**제로트러스트 현황파악을 위한 공급기업 실태조사**

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



안녕하십니까?

과학기술정보통신부와 한국정보보호산업협회에서는 우리나라 사업체의 제로트러스트 인식과 도입을 위한 현황을 파악하기 위해 정보보안 산업 영위 기업을 대상으로 “제로트러스트 현황파악을 위한 공급기업 실태조사 ”를 실시하고 있습니다.

제로트러스트 도입과 관련한 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

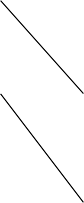
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **주관기관** | **전담기관** | **조사기관** | **실사 문의** | 비바컴퍼니 | **조사 문의** | 한국정보보호산업협회 |
| 과학기술정보통신부 | 한국정보보호산업협회 | ㈜비바컴퍼니 | - 서기현 책임, 070-4905-9522  - 박주연 선임, 070-4905-3137 | - 정호준 팀장, 02-6748-2006  - 이주영 파트장, 02-6748-2009 |

**[조사 대상자]**

**- [Random]**

**정보보안기업 회원사**

\* 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** |  | | | | | | | |  |
| **연간 총매출액**  **(2022)** | 백만원 | **보안매출액**  **(2022)** | 백만원 | | **총 임직원**  **(2022.12.31)** | **명** | **보안 인력수 (2022.12.31** | **명** |  |
| **주력 보안 분야** | ① 네트워크 보안(웹방화벽, IPS, VPN, NAC, NDR 등) | | | ④ 클라우드 보안 솔루션(CWPP, CSPM, CASB, SASE 등) | | | | |  |
| ② 엔드포인트 보안(CDR, EDR, APT대응, 랜섬웨어 대응 등) | | | ⑤ 컨텐츠/데이터 보안 솔루션(DLP, DRM, 메일보안 등) | | | | |
| ③ 플랫폼 보안/보안관리 솔루션(SOAR, XDR, TI 등) | | | ⑥ 공통인프라 보안 솔루션(SSO, EAM, PKI, FIDO, SIEM 등) | | | | |
| **제로 트러스트 부문 주력 보안 분야** | ① 네트워크 보안(웹방화벽, IPS, VPN, NAC, NDR 등) | | | ④ 클라우드 보안 솔루션(CWPP, CSPM, CASB, SASE 등) | | | | |  |
| ② 엔드포인트 보안(CDR, EDR, APT대응, 랜섬웨어 대응 등) | | | ⑤ 컨텐츠/데이터 보안 솔루션(DLP, DRM, 메일보안 등) | | | | |
| ③ 플랫폼 보안/보안관리 솔루션(SOAR, XDR, TI 등) | | | ⑥ 공통인프라 보안 솔루션(SSO, EAM, PKI, FIDO, SIEM 등) | | | | |

**SQ**

**제로트러스트 도입 현황**

+ 제로트러스트 관련 제품 현황 【전체, SA】

# **SQ1** 귀사의 ‘제로트러스트 보안’ 관련 제품/서비스 현황은 어떻게 되십니까?

**‘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 관련 제품/서비스가 출시되어 있다 **☞ SQ2로 이동**

② 현재 출시된 제품은 없으나, 관련 제품/서비스가 개발 단계에 있다

③ 현재 출시된 제품은 없으나, 관련 제품/서비스를 개발 계획이 있다

**☞ SQ3으로 이동**

**☞ SQ3으로 이동**

④ 관련하여 제품/서비스 개발 계획이 전혀 없다.

**☞ A파트로 이동**

+제로트러스트 수요 업종 매출 비중 【SQ1. 1)응답자만, Open】

# **SQ2** 현재, 제로트러스트 관련 주 거래처와 매출액을 업종별로 구분하여 기재해 주십시오.



**※ 향후, 제도 및 정책 설계의 근거가 되는 자료이므로, 대략적으로라도 응답 부탁드립니다.**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **구 분** | | | **거래처수** | **매출액** |
| **수요 기업 업종** | **매출 있음** | 금융 및 보험업 | 개 | 백만원 |
| 정보통신업 | 개 | 백만원 |
| 제조업 | 개 | 백만원 |
| 전기가스 공급 조절업 | 개 | 백만원 |
| 보건업 | 개 | 백만원 |
| 공공기관 | 개 | 백만원 |
| 기타 | 개 | 백만원 |
| 합 계 | 개 | 백만원 |
| **매출 없음** | 제품/서비스는 있으나 관련 매출은 아직 없음 | | |

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

# **SQ3** 귀사가 제로트러스트 제품/서비스를 개발하거나 출시한 이유는 무엇입니까?

# 모두 선택하여 주십시오.

① 기존 고객사의 보안에 대한 인식 향상

② 제로트러스트 기술과 관련한 신규 고객사 확보

③ 제로트러스트 제품/서비스를 개발/출시함으로써,

회사 인지도 향상

④ 경쟁사의 제로트러스트 제품/서비스 확대에 대한 대응

⑤ 기타( )

