**제로트러스트 현황파악을 위한 수요기업 실태조사**

|  |  |  |  |
| --- | --- | --- | --- |
| **ID** |  |  |  |



안녕하십니까?

과학기술정보통신부와 한국정보보호산업협회에서는 우리나라 사업체의 제로트러스트 인식과 도입을 위한 현황을 파악하기 위해 정보보호 공시 대상 기업체를 대상으로 “제로트러스트 현황파악을 위한 수요기업 실태조사 ”를 실시하고 있습니다.

정부의 효과적인 정보보호 정책 수립에 도움이 될 수 있도록 귀사의 적극적인 협조를 부탁드립니다.

아울러 작성해 주신 자료는 조사와 연구에 관련된 목적에만 사용될 것이며, 비밀은 철저히 보장될 것을 약속드립니다. 설문조사에 응해 주심에 감사드리며, 귀사의 평안과 번창하심을 기원합니다.

2023년 8월

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **주관기관** | **전담기관** | **조사기관** | **실사 문의** | 비바컴퍼니 | **조사 문의** | 한국정보보호산업협회 |
| 과학기술정보통신부 | 한국정보보호산업협회 | ㈜비바컴퍼니 | - 서기현 책임, 070-4905-9522  - 박주연 선임, 070-4905-3137 | - 정호준 팀장, 02-6748-2006  - 이주영 파트장, 02-6748-2009 |

\* 본 조사는 통계법 제33조(비밀의 보호)에 따라 통계목적으로 이용되며, 귀사의 비밀이 절대 보장됨을 약속드리는 바입니다.



**본 설문은 향후, 제로트러스트 보안 제도 개선 및 정책 설계의 근거가 되는 자료로 활용됩니다 . 응답해 주신 모든 자료는 익명화 처리되므로 솔직한 응답을 부탁드립니다.**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | | | | 응답 |
| **지 역** | ① 서울 ② 부산 | ③ 대구 | | ④ 인천 ⑤ 광주 | | ⑥ 대전 | ⑦ 울산 ⑧ 세종 | | | ⑨ 경기 | |  |  |
| ⑩ 강원 ⑪ 충북 | ⑫ 충남 | | ⑬ 전북 ⑭ 전남 | | ⑮ 경북 | ⑯ 경남 ⑰ 제주 | | |  | |  |
| **기업명** |  | | | | | | | | | | | |  |
| **업 종** | ① 정보통신업 | | | ② 제조업 | | | | ③ 보건업 | | | | |  |
| ④ 금융 및 보험업 | | | ⑤ 전기가스공급 조절업 | | | | ⑥ 기타 ( | |  | | ) |
| **연간 총매출액** | ① 1억 미만 |  | | ② 1 ~ 5억 미만 | |  | ③ 5 ~ 50억 미만 | | |  | |  |  |
| ④ 50 ~ 100억 미만 |  | | ⑤ 100 ~ 1,000억 미만 | |  | ⑥ 1,000억 이상 | | |  | |  |
| **2022년 공시 정보보호 예산** | 백만원 | | **정보 기술 부문 투자액** | | 백만원 | | **정보 보호부문 투자액** | | 백만원 | | | |  |
| **총임직원** | 명 | | **정보 기술 부문 전담 인력** | | 명 | | **정보 보호 부문 전담 인력** | | 내부 인력 | | 명 | |
| 외부 인력 | | 명 | |

**SQ**

**응답자 선정 질문**

+보안 위험 영역 우려도 【전체, SA】

**SQ1** 귀사는 각 보안 영역의 위험도에 대해 얼마나 우려하고 계십니까?

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **문 항** | **전혀 우려 되지**  **않는다** | **별로 우려 되지**  **않는다** | **보통 이다** | **우려 되는 편이다** | **매우 우려 된다** | **해당 없음** | **응답** |
| **SQ1-1.** 원격 및 재택근무 시 보안위협 | ① | ② | ③ | ④ | ⑤ | ⑥ |  |
| **SQ1-2.** 협력사/파트너사를 통한 보안 위협 | ① | ② | ③ | ④ | ⑤ | ⑥ |  |
| **SQ1-3.** 내부자 유출 관련 보안 위협 | ① | ② | ③ | ④ | ⑤ | - |  |
| **SQ1-4.** 클라우드 이용 관련 보안 위협 | ① | ② | ③ | ④ | ⑤ | ⑥ |  |

