NIST 사이버 보안 프레임워크와 DDI

By Timothy Rooney

Cygna Labs 소개

Cygna Labs 는 소프트웨어 개발업체이자 세계 3 대 DDI 공급업체 중 하나입니다. Fortune 100 대 기업에 선정된 많은 고객들이 Cygna Labs 의 DDI 제품 및 서비스를 사용하여 업계 최고의 보안 및 컴플라이언스 솔루션과 함께 데이터 보안 위협을 탐지 및 사전 예방하고, 저렴한 비용으로 컴플라이언스 감사를 통과하여, IT 부서의 생산성을 높이고 있습니다.

자세한 내용은 https://cygnalabs.com 에서 확인하실 수 있습니다.

NIST CSF 소개

사이버 보안은 지속적으로 IT 조직의 경영진부터 네트워크 엔지니어에 이르기까지 모든 레벨에서 관심사와 계획에 지배적인 영향을 끼치고 있습니다. 예를 들어 컴퓨터 또는 네트워크 사고는 외부 공격, 자연재해로 인하여 발생해도 조직의 평가, 운영, 고객, 그리고 재정에 광범위한 영향을 끼칠 수 있습니다.

IT 조직이 잠재적인 위협으로부터 네트워크를 보호하고 방어할 수 있도록 미국 NIST(National Institute of Standards and Technologies)는 조직이 자체 사이버 보안 계획을 평가하고 정립할 때 적용할 수 있는 사이버 보안 프레임워크를 발표했습니다. NIST 의 비전은 "중요한 측정 솔루션을 제작 및 공평한 표준을 촉진하는 세계 리더가 되는 것. 우리의 노력이 혁신을 촉진하고, 산업 경쟁력을 육성하며, 삶의 질을 향상시킵니다."입니다.

이 백서에서는 미국 정부뿐만 아니라 전 세계 단체들의 사실상 보안 구현 표준인 NIST Cybersecurity Framework[1]에 대해 간략하게 소개합니다. 또한 이 백서에서는 NIST 사이버 보안 프레임워크를 네트워크 내의 DNS/DHCP/IPAM(DDI) 구성 요소에 적용하는 예시에 대해 설명하며, 특히 DNS 에 중점을 두어 기업 내부와 인터넷 서버의 통신에 대해 다룹니다.

NIST 사이버 보안 프레임워크 개요

NIST CSF(Cybersecurity Framework)는 보안 요구 사항 및 구현 수준의 문서화 및 커뮤니케이션을 용이하게 하기 위해 공통 용어를 정의합니다. 이 프레임워크를 통해 조직은 위협을 식별하고 비즈니스 우선순위 및 사용 가능한 자원을 고려하여 위협 완화의 우선순위를 지정할 수 있게 해줍니다. NIST CSF 는 보안 목표, 성숙도 상태, 개선 계획 및 위협을 전달할 때 조직 내부 및 외부의 커뮤니케이션 촉진을 용이하게 합니다. 프레임워크는 세 가지 주요 구성 요소로 구성됩니다.

- 프레임워크 코어는 조직의 사이버 보안 위협 관리 사이클을 위한 보안 활동과 요구 결과를 정의합니다. 코어에는 일반적인 표준으로 분류가 가능하도록 기존 표준에 대한 자세한 참조가 포함되어 있습니다. 코어의 이러한 활동을 다섯 가지 기능으로 정의합니다.
    - Identify(식별) – 보호가 필요한 시스템, 자산, 데이터 및 기능을 다룹니다.
    - Protect(보호) – 보안 이벤트의 피해를 제한하는 보호 장치를 구현합니다.
    - Detect(감지) – 보안 사고를 식별합니다.
    - Respond(대응) – 보안 사고 영향을 포함한 보안 이벤트 관리를 다룹니다.
    - Recover(복구) – 복원과 복원 능력을 다룹니다.

  각 기능에는 정의된 분류와 하위분류가 있으며, 이에 대해서는 이 백서의 뒷부분에서 살펴보겠습니다.

- 프레임워크 프로파일(Profile)은 현재 보안 구현 수준과 목표 구현 수준 또는 계획된 구현 수준을 평가하고 전달하기 위한 메커니즘을 정의합니다. 프로파일은 비즈니스 제약 조건과 우선순위 그리고 프레임워크 핵심 기능에 대한 위협 허용 범위를 적용하여 구현 시나리오를 특화합니다.
- 프레임워크 구현 등급은 보안 구현의 완벽도 수준에 대하여 커뮤니케이션, 신속성, 사전, 사후, 비공식 대응을 기준으로 4 가지 등급을 정의합니다.
    - Tier 1 – 부분 대응형 – 조직 수준의 위협 인식이 제한적이고 외부 담당자들의 참여가 거의 없거나 존재하지 않는 비공식적, 임시적, 사후 대응적 위협 관리 정책.
    - Tier 2 – 위협 인식형 – 경영진 승인하에 위협 인식이 널리 확립되었지만 비공식적이고 조직의 일부만 위협관리 정책을 갖고 있으며, 외부 참여가 비공식적인 상태.

---

1) National Institute of Standards and Technology, Framework for Improving Critical Infrastructure Cybersecurity Version 1.1, April 16, 2018.

- Tier 3 – 반복 대응형 – 위협관리 정책이 공식적으로 승인되며 비즈니스 요구사항, 위협, 기술적 환경 변화에 따라 정립된 프로세스 및 정책이 정기적으로 업데이트되고, 직원 교육 및 이벤트에 대응하여 외부 파트너와 협력하는 상태
- Tier 4 – 적응형 – 변화하는 사이버 보안 환경에서 적시적으로 정책을 적용하고 사이버 보안 위협을 관리하기 위해 조직 전반이 접근하며 위협을 관리하고 파트너와 정보를 공유하는 상태.

구현 등급을 통해 조직은 선택한 완벽도 수준을 타겟 프로파일(Target Profile) 정의에 적용하여 위협 관리 정책을 특정 조직의 보안 정책, 위협 환경, 컴플라이언스 요구 사항, 비즈니스 목표 및 조직의 제약 조건에 맞출 수 있습니다.

프레임워크 구현

사이버 보안 프레임워크 구현에는 다음 세 가지 주요 조직 레벨 간의 상호 작용과 피드백을 포함합니다.