+ 제로트러스트 시장 확대시 어려운 사항 【전체, 5점척도】 \*추후 FGI 질문 사항

# **SQ4** 제로트러스트 관련 사업 확대 시 다음 사항에 대해 어려움을 느끼시는 정도는 어떻게 되십니까?

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **문 항** | **전혀 어렵지 않다** | **별로 어렵지 않다** | **보통 이다** | **어려운 편이다** | **매우 어렵다** | **응답** |
| **SQ4-1.** 수요기업의 제로트러스트 도입에 대한 인식 부족 | ① | ② | ③ | ④ | ⑤ |  |
| **SQ4-2.** 시장의 불확실성 때문에 사업 확대시 위험 부담 | ① | ② | ③ | ④ | ⑤ |  |
| **SQ4-3.** 전문 인력의 부족 | ① | ② | ③ | ④ | ⑤ |  |
| **SQ4-4.** 기술개발의 어려움 | ① | ② | ③ | ④ | ⑤ |  |
| **SQ4-5.** 공급 절차의 복잡성(ex. 인증획득, 도입 절차 등) | ① | ② | ③ | ④ | ⑤ |  |
| **SQ4-6.** 정책 및 방향성의 부재 | ① | ② | ③ | ④ | ⑤ |  |
| **SQ4-7.** 수요기업의 기존 솔루션과의 연동 어려움 | ① | ② | ③ | ④ | ⑤ |  |

+ 제로트러스트 도입 전략 【전체, 순위형】

# **SQ5** 제로트러스트 관련 사업 확대를 위해 귀사가 우선시하는 전략은 무엇입니까? 시급성과 중요도를

# 나누어서 3순위까지 응답하여 주십시오.

|  |  |  |  |
| --- | --- | --- | --- |
| **시급성 1순위** | **2순위** |  | **3순위** |
|  |  |  |  |
| **중요성 1순위** | **2순위** |  | **3순위** |
| ① 기술연구개발을 통한 경쟁력 확보  ② 영업을 통한 수요기업 발굴  ③ 제로트러스트 관련 전문 인력 확보  ④ 유통망 확대  ⑤ 제로트러스트와 제품에 대한 홍보  ⑥ 기타 ( ) |  |  |  |

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

# **SQ6** 제로트러스트 모델 활성화를 위하여 정부지원이 필요한 부분은 무엇입니까? 시급성과 중요도를

# 나누어서 3순위까지 응답하여 주십시오.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **시급성 1순위** |  | **2순위** |  | **3순위** |
|  |  |  |  |  |
| **중요성 1순위** |  | **2순위** |  | **3순위** |
| ① 전문인력 양성  ② 기술 개발 지원 |  |  |  |  |

③ 수요기업과 공급기업을 연계하는 사업 확대(ex. 실증사업, 바우처지원 등)

④ 법/제도 제ㆍ개정

⑤ 공공부문의 시장 수요 창출

⑥ 해외지원 사업 확대

⑦ 제로트러스트 관련 홍보 확대

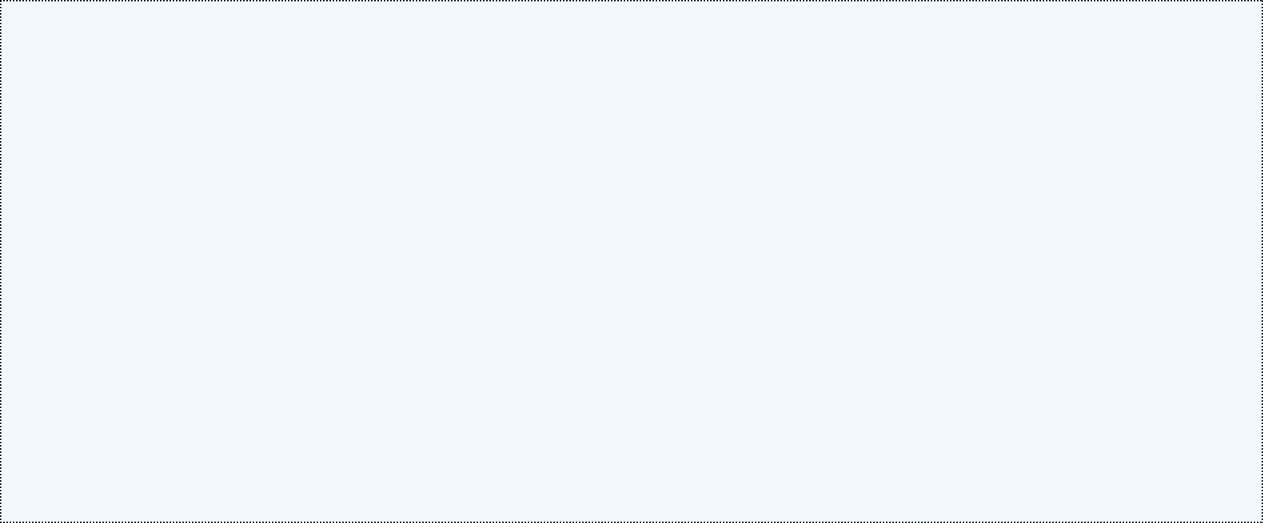
⑧ 기타( )