+제로트러스트 인지 【전체, SA】

**SQ2** 귀사는 ‘제로트러스트’에 대해 알고 계십니까?

**‘신뢰할 수 있는 네트워크’라는 개념 자체를 배제하며, 기업망 내외부에 언제나 공격자가 존재할 수 있고, 명확한 인증 과정을 거치기 전까지는 모든 사용자, 기기 및 네트워크 트래픽을 신뢰하지 않으며, 인증 후에도 끊임없이 신뢰성을 검증함으로써 기업의 정보 자산을 보호할 수 있는 보안 모델.**

**네트워크 혹은 물리적 위치, 접속 기기에 상관없이 기본적으로 ‘비신뢰’에서 출발하여 강화된 인증 및 기기 상태 모니터링 등을 통하여 게속 검증한 후 신뢰도가 일정 수준을 넘어갈 때, 기업망 혹은 기업 데이터를 접근할 수 있는 권한을 부여**

**\* 제로트러스트란?**

① 모른다.

**☞ SQ4로 이동**

② 용어는 들어봤으나, 자세히 알지는 못한다.

**☞ SQ3으로 이동**

③ 용어에 대해 자세히 알고 있다.

**☞ SQ3으로 이동**

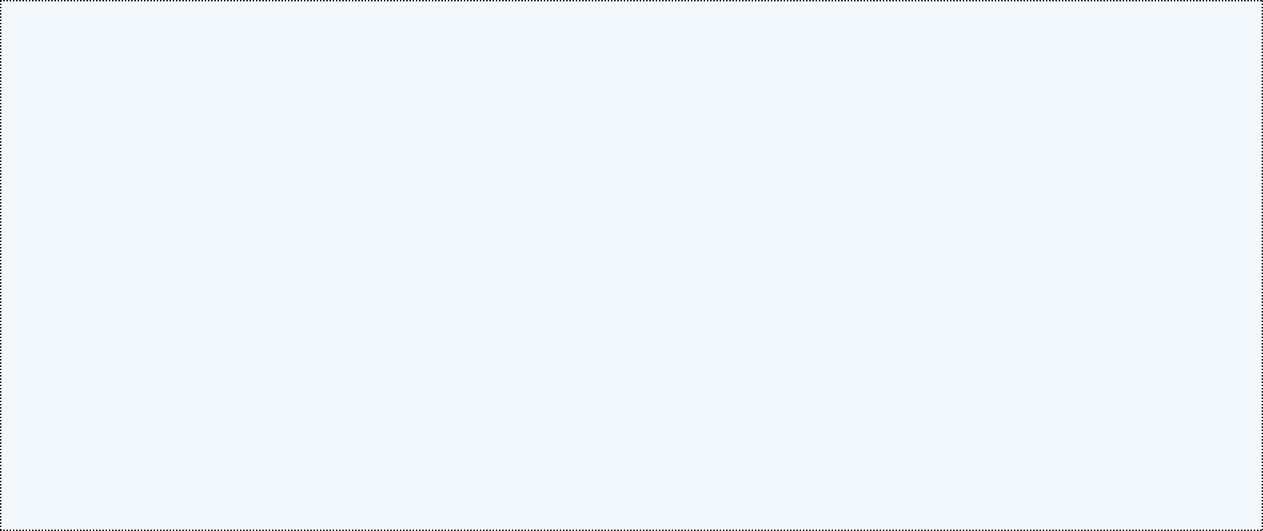
+제로트러스트 핵심원칙 인식 【전체, SQ2. 2),3) 응답자만】

**SQ3** 제로트러스트에 대해 알고 계신다면, 제로트러스트 모델 구현을 위한 핵심원칙 중

가장 중요한 것은 무엇이라고 생각하십니까?

|  |  |
| --- | --- |
| **핵심 원칙** | **세부 내용** |
| **인증 체계 강화** | ▲ 각종 리소스 접근 주체에 대한 신뢰도(사용하는 단말, 자산 상태, 환경요소, 접근 위치  등을 판단)를 핵심요소로 선정하여 인증 정책 수립 |
| **마이크로**  **세그멘테이션** | ▲ 보안 게이트웨이를 통해 보호되는 단독 네트워크 구역(Segment)에 개별 자원(자원그룹)을  배치하고, 각종 접근 요청에 대한 지속적인 신뢰 검증 수행 |
| **소프트웨어 정의**  **경계(SDP)** | ▲ 소프트웨어 정의 경계 기법을 활용하여 정책 엔진 결정에 따르는 네트워크 동적 구성,  사용자·단말 신뢰 확보 후 자원 접근을 위한 데이터 채널 형성 |

