참고 1 실시간 탐지정보 공유(C-TAS연동) FAQ

1. 왜 탐지정보를 실시간 공유해야 하는지?(추진 목적)

o 「K-사이버방역 추진 전략」('21.2.19)에 따라 과기부(한국인터넷진흥원)는 민간기업과 협력기반으로 실시간 공격탐지정보를 공유하고 이를 통해 실시간 사이버공격 현황 파악 및 대응하는 "사이버보안 얼라이언스" 과제 추진 중

o 이를 위해 보안관제, IDC 등 다중이용 서비스 제공자들과 협력체계 구축을 추진 중이며, 다양한 탐지정보 수집을 위해 Secaas 지원 사업의 수혜기업 탐지정보에 대해서 수집 추진 중(시범사업)

※ 수혜기업의 탐지정보 제공 동의하에 수집이 진행될 예정

2. 정보 제공을 위해 꼭 C-TAS에 가입해야 하는지?

o 정보제공 기업 관리를 위해서 가입을 해야 하며, 다만 약식형태로 구성하여 의무활동 제외, 한시적 계정 활성화 등 요구조건 제외

3. C-TAS로 전송해야 하는 정보는?

o 실시간 공격탐지 정보 일체이며, 공격IP·PORT, 탐지명, 탐지룰, 탐지패턴, 탐지규모(DDoS) 등 민감정보를 제외한 사이버공격과 관련된 정보만을 수집할 예정

o 모든 탐지 정보를 제공할 필요는 없으며, 수혜기업 대상 탐지정보만 제공하면 됨

4. KISIA의 Secaas Pool에 들어가면 무조건 정보제공을 해야하는지?

o 지원 대상이 없는 Secaas 기업은 제공할 필요가 없음

5. 제공기업은 있지만 탐지정보가 없는 경우는 어떻게 해야 하는지?

o DB/데이터 백업과 같은 보안 솔루션과 같이 별도의 탐지 기능이 없는 경우 정보를 제공할 필요는 없음

6. 탐지로그를 따로 발생하지 않거나 전송기능이 없는 경우는?

o 실시간 공격 탐지 기능은 있지만 탐지로그가 발생하지 않거나 syslog, snmp, rmon, web api와 같은 로그 전송 기능이 없는 경우 별도의 개발 소요(인력, 비용 등)이 필요하다면 정보제공 필요 없음

o 올해 시범사업 후 가시적인 성과가 나타난다면 해당 기업에 대해서는 발생/전송 등의 기능에 대해 KISA가 개발 지원 등을 추진

7. 언제부터 전송해야 하는지?

o 지원 사업이 시작되는 7월부터 C-TAS 담당자와 협의하여 제공

※ 실시간 탐지정보 수집•분석 시스템 구축(10월쯤 완료 예정) 시점에 따라 수집예정

8. 언제까지 전송해야 하는지?

o 지원사업에 의해 수혜기업이 존재하는 동안만 제공

9. Secaas와 중소기업 매칭 사업은 매년 하는 것으로 아는데 그럼 올해부터 매년 사업이 진행될 때마다 해야 하는 것인지?

o 올해 시범사업 후 가시적인 성과가 나타나면 지속 추진 예정

o 따라서 내년 추진 여부는 미확정

10. 정보를 제공하지 않을 경우 불이익은?

o 올해에는 미 제공에 대한 불이익은 없음.