WISENET

한화테크윈

사이버 보안 강화 활동

2018. 8. 8.

Copyright ⓒ 2018 Hanwha Techwin. All rights reserved

Hanwha Techwin

Contents

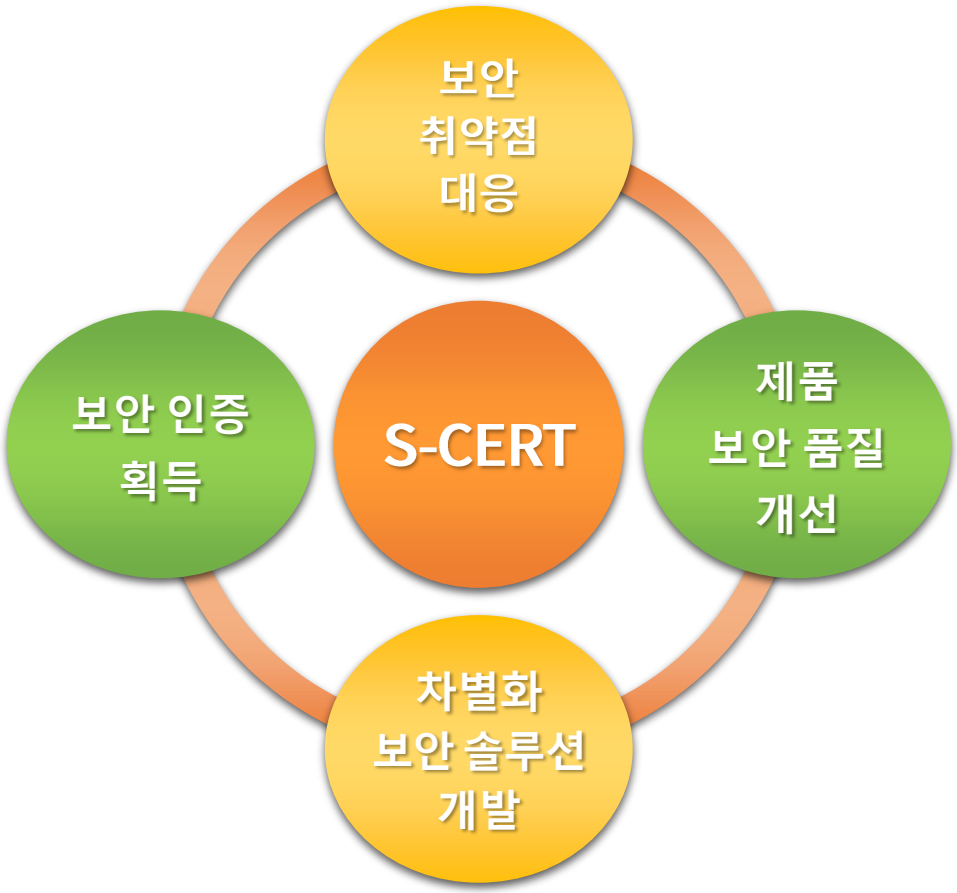
Copyright ⓒ 2018 Hanwha Techwin. All rights reserved

1. 소개

한화테크윈은 보안침해사고 대응팀(S-CERT)을 운영하여 외부로부터 불법적이고 비인가된 보안 침해 사고에 대응하고, 내부 보안 결함 발생을 예방하고 있습니다.

보안 이슈가 발생하면 S-CERT를 중심으로 대책협의회를 구성하여 신속히 대응, 제품 개발단계에서부터 보안성을 사전 점검하고 전문기관을 통하여 정기적으로 침투테스트를 실시하는 등 제품 보안 품질을 높이는데 주력하고 있습니다.

나아가 S-CERT는 영상 감시 분야를 선도하기 위한 차별화 보안 솔루션 개발에도 관심을 가지고 있으며 향상된 제품의 품질을 대외적으로 인정받기 위한 다양한 보안 인증 취득에도 노력을 쏟고 있습니다.



다음 장에서는 4가지 주요 활동인 보안 취약점 대응, 제품 보안 품질 개선, 차별화 보안 솔루션 개발 및 보안 인증 획득 활동을 상세히 살펴보겠습니다.

Copyright ⓒ 2018 Hanwha Techwin. All rights reserved

2. 사이버 보안 강화 활동

2.1 보안 취약점 대응활동

<table>
<tr><th>항 목</th><th>내 용</th></tr>
<tr><td>개 요</td><td>▪ 외부 보안 취약점 모니터링
- CVE*, ICS-CERT, KISA* 및 사이버 보안 뉴스 등 적극적인 취약점 모니터링
▪ 보안침해사고 사후대응규칙에 따른 대응 및 관리
- 보안 이슈 발생 시 보안 침해사고 대책협의회 즉시 소집
- Working Day 5일 이내 펌웨어 발행 원칙
- 보안 취약점 보고서 웹사이트 공지</td></tr>
<tr><td>주요내용</td><td>▪ 보안 취약점 대응 조직
 
</td></tr>
<tr><td>산출물</td><td>▪ 보안 취약점 보고서
▪ 보안 침해 사고 사후대응 규칙</td></tr>
</table>

* CVE: 정보 보안 취약점 표준 코드(Common Vulnerabilities and Exposures), https://cve.mitre.org/about/