**해당 부분 정의는 과기정통부에서 발표한 「제로트러스트 가이드라인 1.0」을 기준으로 작성되었습니다.**

+ 제로트러스트 핵심원칙 인식 【전체, SA】

# **SQ7** 제로트러스트 모델 구현을 위한 핵심 원칙은 무엇이라고 생각하십니까?



**\* 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>**

|  |  |
| --- | --- |
| **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

② 마이크로 세그멘테이션

③ 소프트웨어 정의 경계

+ 제로트러스트 연동체계 인식 【전체, SA】

# **SQ8** 기존 솔루션과 제로트러스트 솔루션을 연동 시, 아래 보기 중 어떤 연동 체계가 가장 적합

# 하다고 생각하십니까?

① 엔드포인트보안 제품군(EDR, AntiVirus 등)과 제로트러스트 솔루션

② 플랫폼 보안/보안관리 제품군(SOAR, SIEM 등)과 제로트러스트 솔루션

③ 네트워크보안 제품군(FW, IPS, NDR 등)과 제로트러스트 솔루션

**A**

**제로트러스트 관련 기술 현황**



**\* 전체 기업**



**해당 기술 영역은 과기정통부에서 발표한 「제로트러스트 가이드라인 1.0」을 기준으로 작성 되었습니다**

**【제로트러스트 기술수준-식별자/신원, 전체】**

# **(핵심요소1 : 식별자-신원)** 다음은 ‘식별자-신원’과 관련된 보안 기능입니다.

**A1**

# 관련된 제품명을 기재해주시고, 각 부문에서 귀사의 제품은 어느 단계에 있습니까?



① ‘식별자-신원’과 관련된 보안 제품/서비스 없음

**☞ A2로 이동**

② ‘식별자-신원’과 관련된 보안 제품/서비스 있음

**☞ A1-1로 이동**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **A1. 제품명** | | **( )**  ※ 귀 사의 제품/서비스는 모두 기재해주시고 아래 항목은 제품/서비스의 전반적인 단계에 대해 응답해주십시오 | | | | **응답** |
| **A1-1.** | 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 |
| **A1-2.** | 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 |
| **A1-3.** | 위험도 평가 | ① 기존 | ② 향상 | ③ 최적화 | ④ |  |
| 위험에 대한 제한된 결정 | 단순한 분석과 정적 규칙을 기반으로 식별자 위험성 판단 | 기계학습 알고리즘으로 실시간 사용자 행동 분성르 통해 위험 결정 및 지속적 보호 | 관련 기능 없음 |
|  |  | ① 기존 | ② 향상 | ③ 최적화 | ④ |  |
| **A1-4.** | 가시성 및 분석 | 기본적이며 정적인 속성을 기반으로 사용자 활동에 대한 가시성 분류 | 기본 속성으로 사용자 활동에 대한 가시성 집계 후 분석 및 보고를 통한 수동적 개선 | 높은 정확도의 속성, 사용자 및 개체 행동 분석(UEBA)솔루션을 통해 사용자 가시성 확보 및 중앙 집중화 | 관련 기능 없음 |
| **A1-5.** | 자동화 및 통합 | ① 기존 | ② 향상 | ③ 최적화 | ④ |  |
| ID와 자격 증명을 수동으로 관리 통합 | ID연합 및 ID저장소를 통한 관리 허용을 위한 기본 자동화 통합 | ID 생명주기를 완벽히 통합하고, 동적 사용자 프로파일링, 동적 ID 및 그룹 멤버십,  적시(just-in-time), 적절한(just-enough)접근제  어 구현 | 관련 기능 없음 |

**【제로트러스트 기술수준-기기 및 엔드포인트, 전체】**

**A2**

**(핵심요소2 : 기기 및 엔드포인트)** 다음은 ‘기기 및 엔드포인트’와 관련된 보안 기능입니다.

관련된 제품명을 기재해주시고, 각 부문에서 귀사의 제품은 어느 단계에 있습니까?