① 인증 체계 강화



**\* 제로트러스트 핵심원칙**

**: 제로트러스트 아키텍처를 구현하기 위한 접근방법으로 네트워크 환경에 따라 일부 상이할 수 있으나, 완전한 제로트러스트 솔루션은 3가지 핵심 원칙을 모두 포함**

**<제로트러스트 구현 핵심원칙>**

**※ 출처 : 제로트러스트 가이드라인 1.0(23.6., 과학기술정보통신부)**

② 마이크로 세그멘테이션

③ 소프트웨어 정의 경계

+제로트러스트 도입 중요성 【전체, SA】

**SQ4** 귀사의 보안 수준을 고려하였을 때, ‘제로트러스트 보안 모델’의 도입의 중요성에 대해 어떻게

생각하십니까?

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **전혀 중요하지 않다** | **중요하지 않은 편이다** | **보통이다** | **중요한 편이다** | **매우 중요하다** | **응답** |
| 실무진 | ① | ② | ③ | ④ | ⑤ |  |
| 경영진 | ① | ② | ③ | ④ | ⑤ |  |

+제로트러스트 도입 시급성 【전체, SA】

**SQ5** 귀사의 보안 수준을 고려하였을 때, ‘제로트러스트 보안 모델’의 도입의 시급성에 대해 어떻게

생각하십니까?

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **전혀 시급한 문제는 아니다** | **시급하지 않은 편이다** | **보통이다** | **시급한 편이다** | **매우 시급한 편이다** | **응답** |
| 실무진 | ① | ② | ③ | ④ | ⑤ |  |
| 경영진 | ① | ② | ③ | ④ | ⑤ |  |

+ 제로트러스트 도입 현황 【전체, SA】

**SQ6** 귀사의 ‘제로트러스트 보안 모델’의 도입 현황은 어떻게 되십니까?

① 현재 적용하고 있다. **☞ SQ8로 이동**

② 현재 적용하고 있지는 않으나, 구체적인 도입 계획이 있다. **☞ SQ8로 이동**

③ 도입 의사는 있으나, 어떻게 해야하는지 모르겠다/구체적 계획 없다. **☞ SQ8로 이동**

④ 도입 계획이 전혀 없다.

**☞ SQ7로 이동**

+ 제로트러스트 도입 현황 【SQ6. 4) 응답자만, MA】

**SQ7** 적용 계획이 없는 이유는 무엇입니까? 모두 선택해 주십시오.

① 임원진의 보안 인식 부족

② 보안 강화의 필요성을 못느껴서

③ 제로트러스트 도입 비용의 부담

④ 도입 시 업무상의 불편성 증가

⑤ 제로트러스트에 대한 정보 부족

⑥ 기타( )

**☞ SQ7 응답 후 설문 종료 \*\*\*\* 설문에 응답해주셔서 감사합니다 \*\*\*\***

+보안 위험 영역 제로트러스트 도입 기대도 【전체, SA】

# SQ8

‘제로트러스트 보안 모델’을 도입함으로써 다음 보안 위협 사항에 대해 얼마나 해결 할 수 있을 것이라고 기대하고 계십니까?

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **문 항** | **전혀 기대 하지 않는다** | **별로 기대 하지 않는다** | **보통 이다** | **기대 하는 편이다** | **매우 기대 한다** | **해당 없음** | **응답** |
| **SQ8-1.** 원격 및 재택근무시 보안위협 | ① | ② | ③ | ④ | ⑤ | ⑥ |  |
| **SQ8-2.** 협력사/파트너사를 통한 보안 위협 | ① | ② | ③ | ④ | ⑤ | ⑥ |  |
| **SQ8-3.** 내부자 유출 관련 보안 위협 | ① | ② | ③ | ④ | ⑤ | - |  |
| **SQ8-4.** 클라우드 이용 관련 보안 위협 | ① | ② | ③ | ④ | ⑤ | ⑥ |  |

**A**

**제로트러스트 수요 인식**

+ 제로트러스트 도입 이유 【전체, MA】 \*추후 FGI 질문 사항

**A1** 귀사가 ‘제로트러스트 보안 모델’을 도입하게 된 계기/도입해야한다고 생각하는 이유는 무엇입

니까? 최대 2순위까지 순서대로 응답하여 주십시오.