- **경영진** 레벨 – 조직 및 비즈니스 위협에 중점을 둔 경영진 레벨은 비즈니스/프로세스 레벨에 있는 사람들에게 비즈니스 우선 순위, 위협 허용 범위 및 보안 예산을 전달합니다.
- **비즈니스/프로세스** 레벨 – 비즈니스 우선 순위, 위협 허용 범위 및 예산을 고려하고, 중요한 인프라 위협을 관리하며 이러한 모든 것들과 현재 프로파일(Current Profile)을 기반으로 조직의 사이버 보안 프레임워크 타겟 프로파일(Target Profile)을 정의하고, 현재와 타겟 프로파일 간의 격차(gap)를 해소하기 위한 예산을 할당합니다. 이 레벨은 보안 위협 및 기술을 기반으로 현재 및 미래의 위협에 대한 변경 사항을 경영진 레벨로 피드백하고 구현/운영 레벨에 구현 지침을 제공합니다.
- **구현/운영** 레벨 – 프레임워크 프로파일 구현 및 위협 관리 전략을 담당합니다. 비즈니스/프로세스 레벨에 피드백에는 실행 진행 상황, 문제 및 자산, 취약성 및 위협의 변경 사항이 포함됩니다.

NIST CSF 문서는 위의 세 레벨 조직 구조를 활용하고, 사이버 보안 계획을 정의하는 데 있어 다음과 같은 기본 단계를 식별합니다.

1. 첫 번째 단계는 경영진 레벨에서 비즈니스 및 조직의 우선 순위 및 목표, 위협 허용 범위를 네트워크 내에 중점을 둘 자산 및 시스템의 집합 우선 순위에 따라 범위를 설정하는 것입니다.
2. 두 번째 단계는 설정한 범위 내에서 조직이 영향을 받는 시스템 및 자산, 컴플라이언스 및 법적 요구 사항, 위협 허용 범위, 범위가 지정된 시스템 및 자산과 관련된 위협 및 취약성을 포함합니다.
3. 이 단계는 사이버 보안 구현의 현재 상태를 정의하는 것으로 구성됩니다. 프레임워크 코어를 사용하면 각 기능 범주 및 하위 범주를 구현할 때 컴플라이언스 준수 및 규율 수준을 식별할 수 있습니다. 결과 분석은 사이버 보안 프레임워크에 대한 조직의 정렬에 대한 스냅샷을 정의하는 현재 프로필이 됩니다.
4. 그런 다음 위협 평가를 수행하여 자산 취약성, 잠재적 위협과 가능성, 각 위협의 잠재적 네트워크 및 비즈니스 영향 측면에서

위협을 파악해야 합니다.

5. 다섯 번째 단계는 타겟 프로파일을 정의하여 원하는 사이버 보안 활동 및 결과를 정의하는 것입니다. 프레임워크 코어를 비즈니스별 범주 및 하위 범주와 함께 사용하면 원하는 결과를 정의할 수 있습니다.
6. 타겟 프로파일과 현재 프로파일을 비교하면 현재 상태에서 원하는 상태로 가기 위해 해결해야 하는 목표를 정의할 수 있습니다. 해당 보안 우선 순위에 비추어 각 범주 및 하위 범주에 대한 격차를 해소하는데 드는 비용에 따라, 비즈니스에 대한 해당 가치를 기반으로 해당 격차 해소에 투자할지 여부를 결정할 수 있습니다. 이를 통해 초기에 해결할 격차와 나중에 해결할 격차, 자본, 비용 및 리소스 관점에서 각각에 대한 비용의 우선 순위를 정할 수 있습니다.
7. 마지막 단계는 우선순위가 지정된 격차를 해결하기 위한 실행 계획을 공식적으로 정의하고 구현하는 것으로 구성됩니다. 구현/운영 레벨 내에서 구현이 진행됨에 따라 현재 프로파일을 업데이트하여 현재 또는 진행 중인 상태의 스냅샷을 전달할 수 있습니다.

현재 프로파일 및 타겟 프로파일은 각각 현재 및 계획된 사이버 보안 구현 상태의 조직 내부 또는 외부에서 소통을 가능하게 합니다. 이 공통 프레임워크를 광범위하게 사용하고 잘 정의된 용어들을 사용하면 담당자들과 이해 관계자 간의 의사 소통을 용이하게 할 수 있습니다.

DNS 범위 지정(Scoping DNS)

거의 모든 IP 연결을 시작할 때 DNS 를 사용하는 경우, 범위 지정에 DNS 를 포함하는 것이 좋습니다. 경영진 레벨에서 DNS 를 우선순위로 식별하고 보안 제어를 적용하는 것으로 결정하면, 비즈니스 레벨은 우선 순위 내에서 영향을 받는 DNS 구성 요소를 정의해야 합니다. 예를 들어, 표 1 에 표시된 대로 인터넷 사용자가 웹 사이트를 찾을 수 있도록 네임서비스를 확인하거나, 동료의 내부 네임서비스를 확인하거나, 연결이나 내부 사용자를 위한 인터넷 네임서비스를 확인할 때 기본 DNS 기능과 관련된 다음 세 가지 광범위한 DNS 범위를 고려할 수 있습니다.

현재 프로파일(Current Profile)

조직에서 이러한 광범위한 영역 중 하나 또는 모두를 포함하는 것으로 범위를 정의한 후에는 연결된 DNS 구성 요소의 현재 보안 수준과 관련하여 현재 프로파일을 개발해야 합니다. 현재 DNS 관리, 보안 정책 및 절차에 적용되는 CSF 코어의 각 범주와 하위 범주를 고려해야 합니다. CSF 자체와 마찬가지로, 구현에서 고려해야 할 추가 프로세스나 원하는 결과물이 존재할 수 있습니다.

표 1: DNS 범위 예

광범위한 DNS 범위	영향을 받는 DNS 구성 요소
인터넷에 게시된 조직의 네임서비스를 정확하게 확인	● 네임서비스를 정확하고 안전하게 확인하도록 권한 있는 DNS 서버 또는 외부 DNS 호스팅 공급자를 구성해야 합니다.
내부 사용자에 대한 조직의 네임서비스를 정확하게 확인	● Stub 리졸버는 내부 DNS 서버 IP 주소로 구성해야 합니다. ● 내부 재귀 DNS 서버는 내부 리졸버의 쿼리를 확인하도록 구성해야 합니다. ● 내부 리졸버에 대한 내부 네임서비스를 확인하도록 권한 있는 DNS 서버를 구성해야 합니다.
올바른 내부 사용자의 인터넷 액세스를 위해 인터넷 도메인을 정확하게 확인	● Stub 리졸버는 내부 DNS 서버 IP 주소로 구성해야 합니다. ● 재귀 DNS 서버는 내부 리졸버에서 인터넷 기반 DNS 서버로 DNS 쿼리를 확인하도록 구성해야 합니다.