① ‘기기 및 엔드포인트’와 관련된 보안 제품/서비스 없음

**☞ A3으로 이동**

② ‘기기 및 엔드포인트’와 관련된 보안 제품/서비스 있음

**☞ A2-1로 이동**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **A2. 제품명** | | **( )**  ※ 귀 사의 제품/서비스는 모두 기재해주시고 아래 항목은 제품/서비스의 전반적인 단계에 대해 응답해주십시오 | | | | **응답** |
| **A2-1.** | 정책 준수 모니터링 | ① 기존 | ② 향상 | ③ 최적화 | ④ |  |
| 기기 정책 준수를 위한 제한된 정보 제공 | 대부분의 기기에 정책 준수 시행 메커니즘 사용 | 지속적인 기기 보안상태 모니터링 및 검증 | 관련 기능 없음 |
| **A2-2.** | 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 |  |
| **A2-3.** | 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 |
| **A2-4.** | 가시성 및 분석 | ① 기존 | ② 향상 | ③ 최적화 | ④ |  |
| 기기 관리는 라벨의 수동 검사 및 주기적 네트워크 검색/보고에 의존 | 정책 미준수 구성 요소를 격리하며, 기기 목록 재조정 | 지속적으로 기기 상태 평가 | 관련 기능 없음 |
| **A2-5.** | 자동화 및 통합 | ① 기존 | ② 향상 | ③ 최적화 | ④ |  |
| 정적 용량이 할당된 기기를 수동 관리 | 정책 기반 용량 할당 및 사후 조정을 통한 자동 반복적 방법을 사용하여 기기 관리 | 동적 조정을 통한 지속적 통합/지속적 배포(CI/CI)원칙 | 관련 기능 없음 |

**【제로트러스트 기술수준-네트워크, 전체】**

**A3**

# **(핵심요소3 : 네트워크)** 다음은 ‘네트워크’와 관련된 보안 기능입니다.

# 관련된 제품명을 기재해주시고, 각 부문에서 귀사의 제품은 어느 단계에 있습니까?

① ‘네트워크’와 관련된 보안 제품/서비스 없음

**☞ A4로 이동**

② ‘네트워크’와 관련된 보안 제품/서비스 있음

**☞ A3-1로 이동**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **A3. 제품명** | | **( )**  ※ 귀 사의 제품/서비스는 모두 기재해주시고 아래 항목은 제품/서비스의 전반적인 단계에 대해 응답해주십시오 | | | | **응답** |
|  |  | ① 기존 | ② 향상 | ③ 최적화 | ④ |  |
|  |  |  |  | 네트워크 구조는 주변 |  |
| **A3-1.** | 네트워크 세분화 | 대규모 경계/분리를 사용하는 네트워크 구조 정의 | 일부 내부적인 세분화를 갖는 송수신 소규모 경계를 통해 더 많은 네트워크 구조 정의 | 응용 워크플로우를 기반으로 완벽히 분산된 송수신 세부경계 및 더욱 깊은 내부 세분화로  구성됨 | 관련 기능 없음 |
| **A3-2.** | 위협 대응 | ① 기존 | ② 향상 | ③ 최적화 | ④ |  |
| 알려진 위협 및 정적 트래픽 필터링을 핵심 기반으로 위협 보호 수행 | 위협을 사전에 발견하기 위한 기본 분석 포함 | 컨텍스트 기반 신호와 기계학습 기반 위협 보호 및 필터링 통합 | 관련 기능 없음 |
| **A3-3.** | 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 |
| **A3-4.** | 가시성 및 분석 | ① 기존 | ② 향상 | ③ 최적화 | ④ |  |
| 중앙 집중식 수집 및 분석을 통하여 경계에서 가시성 제공 | 수동 정책 기반 경고 및 트리거를 사용하여 여러 센서 종류와 위치를 통한 통합 분석 | 자동화된 경고 및 트리거를 사용하여 여러 센서 종류와 위치를 통한 통합 분석 | 관련 기능 없음 |
|  |  | ① 기존 | ② 향상 | ③ 최적화 | ④ |  |
| **A3-5.** | 자동화 및 통합 | 변경 관리 워크플로우에 따라 네트워크 및 환경 변경을 수동으로 초기화 및 실행 | 수동으로 네트워크 및 환경 변화를 시작하기 위한 자동화된 워크플로우 사용 | 네트워크 및 환경설정을 위해 지속적 통합 지속적 배포(CI/CD) 배포 모델에 따라, 자동화와 함께 코드로서의 인프라를 사용 | 관련 기능 없음 |

