있습니다. 또한 단일 콘솔에서 이 모든 작업을 수행 할 수 있습니다.

- 다른 취약점이 발표 되었을 경우, 해당 문제를 해결 할 수 있는 데이터를 제공합니다.
- 실시간으로 필요로 하는 세분화된 정확한 데이터를 제공함으로써, ServiceNow 와 같은 다른 툴에 대한 투자를 극대화 할 수 있습니다.

소프트웨어에 조치를 취합니다

오픈 소프트웨어 패키지에 영향을 받는 어플리케이션을 찾았을 경우, 필요에 따라 패치 적용 등과 같은 조치를 취할 수 있습니다.

Tanium이 제공하는 엔드포인트에 대한 모든 세부적인 데이터와 리스크를 기반으로 결정을 내릴 수 있습니다. 사용 중인 디바이스를 종료할지, 또는 디바이스 리스트에 따른 각각의 조치를 취할지 결정할 수 있습니다.

- 조직의 위험 허용 범위와 엔드포인트에 대한 정보 기반으로 결정을 내립니다.
- 디바이스 사용 중지, 프로세스 중지, 혹은 어플리케이션 전체 삭제 등과 같은 조치를 어떻게 취할지 결정 할 수 있으며, 사용된 세부적인 데이터를 통해 각각의 조치가 어떠한 영향을 끼칠 수 있는지 확인 할 수 있습니다.

소프트웨어 공급망 위험으로부터 조직을 보호 하십시요

어떠한 오픈 소프트웨어 공급망 취약점이 발표 될지 알 수는 없지만, SW 애플리케이션이 어떠한 영향을 받을 수 있는지 데이터에 액세스 할 수 있습니다. 이후 문제 발생 시 단일 콘솔에서 해당 문제를 해결 할 수 있습니다.

- 디바이스 사용 중지가 필요한지 확인합니다.
- 필요한 경우, 프린터 스플러와 같은 특정 프로세스를 종료 합니다.
- 영향을 받을 수 있는 디바이스 목록에 따라 조치를 취합니다.
- 애플리케이션에 패치 업데이트를 합니다.
- 애플리케이션의 새 버전을 배포합니다.
- 위의 모든 작업을 실시간으로 처리합니다.

Tanium SBOM은 Tanium 통합 엔드포인트 관리(XEM) 플랫폼의 핵심 구성요소입니다.

Tanium 플랫폼은 단일 에이전트에서 포괄적인 IT 운영 및 보안 관리를 제공합니다. 규모나 IT 복잡성에 관계없이 완벽하고 정확한 실시간 엔드포인트 데이터를 제공하고 최소한의 인프라를 사용합니다. Tanium XEM은 조직의 엔드포인트 위험을 지속적으로 관리하는 데 필요한 가시성과 제어 기능을 제공합니다.

지금 데모를 요청하십시오

Tanium 체험하기

업계 유일의 통합 엔드포인트 관리(XEM) 공급자인 Tanium은 복잡한 보안 및 기술 환경 관리에 대한 레거시 접근 방식의 패러다임 전환을 주도합니다. Tanium만이 IT, 컴플라이언스, 보안 및 위험을 단일 공유 목적을 위한 공통 분류, 장치 전반에 걸친 포괄적인 가시성을 제공하는 단일 플랫폼으로 통합하여 사이버 위협으로부터 모든 팀, 엔드포인트 및 워크플로를 보호합니다. 즉, 중요한 정보와 인프라를 대규모로 보호합니다.

포춘지 선정 100대 기업의 절반 이상과 미군은 사람들을 보호하고, 데이터를 방어하고, 시스템을 보호하고, 어디서나 모든 엔드포인트, 팀, 워크플로우를 확인하고 제어할 수 있는 Tanium을 신뢰합니다. 이것이 Power of Certainty 입니다.

www.tanium.com 을 방문하고 LinkedIn 및 Twitter를 팔로우하십시오.

© Tanium 2023