**1순위 2순위**

① 정교해지는 보안 공격에 대한 보안 강화를 위해

② 보안제품/서비스 관련 비용 절약을 위해

③ IT환경의 변화로 클라우드 및 다양한 단말 속에서 보안성을 높이기 위해

④ 내부자에 의한 보안 공격 방어를 위해

⑤ 보안 트렌드에 따르기 위해

⑥ 기타( )

+ 제로트러스트 도입 기대효과 【전체, MA】 \*추후 FGI 질문 사항

**A2** 귀사가 ‘제로트러스트 보안 모델’을 도입함으로서 바라는 주된 기대효과는 무엇입니까?

최대 2순위까지 순서대로 응답하여 주십시오.

**1순위 2순위**

① 전체적인 보안 기능 향상

③ 사용자의 이용 환경 개선

⑤ 기타 ( )

② 사고 후 복원력 향상

④ IT 비용 절감

+ 제로트러스트 도입 시 어려운 점 【전체, MA】 \*추후 FGI 질문 사항

**A3** 제로트러스트 보안 모델 도입시 다음 사항에 대해 어려움을 느끼시는 정도는 어떻게 되시나요?

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **문 항** | **전혀 어렵지 않다** | **별로 어렵지 않다** | **보통 이다** | **어려운 편이다** | **매우 어렵다** | **응답** |
| **A3-1.** 고성능 제품을 보유한 공급사 부족 | ① | ② | ③ | ④ | ⑤ |  |
| **A3-2.** 제로트러스트 도입 전략에 대한 지식 부족 | ① | ② | ③ | ④ | ⑤ |  |
| **A3-3.** 경영진의 제로트러스트에 대한 개념 및 인식 부족 | ① | ② | ③ | ④ | ⑤ |  |
| **A3-4.** 기존 사용 중인 보안 제품과의 호환성 | ① | ② | ③ | ④ | ⑤ |  |
| **A3-5.** 도입시 필요한 예산의 부족 | ① | ② | ③ | ④ | ⑤ |  |

+ 제로트러스트 관련 솔루션 선택시 고려 요소 【전체, 순위형】

**A4** 제로트러스트 관련 솔루션/서비스 선택시 고려요소는 무엇인가요?

응답해주십시오.

최대 2순위까지 순차별로

**1순위 2순위**

① 제품 성능

③ 제품 공급사의 이미지

⑤ 원활한 유지보수 및 A/S

**⑦** 기타( )

② 제품 공급사의 인지도

④ 기존 제품과의 호환성

⑥ 제품 가격

+ 제로트러스트 관련 솔루션 선택시 외산/국산 선호도 【전체, SA】

**A5** 제로트러스트 관련 솔루션/서비스 선택시 외산제품과 국산제품 중 어떤 것을 선호하십니까?

① 국산제품 **☞ A5-1로 이동**

③ 특별히 선호도를 구분하지 않음 **☞ A6으로 이동**

② 외산제품 **☞ A5-1로 이동**

+ 제로트러스트 관련 솔루션 선택시 외산/국산 선호 이유 【전체, A5. 1),2) 응답자만, 순위형】

**A5-1** 외산제품 혹은 국산제품을 더 선호하는 이유는 무엇입니까? 순서대로 응답하여 주십시오

**1순위 2순위**

① 제품 성능이 더 좋아서

③ 공급사의 이미지가 더 좋아서

⑤ 유지보수/AS를 위한 인프라가 더 잘 갖춰있어서

⑦ 정부 지원 혜택이 있어서 **☞ 국산제품 응답자만 응답 가능**

② 공급사의 인지도가 더 높아서

④ 기존 제품과의 호환성이 더 잘되어서

⑥ 제품 가격이 더 저렴해서

⑧ 기타( )

+ 제로트러스트 도입시 필요 정책 【전체, 순위형】 \*추후 FGI 질문 사항

**A6** 귀사가 ‘제로트러스트 보안 모델’을 도입을 위해 가장 필요한 정책은 무엇이라고 생각하십니까?   
최대 2순위까지 순차별로 응답해주십시오.

**1순위 2순위**

① 수요기업과 공급기업을 연계하는 실증사업 확대

② 제로트러스트 도입 관련 구체적인 방안 및 절차 마련

③ 보안 강화 및 제로트러스트 필요성 인식 제고

④ 보안 인증 관련 제도 완화(보안 적합성 검증, 클라우드 서비스 보안인증, 정보보호 및 개인정보보호 관리체계 인증)

⑤ 기타( )

