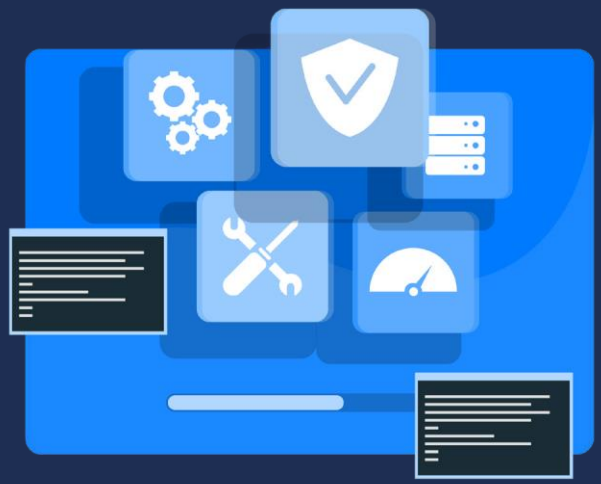
DATASHEET

VitalQIP DNS와 DHCP 보안과 리포팅 향상을 위한 CYGNA RADAR



You can't protect what you can't see

많은 네트워크 관리자들은 DHCP와 DNS 모니터링을 하지 않기 때문에 많은 사이버 범죄자들은 DHCP와 DNS protocol을 표적으로 삼습니다. DHCP와 DNS 서버는 적절한 네트워크 운영에서 중요하지만, 보안 측면에서는 오랫동안 안전하지 않은 것으로 간주되어 왔습니다. 이러한 공격으로부터 네트워크를 Cygna Rader와 함께 보호할 수 있습니다.

가시성 및 보고

최신 TCP/IP 네트워크에서 DNS는 시스템과 어플리케이션의 연결에서 name 제공의 중심적인 역할을 하는 기초적인 네트워크 서비스입니다. DNS 모니터링이 중요하지만 많은 네트워크 관리자들은 DNS가 탐색을 용이하게 하는 "Out of Band" 서비스를 제공하기 때문에 적극적으로 DNS를 모니터링하지 않습니다. 따라서 DNS는 인터넷에서 악의적인 행위자들이 선호하는 대상 중 하나입니다.

사용자를 악의적인 사기 웹 사이트로 리디렉션하기 위해 DNS 응답을 수정하는 것부터 DNS 서비스를 거부하려는 의도로 서버를 플러딩하는 것, DNS 응답을 통해 DOS를 대상에 반영하여 DNS 서버 및 소프트웨어를 해킹하는 것, DNS 프로토콜을 사용하여 민감한 데이터를 빼내고 명령 및 제어(C2) 센터와 통신하는 등 다양한 형태의 공격이 가능하게 됩니다. 이처럼 서비스가 손상될 시 대부분의 애플리케이션의 가용성에 영향을 미칠 수 있어 DNS 보호하는 것은 특히 중요한 편에 속합니다.

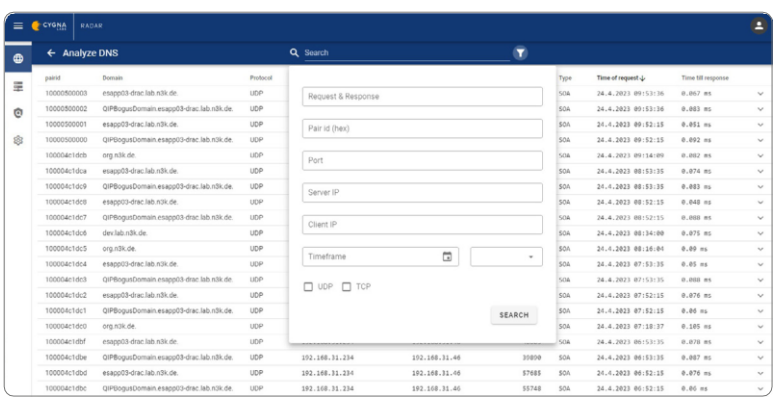
공격 탐지

이러한 공격 형태는 DNS가 공격 대상과 공격 수단으로서 매력적이고 관심의 대상이 된다는 것을 보여줍니다. 공격 형태가 다양한 만큼 마찬가지로 방어 및 보호 조치도 다양하지만 그 중 가장 중요한 것은 가시성입니다. DNS 및 DHCP 트래픽 모니터링은 비정상적인 활동을 감지할 수 있으며 포렌식 조사, 문제 해결 및 감사를 위해 특정 트랜잭션을 분석하는 데 필수적입니다.

DDI 솔루션은 DNS 및 DHCP의 운영을 단순화하지만 대다수의 경우 서비스 가용성을 항상 보장하기 위한 보안 조치는 포함되어 있지 않습니다. Cygna Radar는 이러한 갭을 줄이고 포괄적인 DNS 및 네트워크 보안 전략의 구성 요소로서 DNS 인프라에 대한 효율적이고 강력한 보호를 제공합니다.

진보된 위협으로부터 보호

Cygna Radar는 광범위한 DHCP 및 DNS 트랜잭션 감사정보를 제공할 뿐만 아니라 DNS 트래픽을 분석하여 DNS 터널링을 통한 데이터 유출 가능성을 탐지합니다. 공격자들은 내부 클라이언트들이 인터넷상의 이름을 확인해야 하는 것 때문에 DNS 트래픽이 방화벽을 자유롭게 통과한다는 사실을 악용해 왔습니다. Cygna Radar는 DNS 쿼리 및 응답을 검사하여 시그니처 기반으로 터널링 탐지하여 DNS 터널들을 자동으로 종료합니다. 또한 탐지되고 종료된 터널들은 볼 수 있고, 관리할 수 있어 허용된 트래픽에 사용되는 경우 탐지된 터널을 다시 열 수도 있습니다.