위험성 평가(Risk Assessment)

프로세스의 다음 주요 단계는 영향을 받는 DNS 구성 요소에 대한 위험 평가로 구성됩니다. 이 단계에는 일어날 수 있는 각 위협 이벤트들이 포함됩니다. 위협 이벤트는 발생 시 네트워크와 비즈니스에 해로운 영향을 미칠 수 있는 이벤트입니다. 위협 이벤트에는 자연 재해 또는 인재와 같은 보안 관련 위협 이외의 이벤트가 포함될 수 있으므로 특히 네트워크 및 DNS 를 보호하기 위해 가능한 모든 위협을 고려하는 것이 좋습니다.

식별된 각 위험에 대해 위협 이벤트가 발생할 가능성과 위협 이벤트가 발생할 경우 네트워크 및 비즈니스에 미치는 영향을 고려합니다. 특정 위협 이벤트가 발생할 가능성은 해당 위협 이벤트의 알려진 취약점을 고려하여 추정할 수 있습니다. x 축은 위협의 상대적 영향을 나타내고, y 축은 해당 위협의 상대적 가능성을 나타냅니다. 상대적인 영향은 자원 부족 또는 다운타임, 최종 사용자 또는 고객 불만, 수익 손실 같은 용어로 추정할 수 있습니다. 이러한 방식으로 위험을 표시하면 보다 긴급한 수정이 필요한 위험을 우선 순위로 설정하는 데 도움이 될 수 있습니다.

그림 1 에서 알 수 있듯이 Risk#4(R4)는 상대적으로 높은 가능성과 영향을 가집니다. 이러한 위험은 가장 높은 우선 순위로 설정되어야 합니다. 조금 더 낮은 영향과 낮은 가능성을 가진 Risk#2 가 다음이어야 합니다. Risk#1 이 Risk#2 보다 가능성이 높지만, 영향은 훨씬 적습니다. 제어를 적용함으로써 목표는 완화되지 않은 각 위험을 원점으로 방사형으로 이동하여 조직에 대한 전반적인 잔여 위험을 낮추는 것입니다.

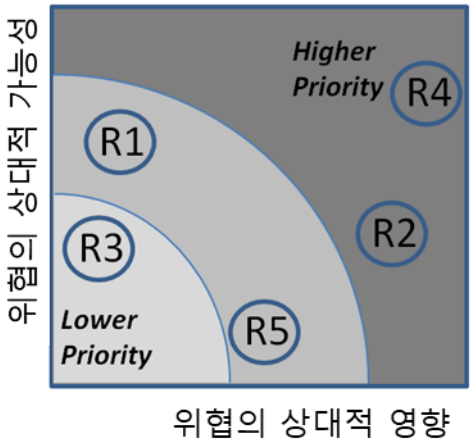

그림 1: 위협의 가능성과 영향

시스템 수준별로 위협을 평가하는 프로세스에 엄격성과 구조를 추가하기 위해 NIST 는 FIPS(Federal Information Processing Standards, 연방 정보 처리 표준) 출판물 199[2]를 발표했습니다. 이 문서에서는 조직에 대한 위협 평가에 사용하기 위해, 특정 위협 이벤트가 발생할 때 조직에 미칠 수 있는 잠재적 영향을 기반으로 정보와 정보 시스템을 분류하기 위한 표준을 정의합니다. 분류는 정보와 정보 시스템에 대한 세 가지 보안 목표에 따라 수행됩니다.

- **기밀성(Confidentiality)** – 무단 공개로부터 정보 보호
- **무결성(Integrity)** – 정보의 무단 수정 또는 파기
- **가용성(Availability)** – 정보 또는 시스템에 대한 액세스 또는 사용의 중단

FIPS 출판물 199 는 이러한 각 목표에 대해 조직에 미치는 영향의 세 가지 수준을 다음과 같이 정의합니다.

- **낮은(Low) 영향** – 조직의 운영, 자산 또는 개인에 제한적인 영향을 미칠 것으로 예상됩니다. 예를 들어, 기밀성, 무결성 또는 가용성 손실로 인해 조직의 능력이 현저히 감소할 수 있습니다. 또한 조직 자산에 심각한 피해, 금전 손실 또는 개인에게 중요하지만 생명에 직접적으로 위협되지 않는 중요한 피해가 발생할 수 있습니다.
- **중간 정도(Moderate) 영향** – 조직의 운영, 자산 또는 개인에게 심각한 악영향을 미칠 것으로 예상됩니다. 예를 들어, 기밀성, 무결성 또는 가용성 손실로 인해 조직의 능력이 상당히 감소할 수 있지만 효과는 상당히 감소합니다. 또한 조직의 자산에 심각한 손상, 상당한 금전적 손실 또는 개인에게 중요하지만 생명에 직접적으로 위협되지 않는 피해가 발생할 수 있습니다.
- **높은(High) 영향** – 조직의 운영, 자산 또는 개인에게 심각하거나 치명적인 영향을 미칠 것으로 예상되며, 기밀성, 무결성 또는 가용성 손실로 인해 조직의 능력이 크게 감소할 수 있고, 주요 기능 중 하나 이상을 수행할 수 없게 될 수 있습니다. 또한 조직의 자산에 큰 피해를 입히거나, 막대한 재정적 손실을 일으키고, 개인에게는 심각하거나 치명적인 피해가 발생할 수 있습니다.