**【제로트러스트 기술수준-시스템, 전체】**

**A4**

# **(핵심요소4 : 시스템)** 다음은 ‘시스템’과 관련된 보안 기능입니다.

# 관련된 제품명을 기재해주시고, 각 부문에서 귀사의 제품은 어느 단계에 있습니까?

① ‘시스템’과 관련된 보안 제품/서비스 없음

② ‘시스템’과 관련된 보안 제품/서비스 있음

**☞ A5로 이동**

**☞ A4-1로 이동**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **A4. 제품명** | | **( )**  ※ 귀 사의 제품/서비스는 모두 기재해주시고 아래 항목은 제품/서비스의 전반적인 단계에 대해 응답해주십시오 | | | | **응답** |
|  |  | ① 기존 | ② 향상 | ③ 최적화 | ④ |  |
|  |  |  | 시스템 접근 시 중앙 집중적 인증/인가/모니터링과 속성에 의존하며, MFA 인증을 기본으로 시스템 파일, 디렉토리에 접속하거나 주요 명령어를 실행할 때 접근제어 정책에 따라 보안정책 적용 | 시스템 접근시 MFA |  |
| **A4-1.** | 접근 | 시스템 접근을 위한 계정 인증은 로컬  시스템에 저장된 | 인증 및 엔드포인트 시스템의 신뢰도를 기반으로 접근인가  진행. 시스템에 영향을 | 관련 |
|  | 통제 | ID/패스워드 등 단순 | 미치는 명령 실행시 | 기능 |
|  |  | 인증을 기반으로 하고 정적 속성 등 최소한의 권한 분리 정책 적용 | 실시간 신뢰도 재산정 및 위험 분석을 기반으로 강력하고  지속적인 접근제어 | 없음 |
|  |  |  | 정책 적용 |  |
| **A4-2.** | 시스템 계정 관리 | ① 기존 | ② 향상 | ③ 최적화 | ④ |  |
|  |  | 접근 인가를 진행하는 |  |
| 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 | 권한 사용자의 계정 관리가 독립 시스템을 기반으로 통합적으로 이루어지고 권한 사용자의 보안 관리 정책이 계정 관리와 통합  및 중앙 일원화되어 | 관련 기능 없음 |
|  |  | 접근제어 정책이 적용 |  |
| **A4-3.** | 네트워크 분리 정책 | ① 기존 | ② 향상 | ③ 최적화 | ④ |  |
| 네트워크 상에서 | 일부 시스템을 중요도에 따라 세분화하여 시스템들 간 접속 이동에 있어 보안 정책 적용 |  |  |
| 시스템들이 분리되어  있지 않거나, 중요도 | 중요 등급 및 기능별  분류, 세분화 및 강력한 | 관련 |
| 구분 없이 네트워크 | 시스템 보안 접근 정책을 | 기능 |
| 경계형 모델을 기반으로  시스템 영역을 구분하고 | 기반으로 분류 그룹간  이동 통제 | 없음 |
| 배치 |  |  |
| **A4-4.** | 시스템 보안 및 정책 관리 | ① 기존 | ② 향상 | ③ 최적화 | ④ |  |
| 온프레미스 시스템 보안 패치 및 정책 변경은 수동으로 이루어짐 | 온프레미스 및 클라우드 시스템에 대한 일관되고 자동화된 보안 패치 기능 | 온프레미스 및 클라우드 상의 모든 시스템 보안 상태에 대한 실시간 모니터링, 심각한 위협에 대한 자동화된 보안 패치  및 정책 변경 가능 | 관련 기능 없음 |
|  |  | ① 기존 | ② 향상 | ③ 최적화 | ④ |  |
| **A4-5.** | 가시성 및 분석 | 외부 센서 및 시스템과 격리된 상태에서 시스템 상태 및 보안 모니터링 수행 | 일부 외부 센서와 시스템을 사용하여 컨텍스트 관점에서, 시스템 상태 및 보안  모니터링 수행 | 외부 센서와 시스템을 사용하여 지속적이고 동적인 응용 상태 및 보안 모니터링 수행 | 관련 기능 없음 |
| **A4-6.** | 자동화 및 통합 | ① 기존 | ② 향상 | ③ 최적화 | ④ |  |
| 시스템 제공시, 응용 호스팅 위치와 접근을 설정 | 변경된 상태를 기기와 네트워크 구성 요소에 알림 | 보안과 성능 최적화를 위한 지속적인 환경 변화에 적응 | 관련 기능 없음 |

