Cygna DDI Guard

DHCP 및 DNS 트래픽의 가시성 향상

Log 스크래핑 없는 모니터링

DNS 및 DHCP 활동 모니터링 및 보고의 전통적인 방법은 대량의 큰 로그 파일을 수집하고 그들을 해석하기 위해 다양한 도구나 스크립트를 사용하는 것이었습니다. 그 출력의 결과와 품질은 제한적이고, 데이터는 단지 과거 흐름과와 트렌드에 기반하였습니다.

DNS와 보안에 대한 관심이 높아지면서 컴플라이언스 준수 및 감사 요구사항을 충족시키기 위해 상세한 활동 데이터를 수집할 필요가 증가하고, 이러한 데이터는 보안 정보 및 이벤트 관리(SIEM) 제품이나 검색가능한 아카이브 형태로 저장될 필요가 생겼습니다.

DDI Guard는 이러한 요구사항을 해결할 수 있도록 설계되었으며 DNS와 DHCP 활동을 수집하여 보고 및 경고 기능을 제공하고 타사 SIEM제품과 통합 가능하며, 선택 사항으로 검색 가능한 아카이브 모듈을 제공합니다. 이러한 데이터는 감사 자료의 주요 부분이며 다른 네트워크 관련 정보와 보완하여 활동의 전체 감사 자료를 제공합니다.

SIEM 데이터의 비용 절감

DNS 및 DHCP 관리자는 수동 프로세스를 사용하거나 전사 SIEM 제품과 같은 복잡한 도구에 액세스할 필요 없이 DDI Guard를 사용하여 간단한 웹 기반 그래픽 사용자 인터페이스를 통해 DNS 및 DHCP 서비스를 보고하고 모니터링할 수 있습니다. SIEM 제품을 사용하는 경우, 종종 로그 데이터 양을 기준으로 비용을 청구하므로 DDI Guard를 구성하여 데이터 필터링을 사용해 로깅으로 전송되는 데이터 양을 현저히 줄일 수 있습니다.

DNS 및 DHCP 관리자는 무허가 클라이언트, 잘못 셋팅된 응용프로그램을 식별하거나 특정 DNS/DHCP 서버를 사용하는 클라이언트를 식별하려고 하는 경우가 많습니다(예, 서비스 해제 목적으로). 또한 경고는 다양한 경고 메커니즘을 통해 주요 이벤트가 관련 직원/시스템에 즉시 통보되도록 하는 자동화된 솔루션을 제공합니다.

멀웨어 위협의 탐지와 차단

악성 소프트웨어(멀웨어)를 탐지하기 위해 위협 탐지 및 완화 제품 산업 전체가 성장했지만, 매일 새로운 변종이 끊임없이 탐지됨에 따라 이러한 탐지 및 완화 시스템을 지속적으로 업데이트해야 합니다.

위협 완화 제품이 제대로 작동하더라도 멀웨어 작성자는 DNS 리소스 레코드를 통해 복제 및 확산하거나 멀웨어가 추가 "지침"을 얻기 위해 인터넷에서 "Command and Control"(C2) 서버를 찾는 방법으로 DNS를 통신 채널로 점점 더 많이 사용합니다.
일반적으로 DNS는 차단하거나 필터링 하지 않기 때문에 멀웨어 제작자들은 이를 악용하려 시도합니다. DDI Guard는 알려진 악성 도메인에 대한 쿼리가 감지될 경우 경고할 수 있도록 설계되어 있습니다.
게시된 악성 도메인 차단 목록들은 DDI Guard에 로드되어, 의심스러운 활동에 대한 즉각적인 경고를 제공하여 DNS 방화벽을 보완합니다.

주요 기능

- DNS/DHCP 패킷 캡처 – DDI Guard는 모니터링 할 DNS/DHCP 서버마다 수집기 설치를 필요로 합니다. 이것은 프로토콜 수준에서 패킷 캡처를 수행하므로 일반적으로 어떤 유형의 DNS/DHCP 서버를 사용하느냐는 중요하지 않습니다. 또한 성능에 영향을 미칠 수 있는 DNS 또는 DHCP 서버의 추가 구성이 필요하지 않습니다. (예, query logging을 활성화할 필요가 없음)
- Multi-vendor support – DDI Guard는 해당 Appliance Management Systems을 통해 VitalQIP 및 N3K runIP 장치로 배포할 수 있는 패키지로 제공됩니다. 대부분의 RedHat Linux 및 Windows 시스템에도 설치할 수 있습니다.
- 중앙 집중식 모니터링 – DDI Guard에는 데이터를 이해하는데 도움이 되는 정렬 가능한 열 및 세분화된 필터가 포함된 직관적인 UI가 있습니다.
- 데이터 필터링 – 필터를 결합하여 표시되는 데이터 양을 줄이고 SIEM 시스템으로 전달할 수 있습니다.
- 단일 뷰 – 다중 DHCP/DNS 장비 전체에 대한 통합 뷰를 제공합니다.
- 양방향 – 쿼리 및 응답 데이터 캡처를 수행합니다.
- 아카이빙 – 선택 사항으로 장기 데이터 아카이빙 및 컴플라이언스 준수 및 분석을 위한 검색이 가능합니다.
- Logging – Syslog 프로토콜을 통해 실시간 데이터 스트리밍을 수행합니다.
- 커스터마이징 가능한 대시보드 위젯 제공

DDI Guard의 이점

DDI Guard는 회사의 여러 조직내 관계자에게 다음과 같은 이점들을 제공합니다.

- IT운영자에게 DDI Guard는 DNS/DHCP 사용 추세에 대한 모니터링을 제공하고, 악용된 네트워크 장치 및 트래픽 이상을 식별하는 데 도움을 줄 수 있고, IT 엔지니어링을 위해 DHCP/DNS 활동에 대한 가시성을 제공하고 트래픽 밸런싱 및 구축 계획, CTI 지원 및 문제해결에 도움을 줄 수 있습니다
- 보안전문가에게는 DDI Guard가 컴플라이언스 준수 및 CTI 포렌식과 아카이브 모듈 또는 중앙 집중식 SIEM 솔루션을 통한 데이터 보존을 위해 DNS 및 DHCP 트랜잭션 데이터를 보존합니다. 또한 임의의 네트워크 장치 및 멀웨어 C2 액세스 시도에 대한 주요 정보를 제공합니다.
- 재무 전문가의 경우 DDI Guard는 데이터 필터링을 통해 SIEM DHCP/DNS 데이터 볼륨의 비용을 크게 절감할 수 있습니다.

About Cygna Labs

Cygna Labs is a software developer and one of the top three global DDI vendors. Many Fortune 100 customers rely on Cygna Labs' DDI products and services, in addition to its industry-leading security and compliance solutions to detect and proactively mitigate data security threats, affordably pass compliance audits, and increase the productivity of their IT departments. For more information, visit https://cygnalabs.com.