---

2) *Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, Standards for Security Categorization of Federal Information and Information Systems, February 2004.*

낮음, 보통 또는 높음으로 세 가지 목표 각각을 분류하는 것은 네트워크 및 정보 시스템 자체(예: 서버, 노트북 등)를 통해 저장 중(예: 서버의 파일 내) 또는 이동 중(예: 네트워크를 통과하는 IP 패킷 내)에 있는 다양한 유형의 정보에 대해 수행됩니다. 정보 유형의 예로는 게시된 DNS 영역 정보 및 DNS 쿼리 응답 트랜잭션 정보가 있습니다. 조직 내의 형식 및 시스템에 대한 보안분류 SC(Security Categorization)는 다음과 같이 공식으로 표시됩니다.

$$\textbf{SC}_{\text{정보 유형/시스템}} = \{(\textbf{기밀성}, \text{LOW}), (\textbf{무결성}, \text{HIGH}), (\textbf{가용성}, \text{MODERATE})\}$$

일반적으로 대부분의 조직에서 DNS 에 대한 최우선 요구 사항은 무결성으로, DNS 데이터가 무단으로 변경되지 않도록 보호합니다. 사용자의 목적지 연결은 DNS 데이터에 의존합니다. 고가용성도 마찬가지로 중요하므로 프로세스와 데이터를 마음대로 사용할 수 있습니다. DNS 데이터는 일반적으로 공개 정보이기 때문에 기밀성은 상대적으로 우선 순위가 낮지만 많은 조직에서는 모든 또는 특정 내부 사용자에 대해서만 DNS 정보를 게시하고 외부 사용자의 액세스는 금지합니다. 이 경우 기밀성은 높지는 않더라도 보통으로 간주될 수 있습니다.

타겟 프로파일(Target Profile) 및 보안 계획

위협 평가는 보안 조치 계획을 수립할 때와 계획의 우선 순위를 정할 때 귀중한 정보를 제공합니다. 웹 사이트에 대상 DNS 관련 CSF 코어를 게시했으며, 이를 시작점으로 사용하거나 직접 만들 수 있습니다. CSF 코어를 사용하여 타겟 프로파일을 생성하면 추가할 수 있는 카테고리와 함께 정의된 각 카테고리에 대해 원하는 결과를 정의할 수 있습니다. 타겟 프로파일과 현재 프로파일의 차이는 현재 보안 구현 상태에서 원하는 대상 상태로 전환하는 데 필요한 구현 및 프로세스 개선을 포함하여 작업 계획에 대한 작업 목록을 정의합니다.

주어진 위험을 줄이거나 가능성 또는 영향을 최소화하기 위해 하나의 제어 또는 복합 제어가 구현될 수 있습니다. 위험 평가 결과를 통해 더 높은 영향과 더 높은 가능성의 위협 이벤트를 완화하기 위해 제어의 우선 순위를 지정할 수 있습니다. 제어는 이러한 위험을 줄이기 위한 기술, 프로세스 또는 인력 자원의 구성입니다. 일반적으로 잔여 위험이 남아 있으면, 추가 통제를 적용해야 할 수 있습니다.

일반적으로 여러 제어를 적용하면 지정된 위협 이벤트에 대해 여러 방어선을 제공하는 심층 방어 보안 접근 방식이 생성됩니다. 공격자가 하나의 제어를 뚫으면 공격의 추가 진행을 막기 위해 다른 컨트롤이 제공됩니다. 주어진 호스트(예: DNS 서버)를 고려할 때 심층 방어 접근 방식에는 다음 계층을 보호하는 작업이 수반됩니다.

표 2: 심층 방어 계층

방어 계층	일반 속성	DNS 서버 속성(예)
미사용 데이터	호스트에 상주하는 데이터(예 : 하드 드라이브, 휴대용 메모리 혹은 데이터베이스)	구성 파일, 영역 파일 또는 데이터베이스, 리소스 레코드, 보류 중인 DNS 업데이트 및 캐시된 데이터
전송 데이터	호스트에서 보내거나 받은 데이터	DNS 쿼리 및 응답, DNS 업데이트, Zone 전송, IPAM 시스템을 통한 구성 업데이트, SSH 또는 기타 수단
어플리케이션	호스트에서 실행 중인 각 응용 프로그램의 평가	ISC BIND, Microsoft Windows, Unbound, NSD, PowerDNS, Knot DNS 등(예: 적용된 DNS 서버 응용 프로그램)
하드웨어 및 운영체제	하드웨어 제조사, 소프트웨어 제조사(예: BIOS), 커널 및 운영체제 강화 전술의 전략	DNS 서버 하드웨어, 커널 및 운영체제
내부 네트워크	내부 방화벽, 호스트 방화벽, 내부 인프라 내 악성코드 존재	DNS, DNS ACL, Port ACL, 악성코드 C&C 쿼리를 탐지하기 위한 DNS 방화벽에 허용되는 포트 및 프로토콜
네트워크 경계	신뢰할 수 있는 환경과 신뢰할 수 없는 환경 간의 경계	DNS 트래픽 통과, DNS 터널링 감지를 위한 허용 가능한 포트 및 프로토콜
외부 네트워크	인터넷 기반 취약점	인바운드 DNS 트래픽, 외부 DNS 제공자, 도메인 등록 기관(들), DNS 터널링 탐지
물리적 보안	건물 / 데이터 센터 / 컴퓨터 접근, 출입 통제, 자산 제거 정책	DNS 서버 물리적 보안
운영	사람, 프로세스, 기술에 의한 보안 정책 준수, 정책 검증 및 시행	DNS 구성 및 트랜잭션 감사, 최소 권한 관리자 액세스 교육, 전체적인 보안 인식

이 심층 방어 전략의 여러 측면은 네트워크의 여러 요소에서 공통적으로 적용됩니다(예: 모든 서버에는 강력한 자격 증명이 필요하고 모든 원격 관리자 액세스는 암호화되어야 함). 이러한 일반적인 제어는 일관된 보호를 제공하며 DNS 서버에도 적용되어야 합니다.

위에서 설명한 예제 특성과 같은 DNS 관련 제어는 추가 보호 기능을 제공합니다. NIST CSF 코어는 심층 방어 전략을 암시적으로 권장합니다. NIST 는 안전한 DNS 배포를 위한 DNS 관련 가이드를 게시했습니다.[3] 이 유용한 가이드에서는 DNS 데이터의 무결성을 보호하는데 중점을 두며, BIND DNS 서버의 보안을 확립하기 위한 프로시저와 DNS Security Extensions(DNSSEC)의 구성 및 관리에 대한 철저한 절차를 제공합니다.

보안 조치 계획은 특정 위협 이벤트를 줄이도록 설계된 제어 구현을 정의해야 합니다. 계획된 각 구현에는 인력 참여와 자본 또는 비용과 관련된 조직 리소스가 필요하기 때문에 일반적으로 리소스가 허용하는 한, 시간이 지남에 따라 단계적으로 계획의 우선 순위를 지정하고 구현해야 합니다. NIST CSF 의 적용은 보안 상태 및 목표를 효율적으로 전달하기 위한 구조와 공통 언어를 제공합니다. 또한 보안 격차의 우선 순위를 지정하여 DNS 및 네트워크 보안 제어를 구현할 수 있습니다.