**【제로트러스트 기술수준-응용 및 워크로드, 전체 】**

**A5**

# **(핵심요소5 : 응용 및 워크로드)** 다음은 ‘응용 및 워크로드’와 관련된 보안 기능입 니다.

# 관련된 제품명을 기재해주시고, 각 부문에서 귀사의 제품은 어느 단계에 있습니까?

① ‘응용 및 워크로드’와 관련된 제로트러스트 보안 제품/서비스 없음

② ‘응용 및 워크로드’와 관련된 제로트러스트 보안 제품/서비스 있음

**☞ A6으로 이동**

**☞ A5-1로 이동**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **A5. 제품명** | | **( )**  ※ 귀 사의 제품/서비스는 모두 기재해주시고 아래 항목은 제품/서비스의 전반적인 단계에 대해 응답해주십시오 | | | | **응답** |
| **A5-1.** | 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 |
|  |  | ① 기존 | ② 향상 | ③ 최적화 | ④ |  |
|  |  | 알려진 위협에 대한 범용 | 일부 응용별 보호 기법을 사용하여 알려진 위협에 대한 보호를 적용하여, 응용 워크플로우와 위협 보호에 대한 기본적인 통합 | 응용 동작을 이해하고 설명하는 보호 기법을 제공하는 분석을 사용하여, 응용 워크플로우와 위협 보호에 대한 강력한 통합 |  |
| **A5-2.** | 위협  보호 | 보호 기법을 적용하여,  응용 워크플로우와 위협 | 관련  기능 |
|  |  | 보호에 대한 최소한의 통합 | 없음 |
|  |  | ① 기존 | ② 향상 | ③ 최적화 | ④ |  |
|  |  | 일부 중요 클라우드 | 모든 클라우드 응용과 일부 온프레미스 응용은 인터넷을 통해 사용자가 직접 접속하며, 그 외의 다른 응용은 VPN을 통한  접속 |  |  |
| **A5-3.** | 접근성 | 응용은 인터넷을 통해  사용자가 직접 접속하며, | 모든 응용은 인터넷을  통해 사용자가 직접 접속 | 관련  기능 |
|  |  | 그 외의 다른 응용은 VPN을 통한 접속 | 가능 | 없음 |
|  |  | ① 기존 | ② 향상 | ③ 최적화 | ④ |  |
|  |  |  | 동적 시험 방법 사용을 | 배포되는 응용에 대한 |  |
| **A5-4.** | 응용보안 | 주로 정적 수동 검사  방법을 통해, 배포 전 | 포함하여, DevSecOps  형태의 응용 개발 및 | 정기적인 자동화된  시험을 사용하여, 개발과 | 관련  기능 |
|  |  | 응용 보안 테스트 수행 | 배포 과정에 응용 보안  테스트 통합 | 배포과정에서 응용 보안  테스트 통합 | 없음 |
|  |  | ① 기존 | ② 향상 | ③ 최적화 | ④ |  |
| **A5-5.** | 가시성 및 분석 | 외부 센서 및 시스템과 격리된 상태에서 응용 상태 및 보안 모니터링 수행 | 일부 외부 센서와 시스템을 사용하여 컨텍스트 관점에서, 응용 상태 및 보안 모니터링 수행 | 외부 센서와 시스템을 사용하여 지속적이고 동적인 응용 상태 및 보안 모니터링 수행 | 관련 기능 없음 |
| **A5-6.** | 자동화 및 통합 | ① 기존 | ② 향상 | ③ 최적화 | ④ |  |
| 응용 제공시, 응용 호스팅 위치와 접근을 설정 | 변경된 상태를 기기와 네트워크 구성 요소에 알림 | 보안과 성능 최적화를 위한 지속적인 환경 변화에 적응 | 관련 기능 없음 |

**【제로트러스트 기술수준-데이터, 전체】**

**A6**

# **(핵심요소6 : 데이터)** 다음은 ‘데이터’와 관련된 보안 기능입니다.

# 관련된 제품명을 기재해주시고, 각 부문에서 귀사의 제품은 어느 단계에 있습니까?

① ‘데이터’와 관련된 제로트러스트 보안 제품/서비스 없음

**☞ A7로 이동**

② ‘데이터’와 관련된 제로트러스트 보안 제품/서비스 있음

**☞ A6-1로 이동**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **A6. 제품명** | | **( )**  ※ 귀 사의 제품/서비스는 모두 기재해주시고 아래 항목은 제품/서비스의 전반적인 단계에 대해 응답해주십시오 | | | | **응답** |
| **A6-1.** | 데이터 목록 관리 | ① 기존 | ② 향상 | ③ 최적화 | ④ |  |
| 데이터를 수동으로 | 일부 자동화된 추적을 | 강력한 태그 작업 및 |  |
| 분류하고 데이터 목록 | 기반으로, 수동으로 | 추적으로 지속적인 | 관련 |
| 작업이 부실하여, | 데이터 목록 작업 수행. | 목록 작업. 기계 학습 | 기능 |
| 일관되지 않은 데이터 분류 | 수동 정적인 방식을 조합하여 데이터 분류 | 모델을 사용하여 분류 강화 | 없음 |
| **A6-2.** | 접근 결정 방법 | ① 기존 | ② 향상 | ③ 최적화 | ④ |  |
| 정적 접근제어를 사용하여 데이터 접근 관리 | 식별자, 기기 위험도 및 기타 속성을 고려하는 최소 접근 제어 기법을 사용하여 데이터 접근 관리 | 데이터 접근은 적시/적절한 원칙 및 지속적인 위험기반 결정을 지원하며, 동적으로 이루어짐 | 관련 기능 없음 |
| **A6-3.** | 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 |
| **A6-4.** | 가시성 및 분석 | ① 기존 | ② 향상 | ③ 최적화 | ④ |  |
| 특정 상황을 제외하고는, 유용한 가시성 및 분석을 방해하는 제한된 데이터 목록 보유 | 대부분 데이터는 목록화 되어 마지막 목록 업데이트 이후 관리 가능. 분석은 평문 데이터에 한정됨 | 데이터는 목록화되어 언제든지 관리 가능. 의심스러운 행위에 대한 모든 접근 이벤트 로그 및 분석. 암호화된  데이터에 분석 수행 | 관련 기능 없음 |
|  |  | ① 기존 | ② 향상 | ③ 최적화 | ④ |  |
|  |  |  | 정기적 검사를 통해 높은 가치의 데이터를 찾고, 접근제어 분석, 접근제어 적용 및 백업 보증을 위한 제한된 범위의 자동화된 통합 | 높은 가치의 데이터에 |  |
|  |  | 자동화 및 통합을 | 대한 엄격한 접근제어 |  |
| **A6-5.** | 자동화 | 어렵게하는, 일관되지 | 자동 집행. 높은 가치의 | 관련 |
|  | 및 통합 | 않은 분류 및 레이블 | 데이터는 모두 저장 | 기능 |
|  |  | 지정. 일부 데이터 관리 작업은 자동으로 실행 | 위치에 관계없이 백업됨. 데이터 목록은 자동으로  업데이트 | 없음 |