**B**

**제로트러스트 기술 현황**



**해당 기술 영역은 과기정통부에서 발표한 「제로트러스트 가이드라인 1.0」을 기준으로 작성 되♘습니다**

+보안영역별 적용 수준-식별자-신원 【전체, SA】

**B1**

**(핵심요소1 : 식별자-신원)** 다음은 ‘식별자-신원’과 관련된 보안 기능입니다. 현재, 귀사에서 각 보안 영역에서의 적용 수준을 응답하여 주십시오.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | | | | | 응답 |
| **B1-1.** 식별자 관리 | ① 기존 | ② 향상 | ③ 최적화 | ④ |  |
| 온프레미스 ID 공급자 | 클라우드와 온프레미스 시스템을 기반으로 ID 연합 | 클라우드 및 온프레미스 환경 전반에 걸쳐 글로벌 ID 활용 | 관련 기능 없음 |
| **B1-2.** 인증 | ① 기존 | ② 향상 | ③ 최적화 | ④ |  |
| 패스워드 혹은 다중 인증 방식 | 다중 인증 방식 기반 인증 | 접근 권한을 승인할 때 뿐만 아니라, 지속적인 신원 검증 | 관련 기능 없음 |

+보안영역별 적용 수준-기기 및 엔드포인트 【전체, SA】

**B2**

**(핵심요소2 : 기기 및 엔드포인트)** 다음은 ‘기기 및 엔드포인트’와 관련된 보안 기능입니다. 현재, 귀사 에서 각 보안영역에서의 적용 수준을 응답하여 주십시오.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | 응답 |
| **B2-1.** | 데이터 접근 제어 | ① 기존 | ② 향상 | ③ 최적화 | ④ |  |
| 데이터 접근 기기에 대한 정보에 의존하지 않음 | 첫 데이터 접근시 기기 상태 고려 | 기기에 대한 실시간 위험 분석 고려 | 관련 기능 없음 |
|  | | ① 기존 | ② 향상 | ③ 최적화 | ④ |  |
| **B2-2.** 자산  관리 | | 단순하며 수동으로 추적되는 기기 목록 관리 | 자동화된 방법을 이용하여 자산 관리, 취약성 식별, 자산에 대한  패치 적용 | 클라우드 및 원격을 포함한 모든 환경에 걸쳐 자산 및 취약점 관리  통합 | 관련 기능 없음 |

+보안영역별 적용 수준-네트워크 【전체, SA】

**B3**

**(핵심요소3 : 네트워크)** 다음은 ‘네트워크’와 관련된 보안 기능입니다. 현재, 귀사에서 각 보안영역에 서의 적용 수준을 응답하여 주십시오.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | | | | | 응답 |
| **B3-1.** 네트워크  세분화 | ① 기존 | ② 향상 | ③ 최적화 | ④ |  |
| 대규모 경계/분리를 사용하는 네트워크 구조 정의 | 일부 내부적인 세분화를 갖는 송수신 소규모 경계를 통해 더 많은 네트워크 구조 정의 | 네트워크 구조는 주변 응용 워크플로우를 기반으로 완벽히 분산된 송수신 세부경계 및 더욱  깊은 내부 세분화로 구성됨 | 관련 기능 없음 |
| **B3-3.** 암호화 | ① 기존 | ② 향상 | ③ 최적화 | ④ |  |
| 최소한의 내외부 트래픽에 대한 명시적 암호화 | 내부 응용에 대한 모든 트래픽 및 일부 외부 트래픽 암호화 | 가능한 경우, 내외부로 전달되는 모든 트래픽 암호화 | 관련 기능 없음 |

+보안영역별 적용 수준-시스템 【전체, SA】

**B4**

**(핵심요소4 : 시스템)** 다음은 ‘시스템’과 관련된 보안 기능입니다. 현재, 귀사에서 각 보안영역에서의 적용 수준을 응답하여 주십시오.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | | | | | 응답 |
| **B4-1.** 접근  통제 | ① 기존 | ② 향상 | ③ 최적화 | ④ |  |
| 시스템 접근을 위한 계정 인증은 로컬 시스템에 저장된 ID/패스워드 등 단순 인증을 기반으로 하고 정적 속성 등 최소한의 권한 분리 정책 적용 | 시스템 접근 시 중앙 집중적인증/인가/모니터링과 속성에 의존하며, MFA 인증을 기본으로 시스템 파일, 디렉토리에 접속하거나 주요 명령어를 실행할 때 접근제어 정책에 따라 보안정책 적용 | 시스템 접근시 MFA 인증 및 엔드포인트 시스템의 신뢰도를 기반으로 접근인가 진행. 시스템에 영향을 미치는 명령 실행시 실시간 신뢰도 재산정 및 위험 분석을 기반으로 강력하고 지속적인 접근제어  정책 적용 | 관련 기능 없음 |
| 시스템  **B4-2.** 계정  관리 | ① 기존 | ② 향상 | ③ 최적화 | ④ |  |
| 접근 인가를 진행하는 권한 사용자의 계정 관리가 시스템별로 상이하게 관리 | 접근 인가를 진행하는 권한 사용자의 계정 관리가 독립 시스템으로 이루어지고 다른 시스템들과 동기화 및 프로비저닝 됨 | 접근 인가를 진행하는 권한 사용자의 계정 관리가 독립 시스템을 기반으로 통합적으로 이루어지고 권한 사용자의 보안 관리 정책이 계정 관리와 통합 및 중앙 일원화되어 접근제어  정책이 적용 | 관련 기능 없음 |