DDI 용 NIST CSF 코어 적용

5 가지 핵심 기능에 걸쳐 범주의 각 하위 범주에 대해 제안된 결과를 제공하는 웹 사이트에서 DNS 용 NIST CSF 코어 예제를 다시 한번 다운로드하도록 초대합니다. 이 섹션에서는 CSF 코어 및 잠재적인 DNS 결과에 대한 소개를 제공하기 위해 범주 수준을 강조 표시합니다.

식별 기능 (ID)

식별 기능은 보호가 필요한 시스템, 자산, 기능, 데이터 및 기능을 다루며 다음 범주를 포함합니다. 또한 각 DNS 의 주요 결과를 요약해 봤습니다

자산 관리 범주(ID.AM)

이 범주에서는 조직이 비즈니스 목적을 달성할 수 있도록 하는 데이터, 인력, 장치, 시스템 및 시설을 조직의 목표 및 조직의 위협 전략에 대한 상대적 중요도에 따라 식별하고 관리해야 합니다. 주요 DDI 결과는 다음과 같습니다.

- 패치 수준, 도메인 이름, IP 주소, 물리적 위치, 서버 역할(예: 재귀적, 권한 등), 관리자 연락처 및 기타 자산 추적 정보를 포함하여 서버 하드웨어, 운영 체제 및 버전, DNS 및 DHCP 애플리케이션 소프트웨어 및 버전을 포함한 관리 DHCP 및 DNS 서버를 문서화합니다.
- 사용 가능하고 할당된 주소 공간 측면에서 사설IP 공간(RFC 1918), 유니캐스트 로컬 및 공인 IP 공간을 포함한 IPv4 및 IPv6 주소 공간을 문서화하고 관리합니다.

---

3) Ramaswamy Chandramouli, Scott Rose, *Secure Domain Name System (DNS) Deployment Guide*, NIST Special Publication 800-81-2, National Institute of Standards and Technology, September, 2013.

- 서버 구성에 필요한 데이터 흐름(예: 관리자 시스템의 서버 경로)을 문서화합니다. 또한 서버 애플리케이션에 대한 데이터 흐름(예: DHCP 및 DNS 트래픽 경로)을 문서화합니다.
- 서비스 지원 및 기술 연락처, 관리 URL 등을 포함하여 IP 주소 공간(인터넷 레지스트리 또는 인터넷 서비스 공급자) 및 DNS(도메인 등록 기관, 외부 DNS 호스팅 공급자)와 관련된 외부 정보 시스템을 문서화합니다.
- 비즈니스 가치 중요도와 관련하여 이러한 자산의 우선순위를 지정합니다.
- 전체 인력 및 제3자 이해관계자(예: 공급업체, 고객, 파트너)에 대한 사이버 보안 역할과 책임이 설정됩니다.

비즈니스 환경 범주(ID.BE)

조직의 사명, 목표, 이해관계자 및 활동을 이해하고 우선순위를 지정하여 사이버 보안 역할, 책임 및 위협 관리 결정을 알립니다. 이 범주에 대해 원하는 DDI 활동은 다음과 같습니다.

- DDI 서버 및 타사(IP 및 DNS) 서비스는 보안 기능, 다양한 공급업체의 비사용자 지정 구성을 포함하는 검증된 공급업체를 고려하여 문서화합니다.
- 서버 및 외부 공급자 서비스의 오류에 대한 중요도 및 비상 계획을 포함하여 조직의 목표와 임무에 미치는 영향 측면에서 DDI 서버를 분류하고 우선 순위를 지정합니다.
- 중요한 DDI 서비스를 제공하기 위한 종속성 및 중요한 기능이 설정됩니다.
- 중요한 DDI 서비스 제공을 지원하기 위한 복구 요구 사항은 모든 운영 상태(예: 위협/공격 중, 복구 중, 정상 작동)에 대해 설정됩니다.

거버넌스 관리 범주 (ID.GV)

이 카테고리는 조직의 규제, 법률, 위험, 환경 및 운영 요구 사항을 관리하고 모니터링하기 위한 정책, 절차 및 프로세스를 이해하고 사이버 보안 위협 관리를 알리도록 규정합니다. 주요 DDI 영향에는 다음 사항을 고려하여 DDI 를 포함하는 것이 수반됩니다.

- 조직의 사이버 보안 정책을 수립하고 소통합니다.
- 사이버 보안 역할과 책임은 내부 역할 및 외부 파트너와 연계되어 조정됩니다.
- 개인 정보 보호 및 시민 자유 의무를 포함한 사이버 보안에 관한 법적 및 규제적 요구 사항을 이해하고 관리합니다.
- 거버넌스 및 위협 관리 프로세스는 사이버 보안 위협을 해결합니다.

리스크 평가 범주 (ID.RA)

이 카테고리는 이 문서의 앞부분에서 논의한 위험 평가와 관련이 있으며, 여기서 위험을 식별하고 상대적 영향과 가능성을 매핑하는 방법에 대해 논의했습니다. 목표는 조직이 운영(임무, 기능, 이미지 또는 평판 포함), 조직 자산 및 개인에 대한 사이버 보안 위협을 이해할 수 있도록 하는 것입니다. 원하는 결과는 다음과 같습니다.

- DDI 자산 취약성이 식별되고 문서화됩니다.
- 사이버 위험 인텔리전스는 CERT(Computer Emergency Response Team) 및 DDI 공급업체와 같은 정보 공유 포럼 및 출처에서 수신됩니다.
- 내부 및 외부 위험이 식별되고 문서화됩니다.
- 잠재적인 비즈니스 영향 및 가능성 또는 각 위험 및 취약성이 식별됩니다.
- 실현된 위험 및 취약성에 대한 위험 대응이 식별되고 우선순위가 지정됩니다.

리스크 관리 범주 (ID.RM)

운영 위험의 결정은 조직의 우선순위, 제약 조건, 위협 허용 범위 및 가정에 의해 결정됩니다. DDI 활동은 다음과 같이 정의됩니다.

- 위험 관리 프로세스에 대한 DDI 영향의 포함은 조직 이해관계자가 설정, 관리 및 동의합니다.
- 조직의 위험 허용 범위는 결정되고 명확하게 표현되며 중요한 인프라 및 부문별 위험 분석에서의 역할에 따라 결정됩니다.