**B**

**제로트러스트 주력 및 협력 분야 수요 (SQ1. 1~3) 응답자만)**

+보안영역별 중요성 【SQ1. 1-3 응답자만, 순위형】

# **B1** 귀사에서 제로트러스트 보안 영역에 대해 가장 주력하고 있는 보안 영역은 어느 부분입니까?

# 최대 2순위까지 응답해 주십시오.

① 식별자-신원 영역

④ 시스템 영역

**1순위**

② 기기 및 엔드포인트 영역

⑤ 응용 및 워크로드 영역

**2순위**

③ 네트워크 영역

⑥ 데이터 영역

+보안영역별 중요성 【 SQ1. 1-3 응답자만, SA】

# **B2** 귀사에서 중요하게 생각하는 보안영역은 무엇입니까? 순서대로 나열해주세요.

**중요순위 > > > > >**

① 식별자-신원 영역

④ 시스템 영역

② 기기 및 엔드포인트 영역

⑤ 응용 및 워크로드 영역

③ 네트워크 영역

⑥ 데이터 영역

+보안영역별 시급성 【 SQ1. 1-3 응답자만, SA】

# **B3** 귀사에서 시급하게 개발해야하는 보안영역은 무엇입니까? 순서대로 나열해주세요.

**시급순위 > > > > >**

① 식별자-신원 영역

④ 시스템 영역

② 기기 및 엔드포인트 영역

⑤ 응용 및 워크로드 영역

③ 네트워크 영역

⑥ 데이터 영역

+타 공급군 기업과 협업 의향 【 SQ1. 1-3 응답자만, SA】

# **B4** 타 공급군 기업과 협업하여(ex. 컨소시엄, 얼라이언스) 제로트러스트 보안 영역을 확대할

# 의향이 있습니까?

① 있다 **☞ B5로 이동**

② 없음 **☞ C1으로 이동**

③ 모르겠음 **☞ C1으로 이동**

+협업 의향 보안 영역 【B4. 1) 응답자만, 순위형】

# **B5** 타 공급군 기업과 협업한다면, 어떤 영역과 가장 협업하고 싶습니까? 3순위까지 응답하여 주십

# 시오.

**1순위**

**2순위**

**3순위**

① 식별자-신원 영역

② 기기 및 엔드포인트 영역

③ 네트워크 영역

④ 시스템 영역

⑤ 응용 및 워크로드 영역

⑥ 데이터 영역

**C**

**제로트러스트 관련 기술 연구개발 (SQ1. 1~3) 응답자만)**

+제로트러스트 관련 연구개발 활동 【 SQ1. 1-3 응답자만, SA】

# **C1** 귀사는 ‘제로트러스트’ 관련 연구개발 활동을 하고 계십니까?

① 예 **☞ C2로 이동**

② 아니오 **☞ C3으로 이동**

+제로트러스트 연구개발 투자액 【C1. 1) 응답자만, Open】

# **C2** 귀사의 ‘제로트러스트’ 관련 연구개발 관련 투자액은 어느정도 되십니까?



**백만원**

+ 제로트러스트 연구개발시 애로사항 【전체, MA】 \*추후 FGI 질문 사항

# **C3** 연구개발 시 애로사항은 무엇입니까? 모두 선택해 주십시오.

 ① 기술개발 인력 확보의 어려움  ② 기술 정보 부족 및 획득 곤란  ③ 연구 설비기자재 부족

 ④ 각종 행정규제 및 제도의 미비(ex. 가이드, 로드맵, 표준화 등)  ⑤ 자금 부족

 ⑥ 기타 ( )