+보안영역별 적용 수준-응용 및 워크로드 【전체, SA】

**B5**

**(핵심요소5 : 응용 및 워크로드)** 다음은 ‘응용 및 워크로드’와 관련된 보안 기능입니다. 현재, 귀사에 서 각 보안영역에서의 적용 수준을 응답하여 주십시오.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | | | | | 응답 |
| **B5-1.** 접근  인가 | ① 기존 | ② 향상 | ③ 최적화 | ④ |  |
| 응용 접근은 주로 로컬 인가 및 정적 속성에 기반 | 응용 접근은 중앙 집중적 인증, 인가, 모니터링과 속성에  의존 | 실시간 위험 분석을 고려하여 응용 접근을 지속적으로 인가 | 관련 기능 없음 |
| **B5-2.** 접근성 | ① 기존 | ② 향상 | ③ 최적화 | ④ |  |
| 일부 중요 클라우드 응용은 인터넷을 통해 사용자가 직접 접속하며, 그 외의 다른 응용은  VPN을 통한 접속 | 모든 클라우드 응용과 일부 온프레미스 응용은 인터넷을 통해 사용자가 직접 접속하며, 그 외의  다른응용은VPN을통한접속 | 모든 응용은 인터넷을 통해 사용자가 직접 접속 가능 | 관련 기능 없음 |

+보안영역별 적용 수준-데이터 【전체, SA】

**B6**

**(핵심요소6 : 데이터)** 다음은 ‘데이터’와 관련된 보안 기능입니다. 현재, 귀사에서 각 보안영역에서의 적용 수준을 응답하여 주십시오.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | | | | | 응답 |
| 데이터  **B6-1.** 목록  관리 | ① 기존 | ② 향상 | ③ 최적화 | ④ |  |
| 데이터를 수동으로 분류하고 데이터 목록 작업이 부실하여, 일관되지 않은 데이터 분류 | 일부 자동화된 추적을 기반으로, 수동으로 데이터 목록 작업 수행. 수동 정적인 방식을 조합하여 데이터 분류 | 강력한 태그 작업 및 추적으로 지속적인 목록 작업. 기계 학습 모델을 사용하여 분류 강화 | 관련 기능 없음 |
| **B6-2.** 암호화 | ① 기존 | ② 향상 | ③ 최적화 | ④ |  |
| 온프레미스 데이터 저장소에 암호화 되지  않은 상태로 데이터 저장 | 클라우드 혹은 원격 환경에서 암호화 저장 | 저장소의 모든 데이터 암호화 | 관련 기능  없음 |

+보안영역(가시성 및 분석) 활용 영역 【전체, MA】

**B7** 각 보안영역 중 **‘가시성 및 분석 기능’**을 활용하고 있는 영역에 대해 모두 선택해 주십시오.

**사용자 혹은 기기, 응용 및 워크로드의 상태 확인 등 중요하고 상황에 맞는 세부 정보를 이용하여 분석하고 가시성을 제공하는 기능을 의미**

**이 기능을 통해 비정상 행위에 대한 탐지를 개선하고, 보안 정책 및 접근제어 결정을 동적으로 변화시킬 수 있음. 또한, 네트워크에 대한 원격 감시 이상으로 트래픽을 패킷 단위로 직접 캡쳐하고 분석함으로써, 네트워크를 통해 진입하는 모든 종류의 위협을 관찰하고 지능화된 방어 기법을 적용 할 수 있음**