공급망 리스크 관리 범주 (ID.SC)

공급망 위험 관리와 관련된 위험 의사결정을 지원하기 위해 조직의 우선순위, 제약조건, 위협 허용오차 및 가정을 설정하고 이를 활용합니다. 조직은 공급망 위험을 식별, 평가 및 관리하기 위한 프로세스를 설정하고 실행하고 있습니다. DDI 를 반영한 주요 결과는 다음과 같습니다.

- DDI 공급망 위험 관리 프로세스는 조직 이해관계자가 식별, 설정, 평가, 관리 및 동의합니다.
- DDI 공급업체 및 제3자 DDI 파트너는 사이버 공급망 위험 평가 프로세스를 사용하여 식별, 우선순위 지정 및 평가됩니다.
- DDI 공급업체 및 타사 DDI 파트너와의 계약은 조직의 사이버 보안 프로그램 및 사이버 공급망 위험 관리 계획의 목적을 달성하기 위해 설계된 적절한 조치를 이행하는 데 사용됩니다.

- DDI 공급업체 및 제3자 DDI 파트너는 감사, 테스트 결과 또는 다른 형태의 평가를 통해 정기적으로 평가되어 계약상의 의무를 이행하고 있는지 확인합니다.
- 대응 및 복구 계획과 테스트는 DDI 공급업체 및 타사 DDI 서비스 제공 업체와 함께 수행됩니다.

보호 기능 (PR)

보호 기능은 보안 이벤트의 영향을 제한하는 세이프가드를 구현하려고 합니다.

ID 관리, 인증 및 액세스 제어 범주 (PR.AC)

물리적 및 논리적 자산 및 관련 시설에 대한 액세스는 승인된 사용자, 프로세스 및 장치로 제한되며, 승인된 활동 및 트랜잭션에 대한 무단 액세스의 평가된 위험과 일관되게 관리됩니다. 관련 DDI 영향 및 결과는 아래에 강조 표시되어 있습니다.

- DDI 시스템 ID 및 자격 증명은 권한 있는 디바이스, 사용자 및 프로세스에 대해 발급, 관리, 확인, 해지 및 감사됩니다.
- DDI 자산에 대한 물리적 액세스가 관리 및 보호됩니다.
- DDI 시스템 및 자산에 대한 원격 액세스가 관리됩니다.
- 네트워크 무결성은 재귀, 내부 권한 및 외부 권한 부여를 위한 전용 DNS 서버를 수반하는 역할 기반 DNS 배포를 포함하여 DDI 구성 요소에 대해 보호됩니다(예: 네트워크 분리 및 세분화).
- DDI 시스템 ID는 자격 증명에 바인딩 되어, 적절한 상호 작용에서 증명됩니다.
- 사용자, 장치 및 기타 자산은 트랜잭션의 위협(예: 개인의 보안 및 개인 정보 보호 위협 및 기타 조직 위협)에 비례하여 인증됩니다(예: 단일 요소, 다중 요소).

인식 및 교육 범주 (PR.AT)

조직의 직원과 파트너는 사이버 보안 인식 교육을 받고 관련 정책, 절차 및 계약에 따라 사이버 보안 관련 의무와 책임을 수행하도록 교육을 받습니다. 보안 교육은 DDI 시스템을 사용하고 운영하는 사람을 포함하여 조직 전체에서 매우 중요합니다.

- 모든 사용자는 정보를 얻고 교육을 받았으며 권한 있는 사용자는 자신의 역할과 책임을 이해합니다.
- 고위 경영진부터 물리적 및 정보 보안 담당자, 제3자 이해관계자(예: ISP, DNS 호스팅 공급업체, 고객, 파트너)에 이르기까지 자신의 역할과 책임을 이해합니다.

데이터 보안 범주 (PR.DS)

정보와 기록은 조직의 위협 전략에 따라 관리되어 정보의 기밀성, 무결성 및 가용성을 보호합니다.

- DDI 데이터가 안전하게 보호됩니다. DDI 데이터를 안전하게 보호하기 위해 다음과 같은 조치가 취해질 수 있습니다:
  - DDI 구성 요소 하드웨어 보호, 운영 체제, 커널 및 소프트웨어 강화
  - ACL은 관리 액세스를 제어하기 위해 정의되며 관리 트랜잭션은 암호화됩니다.
  - DNS ACL 및 트랜잭션 키는 신뢰할 수 있는 DNS 데이터를 업데이트 및 영역 전송으로부터 보호하기 위해 구현됩니다.
  - DNSSEC을 사용하여 DNS 영역 데이터에 서명합니다. DNSSEC 개인 키 보호 및 긴급 롤오버를 포함한 롤오버 프로세스를 문서화합니다.
  - DDI 설정 및 로킹 데이터의 정기적인 백업 및 오프라인 저장을 수행합니다.
  - 서버, 운영 체제 및 DDI 공급업체의 취약성 소스를 모니터링하고 미사용 데이터에 영향을 미치는 공급업체 패치를 배포합니다.
  - DDI 구성 요소 액세스 로그 및 수행된 기능을 주기적으로 감사하여 역할 및 책임과의 일치를 확인합니다.
- 전송 DDI 데이터가 보호됩니다.
  - DDI 관리자 및 시스템 간 통신이 인증되고 암호화됩니다.
  - DNS 확인 데이터는 전송 중 데이터 조작을 감지하기 위해 DNSSEC를 사용하여 서명 및 인증됩니다. DNSSEC 구현이 없는 경우 아웃바운드 쿼리에 대한 DNS 원본 포트, 트랜잭션 ID 및 쿼리 대/소문자를 랜덤으로 지정합니다.
  - DNS 업데이트, 알림 및 전송 데이터가 서명되거나 암호화됩니다.
  - DNS ACL은 쿼리, 캐시 액세스 및 영역 전송에 대한 자격을 제어하도록 구성되며, 리졸버에서 재귀적 DNS 서버 통신은 쿠키 또는 암호화(DoT/DoH)를 통해 보호됩니다.
  - DNS 터널링이 모니터링 됩니다.
  - DNS 방화벽 실행 및 멀웨어 C&C 쿼리가 모니터링 됩니다.
  - 취약성 소스를 모니터링하고 전송 데이터에 영향을 미치는 DDI, 운영 체제 및 커널 공급업체 패치를 배포합니다. 하드웨어, 소프트웨어, 패치 및 파일 무결성을 검증합니다.
  - 인바운드 및 아웃바운드 속도 제한, 쿼리 제한 및 DNS 애니캐스트와 같은 DoS/DDoS 제어를 수행합니다.
  - DDI 구성요소 액세스 로그와 역할 및 책임에 맞게 수행되는 기능을 주기적으로 감사합니다.
- DDI 자산은 폐기, 이전 및 처분 과정을 통해 공식적으로 관리됩니다.
- 가용성을 유지하기 위해 충분한 DDI 용량을 보장합니다.