* KISA(Korea Internet Security Agency): 한국인터넷진흥원

Copyright ⓒ 2018 Hanwha Techwin. All rights reserved

2. 사이버 보안 강화 활동

2.2 제품 보안 품질 개선활동

2.2.1 내부 보안 점검 활동

항 목	내 용
개 요	■ 보안 점검 활동 수행(개발팀) - 제품군별 보안 점검 체크리스트를 이용하여 점검 - 보안 점검 체크리스트는 년 1회 이상 개정 ■ 보안 테스트 활동 수행(검증팀/S-CERT) - 제품군별 보안 테스트케이스를 이용하여 검증 - 보안 테스트케이스는 년 1회 이상 개정 - 전문 역공학 도구를 이용하여 동적 및 정적 분석 수행
주요내용	■ 제품군별 보안 점검(최소 1회 필수 실시) · 사용자 인증, 통신구간 암호화, 저장 암호화, 백도어 등 보안 기술적 부분의 당사 정책 만족 여부에 대한 개발팀 자체 점검 ■ 제품군별 보안 테스트(최소 2회 필수 실시) · 제품 보안 기능의 당사 정책 만족 여부에 대한 검증팀/S-CERT 점검 ■ 동적 및 정적 분석 · 프로세스/메모리/파일 내 중요정보 사용 유무 검증 · Taint 및 주요 바이너리 로직 분석 · BOF(Buffer Over Flow), FSB(Format String Bug)등 취약점 유무 검증
산출물	■ 보안 점검 체크리스트 및 보안 테스트 결과서 ■ 동적 및 정적 분석 결과서

Copyright ⓒ 2018 Hanwha Techwin. All rights reserved

2. 사이버 보안 강화 활동

2.2.2 외부 전문기관을 통한 침투테스트

항 목	내 용
개 요	▪ 정기적인 침투테스트 수행 - 화이트 해커의 해킹 도구와 기법 등을 이용하여 침투 가능성 진단 - 발견된 취약점 대응책 및 개선 방안 마련
주요내용	▪ Memory corruption, Memory leak, Denial of Service, 펌웨어 변조 등 펌웨어/바이너리에 대한 테스트 ▪ Replay attack, Spoofing attack, Sniffing attack 등 네트워크 관련 테스트 ▪ File download/upload, XSS/CSRF attack, Directory listing/traversal attack, HTTP 헤더 변조 등 웹 어플리케이션에 대한 테스트 ▪ 암호키 크랙, 암호문 복호화 / 해시평문 유추 등 암호화 관련 테스트 ▪ 백도어 분석, 하드웨어 디버그 포트 노출 및 접근, 알려진 오픈소스 취약점 공격 등 기타 테스트
산출물	▪ 각 제품별 침투테스트 결과 및 보안 취약점 조치 계획

2.2.3 사이버 보안 기술 가이드

항 목	내 용
개 요	▪ 기술백서 및 보안 강화 가이드 배포 - 영상감시장비 보안강화를 위한 사이버 보안 기술백서 배포 - 안전한 제품사용을 위한 네트워크 장비 보안 강화 가이드 배포
주요내용	▪ 사이버 보안 기술백서 - 비밀번호 설정, 계정 권한의 분리, 인증 및 암호화, 네트워크 설정 및 구성, 공격 식별 및 차단 등에 대한 내용 포함 ▪ 네트워크 장비 보안 강화 가이드 - 사이버 보안 레벨을 4단계로 정의: 기본 / 보호 / 안전 / 최상위 안전 - 사이버 보안 레벨 별 초기 및 추천 설정 값 가이드
산출물	▪ 사이버 보안 기술백서, 네트워크 장비 보안 강화 가이드

Copyright ⓒ 2018 Hanwha Techwin. All rights reserved

2. 사이버 보안 강화 활동

2.3 차별화 보안 솔루션 개발활동

항 목	내 용
개 요	▪ <u>기기인증서 발급관리 시스템 개발</u> - 장비마다 고유한 기기인증서 및 개인키 적용 - FIPS 140-2 Level 3 인증 장비 적용 - RSA2048, SHA256 등의 안전한 보안 알고리즘 적용 ▪ <u>사용자인증, 비디오 인증, 펌웨어 전자서명 적용</u> - 개발 예정
주요내용	▪ 교체 보드용 기기인증서 발급 및 주입(CS/수리기사) ▪ 장비 별 기기인증서 발급 및 전달(생산라인) ▪ 백업용 기기인증서 대량 발급 및 백업
산출물	▪ 한화테크윈 기기인증서 발급관리 시스템 ▪ 한화테크윈 사설 루트 CA 인증서 및 설치 가이드

2.4 보안 인증 획득활동

항 목	내 용
개 요	▪ <u>주요 보안 인증 획득</u> - 사이버 보안에 대한 기밀성, 무결성 및 가용성이 공식 검증된 제품을 제공하기 위한 각종 주요 보안 인증 획득을 추진
주요내용	▪ 국내 보안 인증 내용 - 영상보안시스템에 대하여 국가기관에서 제정한 인증기준에 따라 시험 - IP카메라의 (보안)기능, 성능 및 장비 간 상호연동 시험 수행 - 인증 없이 초기접속 금지, 사용자 인증 시 SHA2 알고리즘 적용, 일정시간 미사용 시 세션 종료 등 Secured by default 개념 적용 ▪ 국제 공인 인증 획득 추진 예정

Copyright ⓒ 2018 Hanwha Techwin. All rights reserved

WISENET

Hanwha Techwin Co.,Ltd.
13488 경기도 성남시 분당구 판교로 319번길 6 한화테크윈 R&D센터
TEL 070.7147.8771-8
FAX 031.8018.3715
http://hanwha-security.com

Copyright ⓒ 2018 Hanwha Techwin. All rights reserved

Hanwha Techwin