CYGNA LABS

특징

Cygna Radar는 데이터 유출 공격으로부터 네트워크를 보호하고 DHCP 및 DNS 트랜잭션에 대한 디테일한 가시성을 제공하기 위해 다음과 같은 주요 기능을 제공합니다.

QIP Appliance 통합

Cygna Radar는 VitalQIP Appliance Management Systems (AMS)에 로드하고 배포된 QIP 어플라이언스에 배포할 수 있는 표준 어플라이언스 패키지로 제공됩니다.

중앙 집중식 가시성

Radar 패키지는 VitalQIP DNS 및 DHCP 어플라이언스에 설치됩니다. 트랜잭션 데이터는 Cygna Radar 중앙 서버 소프트웨어를 통해 중앙에서 볼 수 있습니다. 하나 이상의 어플라이언스에 액세스하여 분석을 위해 DHCP 및 DNS 트랜잭션을 볼 수 있습니다. 또한 탐지된 DNS 터널을 보고 터널 정책 상태를 관리할 수도 있습니다.

자동화된 위협 완화

위협 행위자가 네트워크 무결성에 가하는 APT(지능형 지속 공격)와 DNS를 통해 데이터를 유출하려는 민감한 데이터를 신속하게 탐지하고 종료할 수 있습니다. 탐지된 DNS 터널은 Radar와 연관된 서버의 응답 정책 영역의 차단 목록에 추가되어 터널 패킷을 드롭합니다. 이러한 차단된 터널들은 Radar의 웹 그래픽 인터페이스를 통해 보여지고 관리됩니다.

직관적인 그래픽 인터페이스

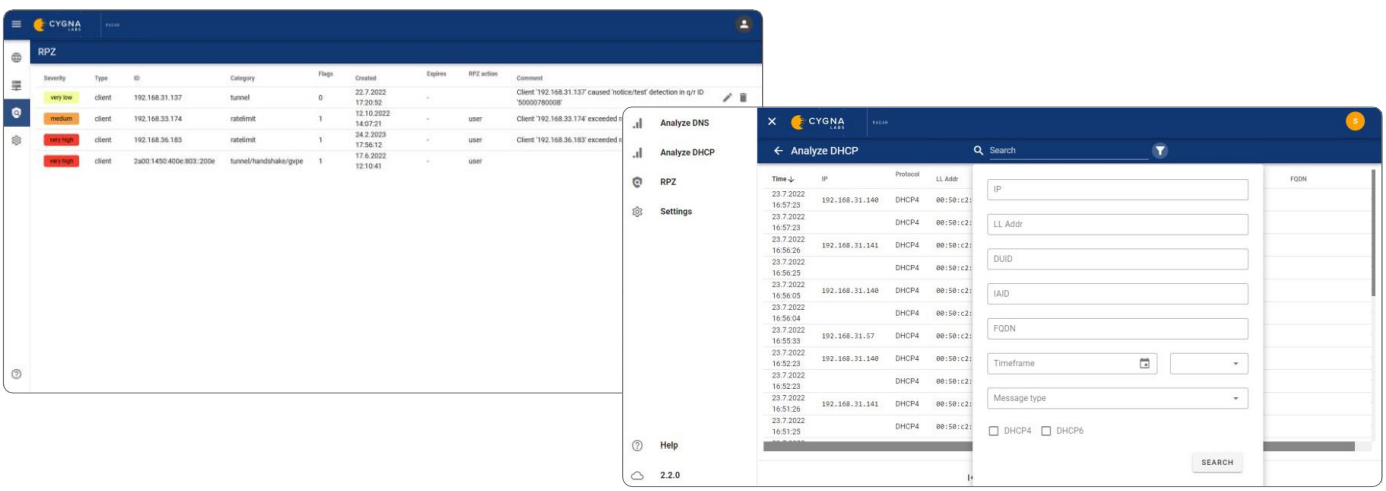
Cygna Radar는 중앙 Radar 서버를 통해 액세스할 수 있는 직관적인 그래픽 인터페이스를 제공합니다. 이 인터페이스는 DNS와 DHCP 트랜잭션을 보여줍니다. 이 정보는 공격 탐지 뿐 만 아니라 지속적으로 새로운 임대를 요청하는 결함이 있는 DHCP 클라이언트와 같은 잠재적인 이상 징후를 식별하는 데 중요합니다. DNS 터널을 보고 이러한 터널 상태를 관리할 수도 있습니다.

관리자 액세스 컨트롤

중앙 Cygna Radar 서버에 대한 다중 관리자 또는 사용자에 대한 액세스는 관리자에 대한 가시성 범위를 지정하여 권한 액세스를 최소화할 수 있습니다.

SIEM 로깅 및 필터링

Cygna Radar를 사용하면 DHCP 및 DNS 트랜잭션을 타사 SIEM 시스템에 기록할 수 있습니다. 기록된 트래픽을 필터링하여 SIEM 데이터 양과 관련된 비용을 절감할 수 있습니다. 또한 관리를 용이하게 하기 위해 각 DNS/DHCP 서버에 귀속될 수 있는 공통 프로파일을 정의할 수 있습니다.



Toll Free: **(844) 442-9462**
International: +1 (305) 501-2430
Fax: +1 (305) 501-2370

Sales: sales@cygnalabs.com
Support: support@cygnalabs.com
Billing: finance@cygnalabs.com

cygnalabs.com