**\* 가시성 및 분석이란?**

① 식별자-신원 영역

② 기기 및 엔드포인트 영역

③ 네트워크 영역

④ 시스템 영역

⑤ 응용 및 워크로드 영역

⑥ 데이터 영역

+보안영역(자동화기능) 활용 영역 【전체, MA】

**B8** 각 보안영역 중 **‘자동화 및 통합 기능’**을 활용하고 있는 영역에 대해 모두 선택해 주십시오.

**기존에 수동적으로 적용하던 보안 프로세스를 개선하여 자동화된 정책 기반 보안 프로세스를 적용하여 보다 신속한 보안 조치가 가능하게 하는 기능.**

**SIEM 및 기타 자동화된 보안 솔루션 통합, SOAR 적용 등의 방법을 통하여, 제로트러스트 아키텍처를 구현하고자 하는 기업망의 모든 환경에서 정의된 프로세스와 일관된 보안 정책을 시행한다면 자동화된 통합 보안 대응이 가능함.**

**\* 자동화 및 통합이란?**

① 식별자-신원 영역

② 기기 및 엔드포인트 영역

③ 네트워크 영역

④ 시스템 영역

⑤ 응용 및 워크로드 영역

⑥ 데이터 영역

+보안영역별 중요성 【전체, SA】

**B9** 귀사에서 중요하게 생각하는 보안영역은 무엇입니까? 순서대로 나열해주세요.

**중요순위 > > > > >**

① 식별자-신원 영역

② 기기 및 엔드포인트 영역

③ 네트워크 영역

④ 시스템 영역

⑤ 응용 및 워크로드 영역

⑥ 데이터 영역

+보안영역별 시급성 【전체, SA】

**B10** 추후 제로트러스트 도입시 가장 시급하게 보강해야하는 보안영역은 무엇입니까? 순서대로 나열

해주세요.

