<주요 Q&A>

원격 근무 환경에서의 계정 보안 강화

Q1. 제로트러스트 기반의 사용자 인증 보안 솔루션과 국내 적용 사례는 어떻게 되나요?

삼성SDS의 SingleID가 제로트러스트 구현을 위한 인증 보안 솔루션 중의 하나로, 삼성 SDS 및 일부 관계사 적용되어 서비스 중입니다.

Q2. 정보유출 관점에서 스마트폰 등 외부기기를 통한 화면 촬영에 대한 보안책도 있는지요?

물리적인 화면을 보호하기 위해서는 특정 장소에서 휴대기기의 기능을 통제하는 MDM을 도입하거나 물리적 통제(반입금지 등)등이 수단이 될 것 같습니다.
다만, 재택근무가 확대되는 환경에서 물리적 통제만으로는 어려우므로 관련 전문 보안 솔루션을 도입하시는 것이 좋습니다. 삼성SDS도 관련 솔루션 출시를 위한 검토 중입니다.

Q3. 최근 카카오워크 등 클라우드 기반의 외부 플랫폼도 활용하고 있는데요, 외부 플랫폼도 연계하여 관리 가능한가요?

요즘 SaaS에 대한 연계가 필수적인데요, Workday 등 다수 Cloud SaaS 앱과도 연계가 가능합니다. (SAML, OIDC 등 활용)

Q4. 이상행위탐지시스템은 이미 출시된 제품인가요?

네, 현재 상품으로 출시되어 서비스 중입니다.

Q5. 일반적으로 사전 탐지가 어려운 것으로 알고 있습니다. 사전 탐지를 위한 요건들은 어떤 것들이 있는지요?

사전탐지에 대한 부분은 일단 공격에 대한 축적된 지식을 기반으로 한 시나리오를 통해 선제 대응해야 하며, 이후 지속적인 지식화 작업으로 사전탐지 대응력을 높여가야 합니다.

Q6. Analytics 솔루션 자체가 모든 개인정보 및 파일에 접근하는데, 개인정보침해와 같은 이슈는 없나요?

모든 데이터는 사전 개인정보수집/이용 동의 후 활용하며, 개인정보보호법 내에 명시된 데이터 관리 시스템 및 접근 가능한 운영자 관리 기준을 체크리스트화 하여 상시 점검을 통해 관련 문제가 생기지 않도록 대응하고 있습니다.

Q7. 계정관리를 통합하려면 각종 시스템에서 사용할 수 있는 모듈이 제공되어야 하는데 그러한 솔루션을 보유하고 계신지요?

SingleID 솔루션은 업계 표준인 OIDC, SAML 프로토콜을 활용하여 연계 지원하고 있습니다.

Q8. 재택근무 시 다양한 기기로 원격으로 접속하는데 보안에 취약한 기기 보안은 어떻게 되어 있는지 궁금합니다.

접속기기의 보안취약성에 대한 부분은 헬스체크용 Agent를 배포 후 이에 대한 로그를 수집하지 않으면 많은 어려움이 있습니다. 다만, 해당 기기가 수행하는 행위 자체를 보고 이상함을 판단하여 대응력을 높이는 방안으로도 충분히 대응 가능할 것으로 생각합니다.