정보 보호 프로세스 및 절차 범주 (PR.IP)

보안 정책(목적, 범위, 역할, 책임, 관리 약속 및 조직 간의 조정을 처리함)은 프로세스 및 절차가 유지 관리되고 정보 시스템 및 자산의 보호를 관리하는 데 사용됩니다.

- 보안 원칙(예: 최소 기능성 개념)을 통합한 DDI 시스템의 기준 구성을 작성하고 유지합니다. 정보의 백업은 수행되고 유지되며 테스트됩니다.
- DDI 시스템을 관리하기 위해 시스템 개발 수명 주기가 구현됩니다.
- 구성 변경 제어 프로세스에 DDI가 통합됩니다.
- 조직 자산의 물리적 운영 환경에 관한 정책 및 규정이 충족됩니다.
- 데이터는 정책에 따라 파기됩니다.
- 보호 과정이 지속적으로 개선됩니다.
- 보호 기술의 효율성이 공유됩니다.
- 대응 계획(Incident Response and Business Continuity)과 복구 계획(Incident Recovery and Disaster Recovery)은 DDI 시스템을 통합하고 있습니다.
- 중요한 DDI 시스템을 포함하여 대응 및 복구 계획을 테스트합니다.
- 사이버 보안은 인적 자원 관행(예: 프로비저닝 해제, 직원 심사)에 포함됩니다.
- 배포된 DDI 시스템 및 소프트웨어를 포함하여 취약점 관리 계획이 개발되고 실행됩니다.

유지 관리 범주 (PR.MA)

DDI 구성 요소를 포함한 산업 제어 및 정보 시스템 구성 요소의 유지 보수 및 수리는 정책 및 절차에 따라 수행됩니다. 조직 자산의 로컬 및 원격 유지 관리는 승인, 기록 및 무단 액세스를 방지하는 방식으로 수행됩니다.

보호 기술 범주 (PR.PT)

기술 보안 솔루션은 관련 정책, 절차 및 계약에 따라 시스템 및 자산의 보안과 복원을 보장하기 위해 관리됩니다. 이 범주는 DDI 시스템에도 적용되며 다음과 같은 전술을 다룹니다.

- 감사/로그 기록은 정책에 따라 결정, 문서화, 구현 및 검토됩니다.
- 이동식 미디어는 보호되며 정책에 따라 사용이 제한됩니다.
- 최소 기능의 원칙은 필수 기능만 제공하도록 시스템을 구성함으로써 통합됩니다.
- 소통과 및 제어 네트워크가 보호됩니다.
- 메커니즘(예: 안전 장치, 부하 분산, 핫 스왑)은 정상 및 불리한 상황에서 복원 요구 사항을 달성하기 위해 구현됩니다.

탐지 기능 (DE)

탐지기 기능은 보안 사고의 식별에 중점을 둡니다.

이상 현상 및 이벤트 범주 (DE.AE)

이 범주에서는 비정상적인 활동이 감지되고 이벤트의 잠재적 영향을 이해해야 합니다. 물론 이는 사고의 모드와 범위를 이해하여 적절하게 해결하는 데 중요합니다. DDI 구성 요소에 대한 공격은 이 범주에 속하지만 DDI 이벤트 관련 정보를 포함하는 것도 검색된 이벤트의 전체 범위를 이해하는 데 중요합니다.

- 사용자 및 시스템에 대한 네트워크 운영 및 예상 데이터 흐름의 기준을 설정하고 관리합니다.
- 탐지된 이벤트를 분석하여 특히 DNS 사용을 포함한 공격 대상 및 방법을 파악합니다.
- 이벤트 데이터는 DDI 시스템을 포함한 여러 소스 및 센서에서 수집되고 상호 연관됩니다.
- 이벤트의 영향이 결정됩니다.
- 사고 경고 임계값은 조직의 위협 수준에 따라 설정됩니다.

보안 연속 모니터링 범주(DE.CM)

모니터링 및 감시는 보안 이벤트를 감지하는 데 필수적입니다. 정보 시스템 및 자산을 모니터링하여 사이버 보안 이벤트를 식별하고 보호 조치의 효과를 검증합니다. DDI 구성 요소, 특히 DNS 서버 및 트래픽은 이벤트를 직접 대상으로 지정하거나 보안 사고에 대한 액세서리로 모니터링해야 합니다.

- 잠재적인 사이버 보안 이벤트를 감지하기 위해 물리적 환경을 모니터링합니다.
- 잠재적인 사이버 보안 이벤트를 감지하기 위해 직원 활동을 모니터링합니다.
- 악성코드는 타겟에서 직접 실행되며 명령 및 제어 센터(예: DNS를 통해)와의 악성코드 통신을 통해 탐지됩니다.
- 승인되지 않은 모바일 코드가 감지됩니다.
- 잠재적인 사이버 보안 이벤트를 감지하기 위해 외부 서비스 제공 업체 활동을 모니터링합니다. 예를 들어 게시된 외부 DNS NS와 글루 레코드를 모니터링하면 DNS 하이재킹(Hijacking) 탐지에 도움이 될 수 있습니다.
- 무단 사용자, 연결, 장치 및 소프트웨어의 모니터링이 수행됩니다.
- 취약점 스캔이 수행됩니다.

탐지 프로세스 범주 (DE.DP)

이상 이벤트를 인식하기 위해 탐지 과정 및 절차를 유지하고 테스트합니다. 증상 테스트를 포함하여 탐지 메커니즘을 테스트하는 것은 모니터링 및 탐지 메커니즘의 적절성을 검증하는 데 중요합니다.

- 탐지에 대한 역할과 책임을 잘 정의하여 책임을 보장합니다.
- 탐지 활동은 적용 가능한 모든 요구 사항을 준수합니다.
- 탐지 프로세스가 테스트됩니다.
- 이벤트 탐지 정보가 전달됩니다.
- 탐지 프로세스가 지속적으로 개선됩니다.