+ 향후 제로트러스트 연구 개발투자 전망 【전체, SA】

# **C4** 향후 제로트러스트 관련 연구개발 투자는 어떻게 되십니까?

① 대폭 줄일 것이다

② 소폭 줄일 것이다

③ 현상 유지할 것이다

④ 소폭 늘릴 것이다

⑤ 대폭 늘릴 것이다

**D**

**KOZETA 인지여부**

+KOZETA 인지여부 【전체】

# **D1** 귀하께서는 한국제로트러스트위원회(KOZETA)에 대해 들어보셨습니까?

① 처음 들어봤다. **☞ D2로 이동**

② 들어봤으나, 자세히 알지는 못한다. **☞ D2로 이동**

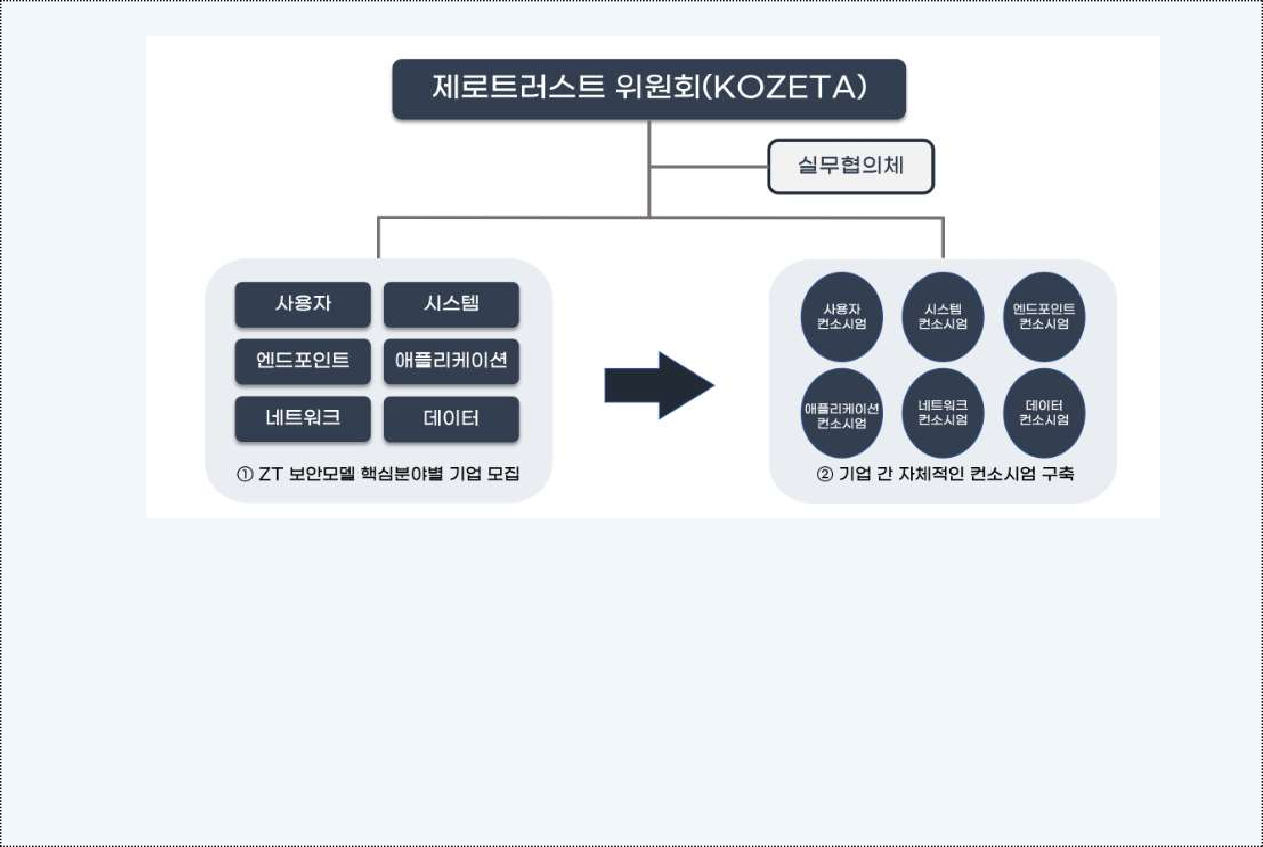
③ 자세히 알고 있으나, 참여기업은 아니다. **☞ D2로 이동**

④ 자세히 알고있으며, 참여기업이다. **☞ Z1으로**

+ KOZETA 참여 수요 【전체, D1 1-3응답자만】

# **D2** 산업계 주도 제로트러스트 모델 개발을 위한 공급 수요기업 간 자유로운 협력환경 조성을

# 지원하기 위해 KOZETA를 운영하고 있습니다. KOZETA에 참여할 의사가 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 의사가 있다 **☞ Z1로 이동**

② 의사 없다 **☞ 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 보유 기술과 앞으로의 개발 방향** 2. **제로트러스트 시장 확대 사유 및 확대 시 어려웠던 점** 3. **제로트러스트 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 \***