**시급순위 > > > > >**

① 식별자-신원 영역

② 기기 및 엔드포인트 영역

③ 네트워크 영역

④ 시스템 영역

⑤ 응용 및 워크로드 영역

⑥ 데이터 영역

**C**

**KOZETA 인지여부**

+KOZETA 인지여부 【전체】

**C1** 귀하께서는 한국제로트러스트위원회(KOZETA)에 대해 들어보셨습니까?

① 처음 들어봤다. **☞ C2로 이동**

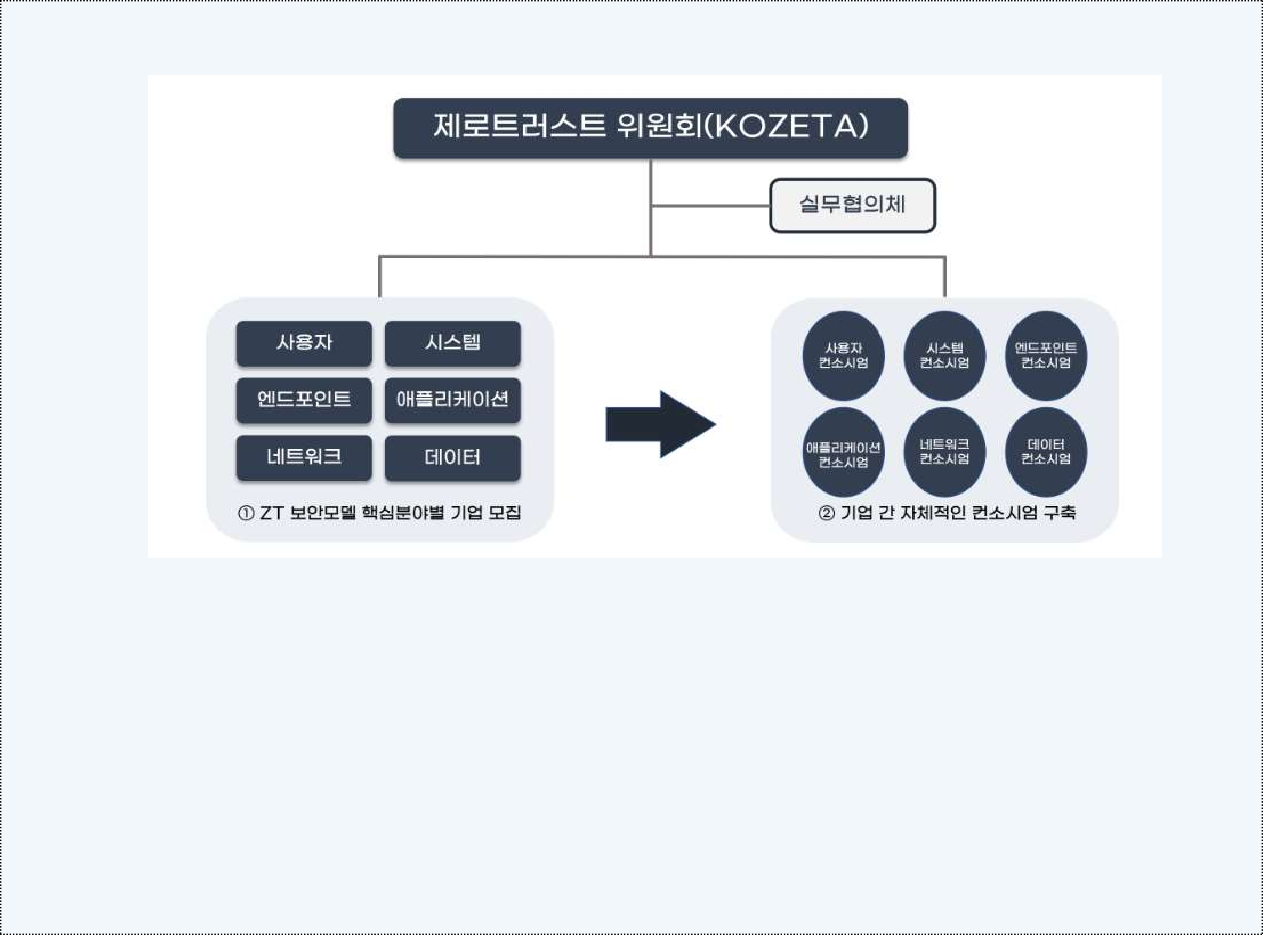
② 들어봤으나, 자세히 알지는 못한다. **☞ C2로 이동**

③ 자세히 알고 있으나, 참여기업은 아니다 **☞ C2로 이동**

④ 자세히 알고있으며 참여기업이다. **☞ Z1으로 이동**

+ KOZETA 참여 수요 【전체, C1 1-3응답자만】

**C2** 산업계 주도 제로트러스트 모델 개발을 위한 공급 수요기업 간 자유로운 협력환경 조성 을 지원하기 위해 KOZETA를 운영하고 있습니다. KOZETA에 참여할 계획이 있으십니까?



**□ KOZETA 활동 주요 내용 ㅇ 위원회 구성**

* **정보보호 산업계가 주도하고 수요기업(기관), 학계 등이 참여하여 제로트러스트 모델 개발 ㅇ 컨소시엄 구축**
* **제로트러스트 보안모델 핵심분야\*를 기반으로 회원사 간 또는 수요기업(기관)과 연계하여 컨소시엄을 구축**
* **컨소시엄을 통한 다양한 제로트러스트 모델 제시**

**\* ①사용자 ②엔드포인트 ③네트워크 ④시스템 ⑤애플리케이션 ⑥데이터**

**☞ KOZETA 회원사 대상 기업 컨택포인트를 공유하여 회원사 간 자유롭게 컨소시엄을 구축할 수 있는 환경 조성**

① 참여할 계획이 있다 **☞ Z1로 이동**

② 계획없다 **☞ 설문 종료**

**Z**

**FGI 참석 여부**

+FGI 참석여부

**Z1** 한국정보보호산업협회는 국내 제로트러스트 도입의 활성화를 위한 ‘제로트러스트 보안 로드맵 마련을 위한 실증방안연구’를 진행하고 있습니다. 이에 설문 참석자 분들을 대상

으로 다음과 같은 논의 주제로 FGI를 개최하고자 합니다. 참석의향이 있으십니까?

|  |  |
| --- | --- |
| **일시** | **2023년 10월 중** |
| **장소** | **서울 송파구 중대로 135 KISIA 사무국** |
| **주요 논의 내용** | 1. **제로트러스트 관련 기술 수요** 2. **제로트러스트 보안 모델 도입 계기 / 바라는 효과 / 도입시 어려운 점** 3. **제로트러스트 보안 모델 도입 관련 정부 지원 방안** 4. **KOZETA 사업 참여 시 기대하는 점** |

① 예 **☞ Z2로 이동**

② 아니오 **☞ 설문 종료**

+컨택포인트

**Z2** 귀하의 정보를 기재해주세요.

|  |  |
| --- | --- |
| **회사명** |  |
| **부서 및 직함** |  |
| **성함** |  |
| **전화번호** |  |

**\* 설문에 응답해 주셔서 감사합니다 \***