응답 기능 (RS)

응답 기능은 사건 영향을 포함한 보안 이벤트 관리를 처리합니다.

대응 계획 범주 (RS.RP)

이 범주는 탐지된 사이버 보안 사고에 대한 대응을 보장하기 위해 실행 및 유지 관리되는 대응 프로세스 및 절차로 구성됩니다.

통신 범주 (RS.CO)

대응 활동은 내부(예: DDI, IT, 컴퓨팅, 네트워크, 클라우드 등) 및 외부 이해관계자(예: 외부 서비스 공급자, ISP)와 조정됩니다. DDI 책임과 DDI 시스템에 대한 액세스 권한이 있는 사람은 다음 각 영역에 참여해야 합니다.

- 직원은 대응이 필요할 때 자신의 역할과 작업 순서를 알고 있습니다.
- 사건은 설정된 기준에 따라 보고됩니다.
- 대응 계획과 일관되게 정보가 공유됩니다.
- 이해관계자와의 조정은 대응 계획과 일관되게 이루어집니다.
- 외부 이해관계자와의 자발적인 정보 공유를 통해 보다 광범위한 사이버 보안 상황 인식을 달성합니다.

분석 범주 (RS.AN)

효과적인 대응을 보장하고 복구 활동을 지원하기 위해 분석이 수행됩니다.

- DDI 시스템 및 통합 수집기(예: SIEM/SOAR 시스템)를 포함한 탐지 시스템의 알림을 조사합니다.
- 사건의 영향을 이해합니다.
- 포렌식은 사고의 근본 원인과 기여 원인을 식별하기 위해 수행됩니다.
- 사건은 대응 계획에 따라 분류됩니다.
- 내부 및 외부 소스(예: 내부 테스트, 보안 게시판 또는 보안 연구원)로부터 조직에 공개된 취약성을 수신, 분석 및 대응하기 위한 프로세스가 설정됩니다.

완화 범주 (RS.MI)

이벤트의 확장을 방지하고, 그 영향을 완화하고, 사건을 해결하기 위한 활동이 수행됩니다. 이를 위해서는 다음이 필요합니다.

- 이 사건은 다른 시스템이나 네트워크로의 추가 확장을 방지하기 위해 격리됩니다.
- 사건이 격리되고, 비상 계획이 구현되고, 포렌식 분석이 수행됨에 따라 이 사건으로 이어진 취약성에 대한 완화 접근 방식을 정의, 평가, 합의 및 구현해야 합니다.
- 새로 식별된 취약성은 완화되거나 허용되는 위험으로 문서화됩니다.

개선 사항 범주 (RS.IM)

조직 대응 활동은 현재 및 이전 탐지/대응 활동에서 배운 교훈을 통합하여 개선됩니다. 사건 복구 후 관련 직원과의 사후 분석은 사건, 대응을 개선하기 위한 가능한 방어 및 완화 단계, 학습한 교훈을 통합하기 위한 권장 대응 계획 업데이트를 검토하는 데 유용합니다. 사건 대응 전략을 적절하게 검토하고 업데이트해야 합니다.

복구 기능 (RC)

이 기능은 복원 능력과 복원 기능을 정의합니다.

복구 계획 범주 (RC.RP)

복구 프로세스 및 절차는 사이버 보안 사고의 영향을 받는 시스템 또는 자산의 복원을 보장하기 위해 실행 및 유지 관리됩니다.

- 사건 복구 계획은 이벤트 도중 또는 이후에 실행됩니다.
- 이벤트 기간 동안 중단, 손상 또는 중단에 직면하여 서비스 수준을 복원하기 위해 비상사태 및 해결 방법이 마련됩니다.
- 사건 종료 및 복원 후 영향을 받는 시스템은 알려진 작동 상태로 완전히 복구하기 위해 이전 기능으로 복원되어야 합니다.

개선 사항 범주 (RC.IM)

복구 계획 및 프로세스는 학습한 내용을 향후 활동에 통합함으로써 개선됩니다.

- 학습한 내용을 반영하도록 복구 계획을 업데이트해야 합니다.
- 복구 전략은 사건 복구 분석을 통해 개선된 사항이 있는 경우 검토하고 업데이트해야 합니다.

통신 범주 (RC.CO)

복원 활동은 내부 및 외부 당사자(예: 코디네이팅 센터, 인터넷 서비스 공급자, 공격 시스템 소유자, 피해자, 기타 CSIRT 및 공급업체)와 조정됩니다.

- 고객 및 일반 대중과의 커뮤니케이션은 사고, 대응 및 복구 상태, 계획된 조치에 대한 정보를 전달하기 위해 신중하게 관리됩니다.
- 일반적으로 사건에 대한 의미 있는 정보 및 사건으로부터 복구하기 위해 수행된 작업을 제공하면 평판을 유지하는 데 도움이 되지만 다른 단계가 필요할 수 있습니다.
- 경영진 및 경영진을 포함한 내부 이해관계자와의 커뮤니케이션은 사건, 대응 및 복구 상태, 공격이 지속될 경우 대체 접근 방식 평가를 포함한 계획된 조치와 관련하여 개방적이고 직접적이어야 합니다.

결론

NIST CSF 는 모든 유형 또는 규모의 조직이 전반적인 사이버 보안 태세를 개선하기 위해 통합할 수 있는 강력하고 광범위한 보안 프레임워크를 제공합니다. 조직의 위협을 줄이고 보안을 개선하려는 조직은 CSF 를 지침으로 사용하여 특정 허용 범위와 관련하여 위협을 식별 및 평가하고 리소스와 우선순위가 허용하는 한 이러한 위험을 줄이기 위한 제어를 구현할 수 있습니다.

권장되는 심층 방어 접근 방식은 특정 사건을 흡수하고 신속하게 대응 및 복구할 수 있는 조직의 능력을 강화합니다. 광범위한 디바이스 및 대역 내 네트워크 방어 수준을 넘어 DDI 및 관련 필수 네트워크 서비스를 통합하는 서비스 방어 수준은 보안 이벤트에 대한 귀중한 통찰력과 완화 수단을 추가할 수 있습니다. 이 백서에서는 DDI 수준의 사용에 대해 설명했으며 DDI 방어 및 전반적인 사이버 보안 태세를 강화하기 위해 고려할 수 있는 NIST CSF 코어 내의 제어 셋을 제공했습니다. 자세한 내용은 DNS 에 적용되는 NIST CSF 코어에 대한 하위 범주 수준을 다운로드하세요.